Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО»

Факультет юридический
Кафедра международного права

СОГЛАСОВАНО
И.о. заведующего кафедрой
_____ М.Ю.Макарова
23.05. 2025 г.

СОГЛАСОВАНО
Проректор по учебной работе
_____ М.А.Юрочкин
16.12. 2025 г.

ЭЛЕКТРОННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И НАЦИОНАЛЬНОЕ РЕГУЛИРОВАНИЕ

для специальности 6-05-0421-02 «Международное право»,
6-05-0421-03 «Экономическое право»

Составители: Сачава Полина Дмитриевна, преподаватель кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»;
Ворошкевич Станислав Анатольевич, старший преподаватель кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО».

Рассмотрено и утверждено к утверждению на заседании кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
23.05.2025, протокол № 15

Утверждено на заседании научно-методического совета учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
16.12.2025 г., протокол № 2

РЕЦЕНЗЕНТЫ:
Кафедра философии и права учреждения образования «Белорусский государственный технологический университет»
Потоцкий А.А., заведующий кафедрой, кандидат философских наук, доцент

Синьков Б.Б., заведующий кафедрой гражданского права и профсоюзной работы учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИСТО», кандидат юридических наук, доцент

Регистрационный № УД-003-26/э

Регистрационное свидетельство № 1102645896 от 03.02.2025 г.

АКТУАЛИЗИРОВАН
заседание кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет МИТСО»
_____20_____, протокол №_____

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Электронный учебно-методический комплекс (далее – ЭУМК) по учебной дисциплине «Защита персональных данных: международные стандарты и национальное регулирование» составлен для обучающихся очной (дневной), заочной и заочной сокращенной формы получения высшего образования формы по специальностям 6-05-0421-02 «Международное право», 6-05-0421-03 «Экономическое право».

Изучение учебной дисциплины «Защита персональных данных: международные стандарты и национальное регулирование» имеет важное значение. Важность теоретического осмысления Data Privacy обусловлена тем фактом, что высококвалифицированному специалисту необходимо знать не только национальное законодательство в области защиты персональных данных, но и международное регулирование для понимания тенденций его развития и отражения его в праве Республики Беларусь.

ЭУМК по учебной дисциплине «Защита персональных данных: международные стандарты и национальное регулирование» позволит обучающимся приобрести системное представление о юридической концепции защиты персональных данных в международном праве, а также формирование у студентов знаний и навыков в области работы с персональными данными в соответствии с требованиями национального законодательства.

ЭУМК по учебной дисциплине «Защита персональных данных: международные стандарты и национальное регулирование» направлен на повышение качества подготовки обучающихся специальностей 6-05-0421-02 «Международное право», 6-05-0421-03 «Экономическое право» и содержит: учебную программу; краткий курс лекций; задания для проведения семинарских занятий; вопросы для контроля знаний; вспомогательный материал. ЭУМК составлен для обеспечения доступа обучающихся к учебной, научной, иной литературе, учебной программе, учебно-методической документации, учебно-методическим, информационно-аналитическими материалам по учебной дисциплине «Защита персональных данных: международные стандарты и национальное регулирование».

Основные цели ЭУМК:

разработка и внедрение в образовательный процесс инновационных образовательных технологий, адекватных компетентностному подходу;

планирование, организация и методическое обеспечение самостоятельной управляемой работы обучающихся;

совершенствование методики преподавания учебной дисциплины «Защита персональных данных: международные стандарты и национальное регулирование» и повышение качества образовательного процесса;

усиление взаимосвязи образовательного процесса с научно-исследовательской работой обучающихся;

выработка умений использовать обучающимися полученные теоретические знания в профессиональной деятельности и повседневной жизни, повышение правовой культуры и воспитание уважения к закону;

обеспечение профессиональной направленности преподавания учебной дисциплины «Защита персональных данных: международные стандарты и национальное регулирование».

Вышеуказанные цели реализуется посредством решения ряда следующих задач:

ознакомление обучающихся с процессом формирования и эволюции концепции защиты персональных данных;

формирование представления о правовой природе и элементах защиты персональных данных, которые нашли отражение в международном праве и в праве Республики Беларусь;

формирование у обучающихся необходимой теоретической и методологической базы и практических навыков работы с персональными данными в контексте законодательства о защите персональных данных;

определение наиболее эффективных правовых средств и методов защиты персональных данных.

Структура ЭУМК. В соответствии с учебной программой учреждения высшего образования по дисциплине «Защита персональных данных: международные стандарты и национальное регулирование» весь материал сгруппирован в 10 темах. Каждая тема содержит лекционный материал («Теоретический раздел»); практические задания для проработки теоретического материала («Практический раздел»); задания для управляемой самостоятельной работы, тестовые задания и вопросы для осуществления контроля знаний («Раздел контроля знаний»), а также список рекомендуемой литературы («Вспомогательный раздел»).

Рекомендации по организации работы с ЭУМК. Для эффективного усвоения получаемых знаний обучающимся рекомендуется первоначальное ознакомление с учебной программой по дисциплине «Защита персональных данных: международные стандарты и национальное регулирование». В учебной программе приводятся требования к освоению учебной дисциплины, общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины, распределение аудиторного времени по видам занятий; формы текущей аттестации по учебной дисциплине; содержание учебного материала и другая значимая информация.

Усвоение материала по каждой теме учебной дисциплины рекомендуется начинать с изучения материалов соответствующей лекции, которые позволят актуализировать знания, полученные на лекциях («Теоретический раздел») и рекомендуемой литературы («Вспомогательный раздел»), после чего следует проработать практические задания («Практический раздел»). Итоговая проверка знаний проводится по результатам выполнения тестовых заданий, а также на основе примерных вопросов к зачету/экзамену по дисциплине «Защита персональных данных: международные стандарты и национальное регулирование» («Раздел контроля знаний»).

Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
Федерации профсоюзов Беларуси
«Международный университет «МИТСО»
_____ М.А. Юрочкин
_____ 2024
Регистрационный № УД -018/02-24/уч.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И НАЦИОНАЛЬНОЕ РЕГУЛИРОВАНИЕ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности

6-05-0421-02 Международное право
6-05-0421-03 Экономическое право

2024 г.

Контрольный экземпляр

Учебная программа составлена на основе Образовательных стандартов высшего образования (общее высшее образование) ОСВО 6-05-0421-02-2023 для специальности 6-05-0421-02 «Международное право» и ОСВО 6-05-0421-03-2022 для специальности 6-05-0421-03 «Экономическое право», утвержденных Постановлением Министерства образования Республики Беларусь 01.09.2023 г. № 297, учебных планов учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», утвержденного 01.03.2023 рег. № 6-05-0421-02/уч., 09.07.2024 рег. № 6-05-0421-02/уч/з для специальности 6-05-0421-02 «Международное право» и утвержденных 01.03.2023 рег. № 6-05-0421-03/уч., 09.07.2024 рег. №№ 6-05-0421-03/уч/з., 6-05-0421-03/уч/зс для специальности 6-05-0421-03 «Экономическое право»

СОСТАВИТЕЛЬ

П. Д. Сачава, преподаватель кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»;

Н.А. Кодак, старший преподаватель кафедры международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой международного права учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
(протокол № 9 от 16.12.2024);

Научно-методическим советом учреждения образования Федерации профсоюзов Беларуси «Международный университет «МИТСО»
(протокол № 3 от 20.12.2024)

Нормоконтроль
ведущий специалист УМУ
_____Г.Д.Лагунович

Заведующий библиотекой
_____О.О.Бабарикина

I. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Защита персональных данных: международные стандарты и национальное регулирование» входит составной частью в систему дисциплин, обеспечивающих подготовку специалистов с высшим образованием по специальностям по специальности 6-05-0421-02 «Международное право» и 6-05-0421-03 «Экономическое право». Учебная дисциплина относится к циклу дисциплин специализации компонента учреждения высшего образования, изучается в тесной взаимосвязи с учебными дисциплинами «Конституционное право Республики Беларусь», «Конституционное право зарубежных стран».

Во все времена люди старались оберегать свои личные данные. Изначально это осуществилось только путем ограничения физического доступа к данным. Первое документальное закрепление privacy было в 1890 году в статье The Right to Privacy двух американских юристов С. Д. Уоррен и Л. Д. Брендайса. В 1948 году право на частную жизнь было закреплено во Всеобщей декларации прав человека, а в 1950 году – в Европейской Конвенции по правам человека.

Важность теоретического осмысления Data Privacy обусловлена тем фактом, что высококвалифицированному специалисту необходимо знать не только национальное законодательство в области защиты персональных данных, но и международное регулирование для понимания тенденций его развития и отражения его в праве Республики Беларусь.

Цель изучения учебной дисциплины – системное представление о юридической концепции защиты персональных данных в международном праве, а также формирование у студентов знаний и навыков в области работы с персональными данными в соответствии с требованиями национального законодательства.

Задачи учебной дисциплины являются:

ознакомить обучающихся с процессом формирования и эволюции концепции защиты персональных данных;

сформировать представление о правовой природе и элементах защиты персональных данных, которые нашли отражение в международном праве и в праве Республики Беларусь;

сформировать у обучающихся необходимую теоретическую и методологическую базу и практические навыки работы с персональными данными в контексте законодательства о защите персональных данных;

определить наиболее эффективных правовых средств и методов защиты персональных данных.

Изучение учебной дисциплины будет способствовать формированию и развитию следующей **специализированной компетенции:** применять знания и решать практические задачи, возникающие в области защиты данных, пользоваться методами защиты персональных данных от несанкционированного доступа.

В результате изучения учебной дисциплины обучающиеся должны

знать:

основные стадии формирования и эволюции защиты персональных данных в международном праве;

содержание источников права, регулирующих защиту персональных данных на наднациональном и национальном уровнях;

международные и зарубежные подходы к определению персональных данных и их защите;

основное содержание законодательства о персональных данных Республики Беларусь, в том числе его термины и основные требования, права и обязанности, связанные с обработкой персональных данных, порядок организации работы с персональными данными и виды ответственности за нарушение законодательства о персональных данных;

уметь:

выявлять и толковать подлежащие применению международно-правовые акты в сфере защиты персональных данных для определения сведений, входящих в понятие «персональные данные»;

выявлять направления деятельности организации, связанные с обработкой персональных данных, угрозы безопасности персональных данных, обрабатываемых с использованием и без использования средств автоматизации;

определять правовые, организационные и технические меры по обеспечению защиты персональных данных;

анализировать правоприменительную практику Республики Беларусь, государств-членов Евразийского экономического союза, Европейского Союза и иных государств в сфере выявления нарушений законодательства о защите персональных данных;

разрабатывать требуемую в связи с защитой персональных данных организационно-распорядительную документацию;

давать правовую оценку действиям субъектов права, связанных с защитой персональных данных, в соответствии с национальным законодательством и рекомендациями уполномоченных государственных органов;

иметь навыки:

владения методами правовой квалификации фактов и ситуаций, связанных с защитой персональных данных на наднациональном и национальном уровнях;

владения правовой терминологией в сфере защиты персональных данных;

консультирования в рассматриваемой сфере.

Методика изучения учебной дисциплины «Защита персональных данных: международные стандарты и национальное регулирование» основана на оптимальном сочетании теоретического обучения, самостоятельной работы и практического применения полученных знаний, что позволит надлежащим образом организовать изучение данной учебной дисциплины. На практических занятиях студент научаться применять полученные на лекциях теоретические знания, решать практические задачи и составлять необходимые юридические документы.

При преподавании используются следующие методы обучения: теоретико-информационные (проблемная лекция, лекция-диспут) и практико-ориентированные (дискуссия, учебные дебаты, мозговой штурм, круглые столы, деловые игры), реализуемые на практических занятиях. Используются методы контроля, самоконтроля и самооценки. Применяются современные мультимедийные технологии преподавания, обеспечивающие наглядность обучения, тестовая система проверки знаний.

Распределение аудиторных часов по видам занятий и семестрам.
Виды и формы аттестации

Семестр	Количество академических часов							Самостоят. работа	Форма промежуточной аттестации
	Всего	Аудит.	Из них						
			Лекции	Лабор. занятия	Практ. занятия	Семи-нары	УСР		
Очная (дневная) форма получения общего высшего образования 6-05-0421-02 Международное право / 6-05-0421-03 Экономическое право									
6/5	68	34	20			10	4	34	экз.
Всего	68	34	20			10	4	34	
Заочная форма получения общего высшего образования 6-05-0421-02 Международное право / 6-05-0421-03 Экономическое право									
4/5	68	6	6					30	
5/6		2				2		30	экз.
Всего	68	8	6			2		60	
Заочная сокращенная форма получения общего высшего образования 6-05-0421-03 Экономическое право									
4	68	4	4					30	
5		4	2			2		30	экз.
Всего	68	8	6			2		60	

II. СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Источники права, регламентирующие защиту персональных данных

Всеобщая декларация прав человека 1948 г. Конвенция о защите прав человека и основных свобод (Европейская конвенция по правам человека) 1950 г. Договор о функционировании Европейского союза 1957. Рекомендация № 509 Парламентской Ассамблеи Совета Европы 1968г.

Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г.: общая характеристика.

Директива 95/46/ЕС 1995г. Хартия Европейского союза по правам человека 2000 г. Директива 2002/58/ЕС 2002 г.

Генеральный регламент о защите персональных данных 2016 г. Влияние принятия и применения Генерального регламента на субъектов права Республики Беларусь.

Законодательство о защите персональных данных государств – членов ЕАЭС.

Тема 2. Приватность и идентификация личности: международные подходы

Личная жизнь человека в различных исторических периодах. Вмешательство государственных институтов в частную жизнь. Законы об именах. Личная жизнь и анонимность. Появление концепции невмешательства в личную жизни.

Приватность как универсальное право человека. Понятие приватности и защиты персональных данных. История информационной приватности. Виды приватности.

Тема 3. Персональные данные в Европейском союзе: понятие и содержание

Предпосылки создания и вступления в силу Генерального регламента о защите персональных данных.

Материальная и территориальная сфера действия Генерального регламента о защите персональных данных.

Ключевые термины и определения в сфере защиты персональных данных. Персональные данные. Обработка персональных данных. Субъекты: «Data controller», «Data processor», «Data subject». Согласие на обработку персональных данных.

Принципы обработки персональных данных. Законность, справедливость и прозрачность обработки персональных данных. Ограничение обработки персональных данных целью. «Минимизация данных». Точность и достоверность персональных данных. Ограничение срока хранения персональных данных. Целостность и конфиденциальность обработки персональных данных.

Законные цели обработки персональных данных. Согласия и отчетность. Типовые документы.

Организационные, административные и технические методы защиты персональных данных.

Тема 4. Средства правовой защиты персональных данных и практика исполнения генерального регламента

Стандартные договорные оговорки. Бизнес-процессы юридических лиц. «Best practices». Представители на территории Европейского Союза.

Виды нарушений Генерального регламента о защите персональных данных. Действия субъектов правоотношений в случаях нарушений в сфере защиты персональных данных.

Меры ответственности за несанкционированную обработку персональных данных. Порядок и условия наложения административного штрафа. Возмещение ущерба контролером в пользу субъекта персональных данных. Уголовная ответственность за нарушение правил обработки персональных данных в государствах-членах Европейского Союза.

Тема 5. Правовое регулирование защиты персональных данных в Республике Беларусь

История регулирования персональных данных до принятия Закона «О защите персональных данных»: до 01.09.2022 года.

Основные нормативные правовые акты в сфере защиты персональных данных: Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных», приказы Оперативно-аналитического центра при Президенте Республики Беларусь, иные акты законодательства.

Закон Республики Беларусь «О защите персональных данных»: общая характеристика.

Национальный центр защиты персональных данных Республики Беларусь: правовой статус, основные задачи и функции.

Приказы директора Национального центра защиты персональных данных Республики Беларусь: общая характеристика, их роль при регулировании защиты персональных данных.

Тема 6. Основные понятия в области защиты персональных данных в Республике Беларусь

Научные подходы к понятию «персональные данные». Нормативное понятие и признаки персональных данных в Республики Беларусь. Соотношение понятий «персональные данные» и «банковская тайна», «врачебная тайна», «нотариальная тайна».

Категории персональных данных. Общедоступные персональные данные. Специальные персональные данные. Биометрические и генетические персональные данные.

Субъекты правоотношения в сфере защиты персональных данных: субъект персональных данных, оператор и уполномоченное лицо. Их функции, права и обязанности в рассматриваемом правоотношении.

Понятие обработки персональных данных, их виды и формы. Общие требования к обработке персональных данных: законность, соразмерность и справедливость, наличие правового основания, ограничение цели, запрет избыточности, прозрачность, ограничение хранения, достоверность.

Особенности обработки персональных данных при их обезличивании, блокировании и удалении. Предоставление и распространение персональных данных.

Тема 7. Правовые основания для обработки персональных данных в Республике Беларусь

Согласие субъекта персональных данных и его характеристики. Условия получения согласия субъекта персональных данных на обработку персональных данных.

Обработка персональных данных без согласия субъекта персональных данных, в том числе специальных персональных данных. Обработка персональных данных по поручению оператора: общая характеристика, обязательные договорные пункты.

Обработка персональных данных в сфере образования и медицины. Особенности обработки персональных данных в рамках трудовых отношений.

Трансграничная передача персональных данных.

Сравнительный анализ оснований обработки персональных данных по законодательству Республики Беларусь и в соответствии с Генеральным регламентом о защите персональных данных.

Тема 8. Права субъектов персональных данных и механизм их реализации в Республике Беларусь

Право на отзыв согласия субъекта персональных данных. Право на получение информации, касающейся обработки персональных данных, и изменение персональных данных. Право на получение информации о предоставлении персональных данных третьим лицам. Право требовать прекращения обработки персональных данных и (или) их удаления. Право на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных. Право на возмещение морального вреда, причиненного незаконной обработкой персональных данных.

Порядок реализации прав субъекта персональных данных.

Основные обязанности оператора. Правовые, организационные и технические меры по обеспечению защиты персональных данных. Состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты персональных данных.

Требования к технической и криптографической защите персональных данных.

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь

Политика оператора (уполномоченного лица) в отношении обработки персональных данных и реестр обработки персональных данных.

Локальные правовые акты оператора и другие меры по обеспечению защиты персональных данных.

Лицо, ответственное за осуществление внутреннего контроля за защитой персональных данных в организации: основные требования, права и обязанности.

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных

Понятие нарушения законодательства в сфере персональных данных. Характеристика незаконности обработки персональных данных.

Административная, уголовная и гражданско-правовая ответственность за нарушение законодательства о персональных данных.

Дисциплинарная ответственность за нарушение порядка обработки персональных данных, установленного законодательством и локальными правовыми актами.

III. УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения общего высшего образования

6-05-0421-02 Международное право / 6-05-0421-03 Экономическое право

Номер раздела, темы	Название раздела, темы	Всего часов	Количество аудиторных часов				УСР	Самостоятельная работа	Литература	Форма контроля
			Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия				
6 семестр / 5 семестр										
1.	Источники права, регламентирующие защиту персональных данных	4	2					2	[1]	
2.	Приватность и идентификация личности: международные подходы	6	2		2			2	[1]	УО, РПЗ, ЗТТ
3.	Персональные данные в европейском праве: понятие и содержание	8	2					6	[1]	
4.	Средства правовой защиты персональных данных и практика исполнения генерального регламента	8	2				2	4	[1]	РПЗ, ЗТТ
5.	Правовое регулирование защиты персональных данных в Республике Беларусь	6	2		2			2	[1]	УО, РПЗ, ЗТТ (ТА)[1]
6.	Основные понятия в области защиты персональных данных в Республике Беларусь	8	2				2	4	[1]	РПЗ, ЗТТ, Э
7.	Правовые основания для обработки персональных данных в Республике Беларусь	6	2		2			2	[1]	УО, РПЗ, ЗТТ
8.	Права субъектов персональных данных и механизм их реализации в Республике Беларусь	8	2					6	[1]	
9.	Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь	6	2		2			2	[1]	УО, РПЗ, ЗТТ (ТА)
10.	Ответственность за нарушения законодательства в сфере персональных данных	8	2		2			4	[1]	УО, РПЗ, К
	Всего по дисциплине	**68**	**20**		**10**		**4**	**34**		**экз.**

[1] Текущая аттестация

Заочная форма получения общего высшего образования

6-05-0421-02 Международное право / 6-05-0421-03 Экономическое право

Номер раздела, темы	Название раздела, темы	Всего часов	Количество аудиторных часов				Самостоятельная работа	Литература	Форма контроля
			Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия			
4–5 семестр / 5–6 семестр									
1.	Источники права, регламентирующие защиту персональных данных	7	2				6	[1]	
2.	Приватность и идентификация личности: международные подходы	7					6	[1]	
3.	Персональные данные в европейском праве: понятие и содержание	7	2				6	[1]	
4.	Средства правовой защиты персональных данных и практика исполнения генерального регламента	7					6	[1]	
5.	Правовое регулирование защиты персональных данных в Республике Беларусь	7	1				6	[1]	
6.	Основные понятия в области защиты персональных данных в Республике Беларусь	6					6	[1]	
7.	Правовые основания для обработки персональных данных в Республике Беларусь	6					6	[1]	
8.	Права субъектов персональных данных и механизм их реализации в Республике Беларусь	7	1				6	[1]	
9.	Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь	7			2		6	[1]	УО, РПЗ
10.	Ответственность за нарушения законодательства в сфере персональных данных	7					6	[1]	УО, РПЗ, К
	Всего по дисциплине	**68**	**6**		**2**		**60**		**экз.**

Заочная сокращенная форма получения общего высшего образования

6-05-0421-03 Экономическое право

Номер раздела, темы	Название раздела, темы	Всего часов	Количество аудиторных часов				Самостоятельная работа	Литература	Форма контроля
			Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия			
4-5 семестр									
1.	**Источники права, регламентирующие защиту персональных данных**	7	2				6	[1]	
2.	Приватность и идентификация личности: международные подходы	7					6	[1]	
3.	Персональные данные в европейском праве: понятие и содержание	7	2				6	[1]	
4.	Средства правовой защиты персональных данных и практика исполнения генерального регламента	7					6	[1]	
5.	Правовое регулирование защиты персональных данных в Республике Беларусь	7	1				6	[1]	
6.	Основные понятия в области защиты персональных данных в Республике Беларусь	6					6	[1]	
7.	Правовые основания для обработки персональных данных в Республике Беларусь	6					6	[1]	
8.	Права субъектов персональных данных и механизм их реализации в Республике Беларусь	7	1				6	[1]	
9.	Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь	7			2		6	[1]	УО, РПЗ
10.	Ответственность за нарушения законодательства в сфере персональных данных	7					6	[1]	УО, РПЗ, К
	Всего по дисциплине	**68**	**6**		**2**		**60**		**экз.**

IV. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Василевич, Г. А. Информационное право : учебн. пособие / М. С. Абламейко [и др.] ; под общ. ред. Г. А. Василевича, М. С. Абламейко. – Минск : Адукацыя і выхаванне, 2021. – 424 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

2. Абламейко, М. С. Защита визуальных персональных данных: правовые аспекты / М. С. Абламейко // Веб-программирование и интернет-технологии WebConf2021 : материалы 5-й Междунар. науч.-практ. конференции, Минск, 18–21 мая 2021 г. / БГУ, Механико-математический фак. ; редкол.: И. М. Галкин (отв. ред.) [и др.]. – Минск : БГУ, 2021. – С. 318–321.

3. Абламейко, М. С. Правовое регулирование персональных данных с учетом введения ID-карт и биометрических паспортов / М. С. Абламейко // Журн. Белорус. гос. ун-та. Серия «Право». – 2018. – № 1. – С. 14–20.

4. Абламейко, М. С. Биометрические персональные данные и дипфейки: правовой аспект / М. С. Абламейко, Н. В. Шакель // Право.by : научно-практический журнал / учредитель Национальный центр правовой информации Республики Беларусь, Кафедра ЮНЕСКО по информационным технологиям и праву. – 2024. – № 3. – URL: https://journal.pravo.by/articles/informatsionnoe-pravo-pravovaya-informatizatsiya/biometricheskie-personalnye-dannye-i-dipfeyki-pravovoy-aspekt/ (дата обращения 19.10.2024).

5. Абламейко, М. С. Трансграничная передача персональных данных в рамках ЕАЭС / М. С. Абламейко, Н. В. Шакель // Право.by : научно-практический журнал / учредитель Национальный центр правовой информации Республики Беларусь, Кафедра ЮНЕСКО по информационным технологиям и праву. – 2023. – № 1. – С. 113–120.

6. Архипов, В. В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория / В. В. Архипов // ЮрФак : изучение права онлайн. – URL: https://urfac.ru/?p=144 (дата обращения 19.10.2024).

7. Вабищевич, В. В. Персональные данные: пределы и объем их уголовно-правовой охраны / В. В. Вабищевич // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы : навукова-тэарэтычны часопіс. – 2020. – Т. 10, № 2. – С. 83–90.

8. Вабищевич, В. В. Социально-правовые и исторические предпосылки криминализации вмешательства в персональные данные / В. В. Вабищевич // Журн. Белорус. гос. ун-та. Право. – 2020. – № 1. – С. 61–71.

9. Вабищевич, В. В. Уголовно-правовая охрана персональных данных: отдельные направления совершенствования / В. В. Вабищевич // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Международный университет "МИТСО". – 2023. – № 2 (22). – С. 81–94.

10. Валюшко-Орса, Н. В. Сущностно-содержательные аспекты персональных данных в Республике Беларусь / Н. В. Валюшко-Орса // Журн. Белорус. гос. ун-та. Право. – 2017. – № 2. – С. 17-23.

11. Гавриленко, А. И. К вопросу о возрасте согласия на обработку персональных данных / А. И. Гавриленко // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Междунар. университет "МИТСО". – 2023. – № 2 (22). – С. 95–106.

12. Дудко, М. О. Правовой механизм защиты персональных данных в сети Интернет / М. О. Дудко // Международное гуманитарное право глазами белорусской общественности : материалы междунар. науч. форума, Минск, 30 окт. 2020 г. / Белорус. гос. ун-т ; редкол.: Е. Ф. Довгань (гл. ред.) [и др.]. – Минск : БГУ, 2020. – С. 87–98.

13. Дудко, О. М. Особенности правового регулирования общедоступных персональных данных / М. О. Дудко // Современные проблемы юридической науки и практики в условиях глобализации общественных отношений : сборник научных статей / Учреждение образования "Гродненский государственный университет им. Я. Купалы". – Гродно, 2022. – С. 67–71.

14. Захилько, К. С. Существенный вред как признак уголовной противоправности незаконных действий в отношении информации о частной жизни и персональных данных / К. С. Захилько // Журн. Белорус. гос. ун-та. Право. – 2022. – № 2. – С. 58–68.

15. Ипатов, В. Д. Проблемы применения законодательства о персональных данных в свете развития информационных технологий / В. Д. Ипатов, Н. А. Саванович // Право.by. – 2021. – № 5. – С. 60–65.

16. Ипатов, В. Д. Проблемы применения законодательства о персональных данных в свете развития информационных технологий / В. Д. Ипатов, Н. А. Саванович // Информационные технологии и право: правовая информатизация-2021 : сб. материалы VII Междунар. науч.-практ. конф. (г. Минск, 28 октября 2021 г.) / под общ. ред. А. Ф. Мательского. – Минск, 2021. – С. 156–159.

17. Исаев, А.С. Правовые основы организации защиты персональных данных / А.С. Исаев, Е.А. Хлюпина // СПб. : НИУ ИТМО, 2014. – 106 с. – URL: https://books.ifmo.ru/file/pdf/1570.pdf (дата обращения 19.10.2024).

18. Кирильчик, А. А. Аудиториум ilex. Персональные данные в банках. Биометрические данные и цифровые технологии / А. А. Кирильчик // КонсультантПлюс / ООО «ЮрСпектр». – Минск, 2024.

19. Кунец, А. Г. Научные подходы к пониманию конституционного права на личную жизнь / А. Г. Кунец // Труд. Профсоюзы. Общество = Labour. Trade Unions. Society : ежеквартальный научно-практический журнал / Федерация профсоюзов Беларуси, Междунар. ун-т "МИТСО". – 2018. – № 2. – С. 74–78.

20. Лосев, В. В. Нарушение законодательства о защите персональных данных: административная и уголовная ответственность / В. В. Лосев // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Международный университет "МИТСО". – 2023. – № 2 (22). – С. 65–80.

21. Методологические документы, рекомендации // Национальный центр

защиты персональных данных Республики Беларусь. – URL: https://cpd.by/ (дата обращения 19.10.2024).

22. Михалевич, Е. В. Обработка персональных данных: анализ законодательства и судебной практики – М., 2019. – Вып. 18. – 143 с.

23. Официальные руководства и разъяснения, заключения и рекомендации общеевропейского надзорного органа в области защиты персональных данных // GDPR TEXT. – URL: https://gdpr-text.com/ru/guidelines/ (дата обращения 19.10.2024).

24. Полещук, Д. Г. Видеонаблюдение и видеосъемка как обработка персональных данных / Д. Г. Полещук // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Междунар. университет "МИТСО". – 2023. – № 2 (22). – С. 32–48.

25. Полещук, Д. Г. Ответственность за незаконные действия с персональными данными: текущее состояние и перспективы / Д. Г. Полещук // Законность и правопорядок. – 2020. – № 4. – С. 44-49.

26. Полещук, Д. Г. Уголовная ответственность за незаконные действия с персональными данными: новеллы правового регулирования и направления их возможного практического применения / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2021. – Вып. 16. – С. 756-768.

27. Полещук, Д. Г. Право на защиту персональных данных: конституционные основы и их реализация в законодательстве и правоприменении / Д. Г. Полещук // Конституционное право как фактор динамичного развития белорусского государства: история и современность : материалы респ. науч.-практ. конф., Минск, 15 окт. 2021 г. / Белорус. гос. ун-т ; редкол.: Г. А. Василевич (гл. ред.), А. В. Шавцова; В. Е. Петухова. – Минск : БГУ, 2021. – С. 225–229.

28. Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» : по состоянию на 19.10.2024 г. / А. А. Гаев [и др.] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

29. Рыбак, С. В. Направления развития защиты персональных данных в Республике Беларусь / С. В. Рыбак // Право. Экономика. Социальное партнерство : сб. докладов Междунар. науч.-практ. конф., посвященной 90-летию Учреждения образования Федерации профсоюзов Беларуси "Международный университет "МИТСО" (г. Минск, 26 марта 2020 г.) : в 2 ч. / редкол.: В. В. Лосев (гл. ред.) [и др.]. – Минск : МИТСО, 2020. Ч. 1. – С. 491–496.

30. Саванович, Н. А. К вопросу о соотношении информации о частной жизни и персональных данных / Н. А. Саванович // КонсультантПлюс / ООО «ЮрСпектр». – Минск, 2024.

31. Саванович, Н. А. Персональные данные в условиях технологии Big Data (больших данных): по состоянию на 12.02.2019 г. / Н. А. Саванович // ЭТАЛОН. Правоприменительная практика / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

32. Саванович, Н. А. Эволюция понимания персональных данных на современном этапе: по состоянию на 11.02.2019 г. / Н. А. Саванович // ЭТАЛОН. Правоприменительная практика / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

33. Саванович, Н. А. Дефиниция персональных данных в Законе Республики Беларусь «О защите персональных данных» и проблемы ее применения / Н. А. Саванович // Юридический научно-практический журнал «Юстиция Беларуси». – 2022. – № 6. – С. 41–44. – URL: https://cpd.by/storage/2024/03/Str_41-44-Savanovich_2.pdf (дата обращения 19.10.2024).

34. Саванович, Н. А. Обработка персональных данных в сфере государственного управления на примере Республики Беларусь и Российской Федерации / Н. А. Саванович, Е. В. Кудряшова // Право в современном белорусском обществе. – 2020. – Вып. 15. – С. 144–158.

35. Сачава, П. Д. Защита персональных данных в компании. Локальные документы / П. Д. Сачава // Бюллетень «Меркурый». – Минск, 2024. – № 1. – URL: https://www.cci.by/byulleten-merkuryy/publikatsii/v-interesakh-biznesa/zashchita-personalnykh-dannykh-v-kompanii-lokalnye-dokumenty/ (дата обращения 23.09.2024).

36. Синкевич, К. В. Дискуссия о месте персональных данных в системе объектов гражданских прав / К. В. Синкевич // Государство и право в XXI веке : материалы междунар. науч.-практ. конф., посвященной 95-летию юридического факультета Белорусского государственного университета, 26–27 ноября 2020 года, г. Минск / БГУ, Юридический фак. ; редкол.: Т. Н. Михалёва (гл. ред.) [и др.]. – Минск : БГУ, 2021. – С. 597–602.

37. Тенюта, Е. С. Юридическая ответственность за нарушение законодательства в сфере персональных данных (на примере законодательства Республики Беларусь) / Е. С. Тенюта // Приоритетные направления развития правовой системы общества : материалы IX Междунар. науч.-практ. конференции (Гомель, 12–13 мая 2022 года) : в 2 ч. Ч. 2 / редкол. : И. И. Эсмантович (гл. ред.) [и др.] ; Гомельский гос. ун-т им. Ф. Скорины. – Гомель : ГГУ им. Ф. Скорины, 2022. – С. 104–108.

38. Томашевский, К. Л. Все об обработке и защите персональных данных в трудовых и связанных с ними отношениях / К. Л. Томашевский // Отдел кадров: профессиональный ежемесячный журнал / учредитель ОДО «Профигруп». – 2023. – № 5. – С. 72–79.

39. Шакель, Н. В. Права субъектов персональных данных и юридические возможности их защиты в Республике Беларусь / Н. В. Шакель // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы : навукова-тэарэтычны часопіс. – 2022. – Т. 12, № 3. – С. 14–19.

40. Шакель, Н. В. Проблемы определения статуса сооператоров в праве Республики Беларусь / Н. В. Шакель // Юстиция Беларуси : юридический научно-практический журнал / учредитель Министерство юстиции Республики Беларусь. – 2024. – № 3. – С. 23–26.

41. Шебанова, Н. А. Охрана персональных данных: опыт Европейского

сообщества / Н. А. Шебанова // Журнал Суда по интеллектуальным правам – Москва, 2019. – № 25. – С. 5–14. – URL: https://ipcmagazine.ru/articles/1729209/ (дата обращения 19.10.2024).

42. The European Union data Privacy Directive / Julia M Fromholz - Berkeley Technology Law Journal, 2000. – Volume 15, issue 1. – P. 468–484.

43. Korff, D. The DPO Handbook Guidance for data protection officers in the public and quasi- public sectors on how to ensure compliance with the European Union General Data Protection Regulation (Regulation (EU) 2016/679) // D. Korff, M. Georges. – URL: https://ssrn.com/abstract=3428957 (Date of access: 19.10.2024).

44. Laputko, K. European Data Protection Law: Analysis of European (GDPR), Canadian, and US regulations / K. Laputko // Success Publication. – 2023. – 411 pages.

45. Laputko, K. CIPP/e 2024 prep: European Data Protection Law / K. Laputko. – 2024. – 398 pages.

46. McCarty-Snead, Steven S. Research Guide to European Data Protection Law / Steven S. McCarty-Snead, Anne Titus Hilby. – URL: https://doi.org/10.2139/ssrn.2355833 (Date of access: 19.10.2024).

47. Mondschein, C. F. The EU's General Data Protection Regulation (GDPR) in a Research Context / C. F. Mondschein, C. Monda. // Springer. Fundamentals of Clinical Data Science. – URL: https://doi.org/10.1007/978-3-319-99713-1_5. (Date of access: 19.10.2024).

48. Streinz, T. The Evolution of European Data Law / T. Streinz // Paul Craig and Gráinne de Búrca (eds). Oxford University Press. – Mode of access: http://dx.doi.org/10.2139/ssrn.3762971. (Date of access: 19.10.2024).

49. Handbook on European data protection law // European Union Agency for Fundamental Rights. – Luxembourg: Publications Office of the European Union, 2018. – 402 pages. – URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. (Date of access: 19.10.2024).

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

50. Конституция Республики Беларусь 1994 года (с изм. и доп., принятыми на респ. референдумах 24.11.1996, 17.10.2004 (Решение от 17.11.2004 № 1); в ред. Закона Республики Беларусь от 12.10.2021 № 124-З) // ilex : информ.-поисковая система / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

51. Конвенция о защите физических лиц при автоматизированной обработке персональных данных : заключена в г. Страсбурге 28.01.1981 г.. – URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?doc umentId=0900001680078c46. (дата обращения: 20.10.2024).

52. О соответствии Конституции Республики Беларусь Закона Республики Беларусь «О защите персональных данных» : Решение Конституционного Суда Респ. Беларусь, 29 апреля 2021 г., № Р-1261/2021 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

53. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : с изм. и доп., внес. Законом Респ. Беларусь от 01.06.2022 г. // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ.

Беларусь. – Минск, 2024.

54. Об архивном деле и делопроизводстве в Республике Беларусь: Закон Респ. Беларусь, 25 нояб. 2011 г., № 323-З : с изм. и доп., внес. Законом Респ. Беларусь от 18.04.2022 г. // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

55. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : с изм. и доп., внес. Законом Респ. Беларусь от 10.10.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

56. О мерах по совершенствованию защиты персональных данных : Указ Президента Респ. Беларусь, 28 окт. 2021 г., № 422 // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

57. Кодекс Республики Беларусь об административных правонарушениях : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г : в ред. от 22.04.2024 г.. // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

58. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях: принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г.: в ред. от 22.04.2024 г. // Эталон – Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

59. Трудовой кодекс Республики Беларусь : 26 июля 1999 г., № 296-З : принят Палатой представителей 8 июня 1999 г. : одобрен Советом Респ. 30 июня 1999 г. : в ред. от 08.04.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

60. Уголовный кодекс Республики Беларусь : 9 июля 1999 г., №: 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. от 08.04.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

61. Об обучении по вопросам защиты персональных данных : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 ноября 2021 г., № 194 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

62. О технической и криптографической защите персональных данных : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 ноября 2021 г., № 195 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

63. General Data Protection Regulation : Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016 // EURLex. – Mode of access: https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Date of access: 20.10.2024).

СРЕДСТВА ОБУЧЕНИЯ

1. Система дистанционного обучения «Moodle».
2. Учебная литература.
3. Конспект.
4. Интернет-ресурсы.

СРЕДСТВА ДИАГНОСТИКИ РЕЗУЛЬТАТОВ ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Диагностика результатов образовательной деятельности обучающихся осуществляется в ходе проведения всех видов учебных занятий, управляемой самостоятельной работы и текущей аттестации по учебной дисциплине.

Текущая аттестация обучающихся проводится в течение семестра в целях периодического контроля и оценки результатов их учебной деятельности по учебной дисциплине с выставлением отметок.

Текущий контроль проводится строго в соответствии с учебно-методической картой дисциплины. Обучающийся должен в обязательном порядке участвовать во всех контрольных мероприятиях текущего контроля, предусмотренных учебной программой дисциплины.

Основными **формами контроля** знаний по учебной дисциплине являются:

устный опрос	УО;
решение практических задач	РПЗ;
задание тестового типа (тест)	ЗТТ;
коллоквиум	К;
эссе	Э.

Форма текущей аттестации по учебной дисциплине:

задание тестового типа (тест)	ЗТТ.

К промежуточной аттестации по учебной дисциплине обучающиеся допускаются при условии успешного прохождения текущей аттестации, предусмотренной учебной программой в текущем семестре.

Формой промежуточной аттестации является:

экзамен	экз.

В образовательном процессе используются рекомендованные Министерством образования Республики Беларусь критерии оценок результатов учебной деятельности, основанные на десятибалльной шкале оценки знаний. Итоговая оценка выставляется на основании: Правила проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования, утвержденные постановлением Министерства образования Республики Беларусь от 13.10.2023 г. № 319.

ТЕМЫ СЕМИНАРСКИХ ЗАНЯТИЙ

Целью семинарских занятий является углубление знаний, их систематизация и обобщение на основе изучения разнообразных источников, развития широкого спектра аналитических умений, в том числе конспектирования, рецензирования, подготовки развернутых тематических выступлений, критического сопоставления источников и т. д

Для очной (дневной) формы получения общего высшего образования

Тема 2. Приватность и идентификация личности: международные подходы

Семинарское занятие 1. Приватность и идентификация личности: международные подходы

Вопросы, подлежащие рассмотрению на занятии:

1. Личная жизнь человека в различных исторических периодах.
2. Вмешательство государственных институтов в частную жизнь.
3. Законы об именах. Личная жизнь и анонимность.
4. Появление концепции невмешательства в личную жизни.
5. Приватность как универсальное право человека.
6. Понятие приватности и защиты персональных данных.
7. История информационной приватности. Виды приватности

Тема 5. Правовое регулирование защиты персональных данных в Республике Беларусь

Семинарское занятие 2. Правовое регулирование защиты персональных данных в Республике Беларусь

Вопросы, подлежащие рассмотрению на занятии:

1. История регулирования персональных данных до принятия Закона «О защите персональных данных»: до 01.09.2022 года.
2. Основные нормативные правовые акты в сфере защиты персональных данных: Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных», приказы Оперативно-аналитического центра при Президенте Республики Беларусь, иные акты законодательства.
3. Закон Республики Беларусь «О защите персональных данных»: общая характеристика.
4. Национальный центр защиты персональных данных Республики Беларусь: правовой статус, основные задачи и функции.
5. Приказы директора Национального центра защиты персональных данных Республики Беларусь: общая характеристика, их роль при регулировании защиты персональных данных

Тема 7. Правовые основания для обработки персональных данных в Республике Беларусь

Семинарское занятие 3. Правовые основания для обработки персональных данных в Республике Беларусь

Вопросы, подлежащие рассмотрению на занятии:

1. Согласие субъекта персональных данных и его характеристики. Условия получения согласия субъекта персональных данных на обработку персональных данных.
2. Обработка персональных данных без согласия субъекта персональных данных, в том числе специальных персональных данных.
3. Обработка персональных данных по поручению оператора: общая характеристика, обязательные договорные пункты.
4. Обработка персональных данных в сфере образования и медицины. Особенности обработки персональных данных в рамках трудовых отношений.
5. Трансграничная передача персональных данных.
6. Сравнительный анализ оснований обработки персональных данных по законодательству Республики Беларусь и в соответствии с Генеральным регламентом о защите персональных данных.

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь

Семинарское занятие 4. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь

Вопросы, подлежащие рассмотрению на занятии:

1. Политика оператора (уполномоченного лица) в отношении обработки персональных данных и реестр обработки персональных данных.
2. Локальные акты оператора и другие меры по обеспечению защиты персональных данных.
3. Лицо, ответственное за осуществление внутреннего контроля за защитой персональных данных в организации.

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных

Семинарское занятие 5. Ответственность за нарушения законодательства в сфере персональных данных

Вопросы, подлежащие рассмотрению на занятии:

1. Понятие нарушения законодательства в сфере персональных данных. Характеристика незаконности обработки персональных данных.
2. Административная ответственность за нарушение законодательства о персональных данных.
3. Гражданско-правовая ответственность за нарушение законодательства о персональных данных.
4. Уголовная ответственность за нарушение законодательства о персональных данных.

5. Дисциплинарная ответственность за нарушение порядка обработки персональных данных, установленного законодательством и локальными правовыми актами.

Для заочной / заочной сокращенной формы получения общего высшего образования

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных

Семинарское занятие 1. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь

Вопросы, подлежащие рассмотрению на занятии:

1. Политика оператора (уполномоченного лица) в отношении обработки персональных данных и реестр обработки персональных данных.
2. Локальные акты оператора и другие меры по обеспечению защиты персональных данных.
3. Лицо, ответственное за осуществление внутреннего контроля за защитой персональных данных в организации.
4. Понятие нарушения законодательства в сфере персональных данных. Характеристика незаконности обработки персональных данных.
5. Административная, уголовная и гражданско-правовая ответственность за нарушение законодательства о персональных данных.
6. Дисциплинарная ответственность за нарушение порядка обработки персональных данных, установленного законодательством и локальными правовыми актами.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ УПРАВЛЯЕМОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Управляемая самостоятельная работа студентов служит закреплению знаний, а также способствует овладению практическими материалами с учетом их индивидуальных способностей и наклонностей. Управляемая самостоятельная работа студентов включает: изучение международных договоров, нормативных правовых актов по темам дисциплины с последующим обсуждением на семинарских занятиях и решением ситуационных задач; решение тестовых заданий; проверка контрольной работы.

Управляемая самостоятельная работа по изучению учебной дисциплины является объективно необходимым компонентом комплексного метода подготовки и обучения в образовательном процессе, в равной степени важным и логически связанным с иными элементами и формами. Управляемая самостоятельная работа предполагает автономное, дистанционное освоение поставленных целей и задач в пределах учебного материала. Данная форма подготовки должна носить логически последовательный, системный,

комплексный характер и предполагает использование всех доступных рекомендуемых форм и методов подготовки.

Важным этапом формирования первичных навыков управляемой самостоятельной работы является ознакомление с содержанием учебной программы, темами и информационно-методической частью. Непременным условием усвоения содержания учебной дисциплины является углубленное изучение рекомендуемой учебной и специальной литературы.

Управляемая самостоятельная работа предусмотрена учебным планом для развития способностей обучающихся к самостоятельной научной исследовательской деятельности. Такая форма приобретения обучающимися знаний, навыков, умений служит: углубленному изучению определенной темы, ее отдельных вопросов, теоретико-правовых проблем и, тем самым, росту знаний студента; формированию умений использования литературных источников; поиска, отбора и изучения информации; критического обзора литературы, осуществлению полного и последовательного анализа источников; овладению отдельными методами и методологией научного исследования, анализом нормативных правовых актов, относящихся к используемым источникам; выработке навыков изложения изученного материала; формированию собственной позиции студента по правовым вопросам и возможности ее выражения, в том числе изложения собственных теоретических и экспериментальных результатов, оценка достоверности полученных данных.

При подготовке управляемой самостоятельной работы студентами рекомендуется проводить самостоятельный подбор соответствующих нормативных правовых актов, учебной и специальной литературы по темам дисциплины.

ПЕРЕЧЕНЬ ЗАДАНИЙ И КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ УСР

№ темы	Тема УСР	Кол-во часов	Метод. обеспечение	Форма контроля
4 семестр (4 часа)				
4.	Средства правовой защиты персональных данных и практика исполнения генерального регламента	2	Интернет-ресурсы, библиотека университета	РПЗ, ЗТТ
6.	Основные понятия в области защиты персональных данных в Республике Беларусь	2	Интернет-ресурсы, библиотека университета	РПЗ, ЗТТ, Э

ПРИМЕРНЫЕ ЗАДАНИЯ УСР

Тема 4. Средства правовой защиты персональных данных и практика исполнения генерального регламента

4. *Подготовить презентацию по вопросу*: Стандартные договорные оговорки. Бизнес-процессы юридических лиц. «Best practices». Представители на территории Европейского Союза.

5. *Подготовить сравнительную таблицу по вопросу:* Виды нарушений Генерального регламента о защите персональных данных. Действия субъектов правоотношений в случаях нарушений в сфере защиты персональных данных.

6. *Охарактеризовать*: Меры ответственности за несанкционированную обработку персональных данных.

7. *Подготовить письменный доклад по вопросам*: Порядок и условия наложения административного штрафа. Возмещение ущерба контролером в пользу субъекта персональных данных. Уголовная ответственность за нарушение правил обработки персональных данных в государствах-членах Европейского Союза

Тема 6. Основные понятия в области защиты персональных данных в Республике Беларусь

Вопросы, подлежащие изучению:

1. Научные подходы к понятию «персональные данные». Нормативное понятие и признаки персональных данных в Республики Беларусь. Соотношение понятий «персональные данные» и «банковская тайна», «врачебная тайна», «нотариальная тайна».

2. Категории персональных данных. Общедоступные персональные данные. Специальные персональные данные. Биометрические и генетические персональные данные.

3. Субъекты правоотношения в сфере защиты персональных данных: субъект персональных данных, оператор и уполномоченное лицо. Их функции, права и обязанности в рассматриваемом правоотношении.

4. Понятие обработки персональных данных, их виды и формы. Общие требования к обработке персональных данных: законность, соразмерность и справедливость, наличие правового основания, ограничение цели, запрет избыточности, прозрачность, ограничение хранения, достоверность.

5. Особенности обработки персональных данных при их обезличивании, блокировании и удалении. Предоставление и распространение персональных данных.

Задание: составить тестовое задание, состоящее из 35 вопросов (5 вариантов ответа)

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЭКЗАМЕН)

1. История развития правового регулирования защиты персональных данных в Европейском союзе. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г.
2. Общая характеристика законодательства о защите персональных данных государств – членов ЕАЭС.
3. Понятие приватности и защиты персональных данных. История информационной приватности. Виды приватности.
4. История создания и общая характеристика Генерального регламента о защите персональных данных 2016г.
5. Ключевые термины и определения в Генеральном регламенте о защите персональных данных 2016 г. Основные принципы обработки персональных данных в Европейском Союзе.
6. Субъекты правоотношения в сфере защиты персональных данных в Европейском Союзе: «Data controller», «Data processor», «Data subject».
7. Основания обработки персональных данных и их характеристика по Генеральному регламенту о защите персональных данных 2016 г.
8. Основания и условия привлечения к ответственности по Генеральному регламенту о защите персональных данных 2016 г.
9. Правовое регулирование защиты персональных данных в Республике Беларусь.
10. Общая характеристика Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
11. Национальный центр защиты персональных данных Республики Беларусь: правовой статус, основные задачи и функции.
12. Юридическая сила и общая характеристика приказов директора Национального центра защиты персональных данных Республики Беларусь.
13. Понятие и категории персональных данных по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
14. Общая характеристика специальных персональных данных.
15. Особенности защиты биометрических и генетических персональных данных.
16. Субъекты правоотношения в сфере защиты персональных данных в Республике Беларусь: субъект персональных данных, оператор и уполномоченное лицо.
17. Права и обязанности оператора при обработке персональных данных.
18. Права и обязанности уполномоченного лица при обработке персональных данных.
19. Понятие, виды и формы обработки персональных данных в Республике Беларусь.
20. Правовые основания обработки персональных данных по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

21. Общая характеристика согласия субъекта персональных данных на обработку персональных данных в Республике Беларусь.

22. Условия получения согласия субъекта персональных данных на обработку персональных данных.

23. Основания обработки персональных данных без согласия субъекта персональных данных (специальных персональных данных) в Республике Беларусь.

24. Общая характеристика обработки персональных данных по поручению оператора в Республике Беларусь. Обязательные договорные пункты.

25. Особенности обработки персональных данных в рамках трудовых отношений в Республике Беларусь.

26. Общая характеристика трансграничной передачи персональных данных. Порядок документального оформления.

27. Права субъектов персональных данных в Республике Беларусь. Характеристика права на отзыв согласия субъекта персональных данных, права на получение информации, касающейся обработки персональных данных, и изменение персональных данных, а также права на получение информации о предоставлении персональных данных третьим лицам.

28. Права субъектов персональных данных в Республике Беларусь. Характеристика права на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных, а также права на возмещение морального вреда, причиненного незаконной обработкой персональных данных. Порядок реализации прав субъекта персональных данных.

29. Правовые, организационные и технические меры по обеспечению защиты персональных данных в Республике Беларусь.

30. Документационное оформление обработки персональных данных оператором по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

31. Функции, права и обязанности лица, ответственного за осуществление внутреннего контроля за защитой персональных данных в организации, в Республике Беларусь.

32. Порядок и условия привлечения к административной ответственности за незаконную обработку персональных данных в Республике Беларусь.

33. Порядок и условия привлечения к уголовной ответственности за незаконную обработку персональных данных в Республике Беларусь.

34. Основания и условия привлечения к гражданско-правовой ответственности за нарушение законодательства о персональных данных в Республике Беларусь.

35. Порядок и условия наложения дисциплинарного взыскания за нарушение порядка обработки персональных данных, установленного законодательством и локальными правовыми актами.

V. ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Конституционное право Республики Беларусь	Кафедра международного права	Предложений нет	протокол заседания кафедры международного права № 9 от 16.12.2024
Конституционное право зарубежных стран	Кафедра международного права	Предложений нет	протокол заседания кафедры международного права № 9 от 16.12.2024
Право прав человека	Кафедра международного права	Предложений нет	протокол заседания кафедры международного права № 9 от 16.12.2024
Европейское право	Кафедра международного права	Предложений нет	протокол заседания кафедры международного права № 9 от 16.12.2024
Составление юридических документов	Кафедра международного права	Предложений нет	протокол заседания кафедры международного права № 9 от 16.12.2024

1. ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

КОНСПЕКТ ЛЕКЦИЙ

ЛЕКЦИЯ 1. ИСТОЧНИКИ ПРАВА, РЕГЛАМЕНТИРУЮЩИЕ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Защита персональных данных как общегуманитарная концепция начинается в период Великой Французской революции. Она впервые провозгласила это понятие, выделяющее отдельную личность и обозначающее приоритет ее интересов над интересами ничем не ограниченного государства. В дальнейшем сформировалось понимание права на неприкосновенность частной жизни, одной из составляющих которого стало и право на защиту персональной информации.

В первой половине XX века сформулированное право на частную жизнь находит отражение в американской судебной практике. Эта идея достаточно быстро распространяется за пределами США.

В 1948 году право на частную жизнь отражается вместе с другими фундаментальными правами и свободами в ст. 12 Всеобщей декларации прав человека. В ней указано, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. В 1950 году появляется ст. 8 Европейской Конвенции по правам человека, которая отчасти продублировала положение Всеобщей декларации прав человека, расширив ее некоторые пункты. Так, каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.

Повышенное внимание к правам человека на тот момент времени объяснялось разрушительными последствиями Второй мировой войны. Главным приоритетом того времени были более значимые социальные вопросы послевоенного периода: неприкосновенность личной и семейной жизни, тайна переписки. Проблема защиты персональных данных была связана с тенденцией защиты частной жизни, но не являлась основной.

В начале второй половины XX века начинают развиваться информационные технологии, позволяющие значительно быстрее обрабатывать гораздо большее количество информации. В 60-ые годы эти технологии становятся все более доступными широкому кругу лиц, что вызывает определенное беспокойство у Совета Европы.

В 1968 году Парламентская ассамблея публикует рекомендацию №509 о правах человека и современных научно-технических достижениях. В ней содержалась просьба изучить и представить доклад на тему обеспечения национального законодательства государств-членов с учетом ст. 8 Европейской Конвенции по правам человека, адекватную защиту права на

неприкосновенность частной жизни от нарушений, которые могут быть совершены при использовании современных научных и технических методов.

С 22 апреля по 13 мая 1968 года проходит Первая международная конференция по правам человека для рассмотрения прогресса с момента принятия Всеобщей декларации прав человека.

12 мая 1968 года на этой конференции принимается резолюцию под названием «Права человека и научно-технический прогресс». 19 декабря 1968 года Генеральная Ассамблея ООН принимает резолюцию «Права человека и научно-технический прогресс». В ней было предложено изучить проблемы, возникающие в области прав человека в связи с научно-техническим прогрессом. В частности, особый акцент делался на уважении частной жизни человека и неприкосновенности и суверенитета наций в условиях прогресса техники звукозаписи и других средств, защите человеческой личности и физической и интеллектуальной неприкосновенности человека в условиях прогресса биологии, медицины и биохимии, применении электроники, которое может затронуть права человеческой личности, а также допустимые пределы такого применения электроники в демократическом обществе. В истории этот момент считается отправной точкой для защиты персональных данных.

Первой европейской страной, в которой было уделено внимание защите персональных данных, стала Федеративная Республика Германия (ФРГ), где на земле Гессен в 1970 году принимается первый в истории закон о персональных данных. Важно отметить, что это был лишь локальный закон, который применялся исключительно на территории этой земли, а не на федеральном уровне.

В 1974 году принимается Закон «О защите персональных данных» (Privacy Act) в США, в котором американский конгресс впервые устанавливает связь между правом на частную жизнь и персональными данными. Данный закон указывает, что личная жизнь человека может быть напрямую затронута в результате сбора, использования и распространения персональной информации государственными органами власти.

Однако ни один из актов нельзя назвать полноценным законом, регулирующим обработку персональных данных. Тем не менее, право на защиту персональных данных начинает выделяться отдельно от права на частную жизнь.

Первый национальный закон «О защите персональных данных» (Bundesdatenschutzgesetz) принимается в ФРГ в 1977 году. Особое отношение немецкой общественности к этому вопросу связано, в первую очередь, с локальными историческими событиями. В середине XX века немцы пережили два противоречивых политических режима: с одной стороны, Третий Рейх, с другой стороны, разделение Германии на ФРГ и ГДР. Указанные строи были основаны, в том числе и на массовой слежке за населением. Такие потрясения привели к тому, что впоследствии требование о конфиденциальности оказалось чрезвычайно востребованным. Именно по этой причине ФРГ до сих пор считается одним из мировых лидеров по защите частной жизни и персональных данных.

Другой значимой страной для защиты персональных данных является Франция, которая отстала от ФРГ всего на один год. Принятие в 1978 году закона было связано с локальными событиями. В начале 70-ых годов французское правительство разработало проект SAFARI, смысл которого заключался в создании единого реестра данных с использованием номера социального страхования, что позволяло бы идентифицировать любого гражданина. Обработку всей этой информации планировалось осуществлять благодаря передовым на тот момент времени вычислительным технологиям. В 1974 году газета «Le Monde» публикует об этом статью под названием «САФАРИ или охота на французов» («SAFARI ou la chasse aux Français»), чем провоцирует громкий скандал на тему массовой слежки. Под давлением общественности правительство вынуждено было отступить, что привело к принятию закона и созданию специальной комиссии. Несмотря на создание реестра, новая комиссия смогла установить определенные ограничения по обработке персональных данных.

Немецкий и французский законы становятся краеугольным камнем для персональных данных и придают значительный импульс для развития этой сферы. На проблему начинают обращать внимание все больше и больше стран и международных организаций.

В 1980 году Организация экономического сотрудничества и развития (ОЭСР) публикует Гайдлайны по защите персональных данных с учетом продолжающегося развития компьютерных технологий и их использования для коммерческих транзакций.

Через год в 1981 году принимается первый международный договор в сфере защиты персональных данных – Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981). Она считается первым обязывающим международным инструментом, защищающим физических лиц от злоупотреблений, которые могут иметь место при сборе и обработке данных, и ставящий в то же время задачу регулировать трансграничный поток персональных данных. Конвенция применяется к автоматизированным базам персональных данных и к автоматической обработке персональных данных в публичном и частном секторах.

В Конвенции установлены требования к автоматической обработке персональных данных:

1. должны быть получены и обработаны добросовестным и законным образом;
2. должны накапливаться для точно определенных и законных целей и не использоваться в противоречии с этими целями;
3. должны быть адекватными, относящимися к делу и не быть избыточными применительно к целям, для которых они накапливаются;
4. должны быть точными и в случае необходимости обновляться;
5. должны храниться в такой форме, которая позволяет идентифицировать субъектов данных не дольше, чем этого требует цель, для которой эти данные накапливаются.

Конвенция дает гарантии применительно к сбору и обработке персональных данных, запрещает, если национальное право не обеспечивает надлежащих гарантий, обработку «чувствительных» данных относительно расовой принадлежности лица, его политических взглядов, здоровья, религии, сексуальной жизни, уголовного прошлого и т.п. В Конвенции предусмотрено право лица знать, что данные о нем собраны (наличие автоматизированной базы персональных данных, ее главных целях, о контролере базы данных, месте жительства либо юридическом адресе), направлять запросы об этом, требовать уточнения или уничтожения таких данных, прибегнуть к судебной защите нарушенного права. Уже в 1981 в Конвенции установлен порядок трансграничной передачи персональных данных. По общему правилу, трансграничная передача разрешена, то есть в Конвенции указано, что нельзя запрещать или ставить под специальный контроль информационные потоки персональных данных, идущие на территорию государства, исходя исключительно из соображений защиты неприкосновенности личной сферы. Однако если в законодательстве государства установлены специальные правила в отношении определенных категорий персональных данных или автоматизированных баз персональных данных, то трансграничная передача запрещена, если в другом государстве не предусмотрена равноценная защита. Еще одним основанием для ограничения трансграничной передачи является передача на территорию Государства, не являющегося Стороной Конвенции, через территорию другой Стороны с целью скрыть первоначальное государство-получатель.

На сегодняшний день к ней присоединилась 55 государств. Беларусь, Казахстан, Кыргызстан, Узбекистан не присоединились к Конвенции, Россия и Армения присоединились в 2013 и 2012 году соответственно.

Постепенно ускоряется развитие информационных технологий, что создает новые проблемы в сфере приватности данных и частной жизни. Главной проблемой становится появление Интернета и его быстрое развитие. Первым потенциальную угрозу замечает Европейский союз (ЕС). 24 октября 1995 года принимается Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных. В качестве причины принятия были названы, в том числе, существенный рост потока персональных данных через границы ввиду экономической и социальной интеграции, различные степени защиты прав и свобод граждан, в особенности права на частную жизнь, применительно к обработке персональных данных в государствах-членах, необходимость создания эквивалентной степени защиты прав и свобод частных лиц применительно к обработке их данных.

Эта директива закрепляет две старейшие амбиции европейского интеграционного проекта: достижение внутреннего рынка (свободное перемещение личной информации) и защиту основных прав и свобод личности. Утверждается, что обе цели одинаково важны. Статус такой директивы заключается в том, что она обязывает государства-члены к достижению целей,

оставляя при этом национальным властям право выбора формы и средств для реализации этих целей. Директива применяется к государственному и частному сектору.

В качестве предмета регулирования была названа защита фундаментальных прав и свобод физических лиц, и, в частности, право на неприкосновенность частной жизни применительно к обработке персональных данных. Под «персональными данными» понималась любая информация, связанная с идентифицированным или идентифицируемым физическим лицом («субъектом данных»). Под идентифицируемым лицом понимается лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один или несколько факторов, специфичных для его физической, психологической, ментальной, экономической, культурной или социальной идентичности.

В качестве субъектов выступали контролер (самостоятельно или совместно с другими определяет цели и средства обработки персональных данных), обработчик (обрабатывает персональные данные по поручению контролера) и третья сторона (уполномочены обрабатывать данные с прямой санкции контролера или обработчика).

Директива применялась к обработке персональных данных, полностью или частично автоматическими средствами, и обработке средствами, отличными от автоматических, персональных данных, составляющих часть картотеки или предназначенных составлять часть картотеки. Директива не применялась к обработке персональных данных физическим лицом в ходе личной или бытовой деятельности.

В качестве оснований обработки персональных данных было указано следующее:

(a) субъект данных недвусмысленно дал свое согласие; или

(b) обработка необходима для исполнения контракта, в котором субъект данных является стороной или для принятия мер до заключения контракта по просьбе субъекта данных; или

(c) обработка необходима для выполнения юридического обязательства, субъектом которого является контролер; или

(d) обработка необходима для защиты жизненных интересов субъекта данных; или

(e) обработка необходима в целях обеспечения законных интересов контролера или третьей стороны (сторон), которым раскрыты данные, кроме случаев, когда такие интересы перекрываются интересами фундаментальных прав и свобод субъекта данных, защита которых требуется согласно Статье 1(1).

В Директиве особое внимание было уделено обработке особых персональных данных. В ней был указан запрет на обработку персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, вероисповедание или философское воззрение, членство в профессиональном союзе, а также обработку данных, касающихся здоровья или интимной жизни. В качестве исключений было, например, явное согласие, в

целях исполнения обязательств и особых прав контролера в сфере законодательства о труде, для защиты жизненных интересов субъекта данных или иного лица, если субъект данных физически или юридически неспособен дать свое согласие, в целях превентивной медицины, медицинского диагноза, предоставления медицинского обслуживания, лечения или управления услугами здравоохранения.

В качестве меры защиты было обязанность обеспечить, чтобы контролер реализовал надлежащие технические и организационные меры для защиты персональных данных от случайного или незаконного уничтожения или случайной утраты, изменения, неправомерного раскрытия или доступа, в частности, когда обработка влечет передачу данных по сети, а также от всех иных незаконных форм обработки.

К концу 90-ых годов начинают формироваться основные гиганты-монополисты Интернета. Сегодня их принято называть большой пятеркой или GAFAM (Google, Amazon, Facebook, Apple, Microsoft). При непосредственном участии перечисленных корпораций зарождается новая система монетизации коммерческой деятельности в Интернете. Поисковики Google и Facebook, не имея прямых источников капитализации (в отличие от Amazon и Microsoft), начинают показывать рекламу, основываясь на анализе поведения своих пользователей. Так появляется таркетинг. Контекстная реклама быстро становится чрезвычайно востребованной и к этой системе подключаются Amazon, Microsoft и Apple.

Чтобы реклама оставалась наиболее релевантной, пять названных компаний активно собирают огромные объемы данных о пользователях со всего мира. При этом быстро развиваются технологии, позволяющие анализировать всю информацию и выявлять особенности поведения пользователей. Аналитические выводы отправляются в США, которые не придавали большого значения защите персональных данных.

В ответ на контекстную рекламу, ЕС принимает Директиву 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. об обработке персональных данных и защите конфиденциальности в секторе электронных коммуникаций» (Директива о конфиденциальности и электронных коммуникациях) (Директора ePrivacy). Директива была принята в развитие Директивы 95/46/ЕС.

В качестве предмета названа обработка персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи общего пользования в ЕС. В целях маркетинга услуг электронной связи или предоставления услуг с добавленной стоимостью поставщик общедоступной услуги электронной связи может обрабатывать данные, в объеме и в течение периода, необходимого для таких услуг или маркетинга, если абонент или пользователь, к которому относятся данные, дал свое согласие. Пользователям или абонентам должна быть предоставлена возможность отозвать свое согласие на обработку данных трафика в любое время. Поставщик услуг должен

информировать абонента или пользователя о типах данных трафика, которые обрабатываются, и о продолжительности такой обработки.

В рамках реформирования системы управления ЕС принятый в 2009 г. Лиссабонский договор официально закрепил право на защиту данных в качестве фундаментального права, разграничив его с правом на неприкосновенность частной жизни.

Следом за принятием этой Директивы появляются утечки и разоблачения, связанные с кибербезопасностью. Здесь можно говорить и о WikiLeaks Джулиана Ассанжа, разоблачении Эдварда Сноудена американской программы массовой слежки PRISM. Пик приходится на 2010 год. Ярким примером является утечка персональных данных 37 миллионов человек – пользователей Ashley Madison, канадского сайта знакомств, предназначенного для людей, состоящих в браке. В 2015 году базы данных сайта подверглись хакерской атаке, и вся приватная информация была выложена в Интернет. В результате значительная волна разводов по всему миру, несколько случаев суицида. К тому же в свободном доступе оказались данные около 1,200 пользователей из Саудовской Аравии, где наказание за измену доходит вплоть до смертной казни. В таких обстоятельствах, трудно недооценивать значение защиты персональных данных.

В результате этих событий, Европейский Союз приходит к выводу о необходимости обновления Директивы 1995. Основная проблема заключалась в том, что она не применялась напрямую в странах членах ЕС, что в свою очередь привело к значительным различиям на уровне национальных законодательств. Новый же регламент действовал бы напрямую в каждой европейской стране и позволил бы создать повышенный уровень защиты персональных данных по всему Союзу. Дискуссии в целях принятия нового закона начались в 2012 году, а в 2016 году окончательный текст регламента был официально опубликован и 25 мая 2018 года вступил в силу. Акт получил название Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (Общий Регламент о защите персональных данных, GDPR).

Цели GDPR:

– защитить права граждан Европейского союза;

– автоматизировать обработку персональных данных в целях безопасности и сохранения конфиденциальности пользователей;

– установить единые международные стандарты и средства для обработки персональных данных в ЕС;

– наладить сотрудничество между органами надзора в вопросах защиты и контроля персональных данных;

– стимулировать рост цифровой экономики.

GDPR не применяется в отношении обработки персональных данных физическими лицами в ходе осуществления исключительно личной или бытовой деятельности, не связанной с профессиональной или коммерческой деятельностью. Личная или бытовая деятельность может включать в себя

переписку и сохранение адресов или взаимодействие через социальные сети и сетевую активность, осуществляемые в контексте такой деятельности.

GDPR применяется в отношении обработки персональных данных полностью либо частично при помощи автоматизированных средств, а также в отношении обработки персональных данных иными способами, которые являются частью файловой системы или которые имеют целью стать частью файловой системы.

Общий Регламент о защите персональных данных применяется в отношении обработки персональных данных в контексте деятельности учреждения контролера или обрабатывающего данные лица в Союзе, вне зависимости от того, проводится обработка в Союзе или нет.

GDPR применяется в отношении обработки персональных данных субъектов данных, находящихся в Союзе, контролером или обрабатывающим данные лицом, не учрежденными в Союзе, если обработка данных касается:

(a) предоставления товаров и услуг субъектам данных в Союзе вне зависимости от того, требуется ли оплата от указанного субъекта данных, или

(b) мониторинга их деятельности при условии, что деятельность осуществляется на территории Союза.

Регламент не применяется в отношении персональных данных умерших лиц.

В GDPR установлены термины, связанные с категориями персональных данных.

«Генетические данные» – персональные данные, касающиеся унаследованных или приобретенных генетических характеристик физического лица, которые предоставляют уникальную информацию о физиологии или здоровье указанного физического лица и которые являются результатом, в частности, анализа биологического образца соответствующего физического лица.

«Биометрические данные» – персональные данные, возникающие в результате особой технической обработки, касающиеся физических, физиологических или поведенческих характеристик физического лица, которые предусматривают или подтверждают уникальную идентификацию указанного физического лица, например, изображение лица человека или дактилоскопические данные.

GDPR предусматривает четкое и прозрачное разграничение каждого из субъектов персональных данных: контролер, обработчик, субъект данных:

– контролер (controller) – физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных;

– обработчик (processor) – это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени по поручению контролера;

– субъект данных (data subject) – физическое лицо, данные которого обрабатываются.

Несмотря на то, что в Беларуси установлено специальное законодательство в области защиты персональных данных, в некоторых ситуациях у белорусских организаций появляется обязанность по соблюдению GDPR. Например, организация предлагают товары и услуги через веб-ресурсы, то есть имеют свой сайт, онлайн-сервис или мобильное приложение с регистрацией на языке хотя бы одной из стран ЕС, используется Google Analytics, Яндекс Метрика, cookie-файлы и мониторинг IP-адресов и другие технологии онлайн-трекинга для того, чтобы идентифицировать пользователей и анализировать их поведение, использует инструменты интернет-рекламы для продвижения своих продуктов или проектов в ЕС.

Общий Регламент о защите персональных данных предоставляет субъектам персональных данных следующие права:

- право на доступ к своим данным
- право на исправление своих данных
- право на удаление своих данных
- право на ограничение возможностей обработки их данных
- право на переносимость данных
- право на возражение

После принятия GDPR в ЕС принимается Директива № 2016/680 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования преступлений или исполнения уголовных наказаний, о свободном обращении таких данных, а также об отмене Рамочного Решения 2008/977/ПВД Совета ЕС». Это обусловлено тем, что обработка персональных данных в целях уголовного правосудия не входит в предмет действия GDPR.

Директива устанавливает правила в отношении защиты физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления или уголовного преследования преступлений или исполнения уголовных наказаний, включая защиту от угроз общественной безопасности и предотвращение таких угроз.

Государства-члены ЕС должны предусмотреть, что обработка является законной, только если и поскольку такая обработка необходима для выполнения задач, осуществляемых компетентными органами в целях, изложенных в Статье 1(1) Директивы, и основана на законодательстве Европейского Союза или государства-члена ЕС.

Обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные убеждения или философские воззрения, членство в профессиональном союзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных касающихся здоровья, половой жизни или сексуальной ориентации физического лица, разрешается только, если это строго

необходимо, с учетом надлежащих гарантий для прав и свобод субъекта данных, и только в следующих случаях:

(a) если это разрешено законодательством Европейского Союза или государства-члена ЕС;

(b) если это необходимо для защиты жизненных интересов субъекта данных или другого физического лица; или

(c) если такая обработка относится к персональным данным, которые субъект данных явно сделал общедоступными.

В том же году принимается директива NIS (Network and Information Security). Основной задачей этого правового акта становится обеспечение высокого уровня информационной безопасности для операторов критических инфраструктур и провайдеров цифровых услуг. Речь идет о защите не только персональных данных, но о безопасности любых данных.

Таким образом, акты ЕС являются результатом политики Европейского Союза в сфере электронных коммуникаций, кибербезопасности и приватности данных.

В Российской Федерации (РФ) концепция права на неприкосновенность частной жизни и тайну переписки имеет давнюю историю. Второго Почтовый устав, принятый в 1857 году и вступивший в силу 1876 году, Телеграфный устав провозглашали тайну корреспонденции. Она защищалась на уровне уголовного законодательства, за нарушение конфиденциальности отправляемых сообщений наказание предусматривалось в Уголовном уложении. Интересно, что к ответственности на основании Уложения 1903 года могли быть привлечены даже должностные лица, если при выполнении ими обязанностей, связанных с отправлением правосудия, они вмешивались в личную жизнь подданных Российской империи.

Но эта концепция правового регулирования неприкосновенности частной жизни исчерпала себя после революции 1917 года, отменившей все ранее принятые законы, в том числе имеющие отношение к защите персональных данных граждан и тайны их частной жизни и переписки. Конституция 1918 года содержала раздел о правах человека, но на тот военный и революционный период можно говорить о его декларативном характере. Документ не воспринял большинство достижений европейской демократии в части прав человека, провозгласив только право на защиту от эксплуататоров; на участие в управлении; на свободное землепользование.

Принцип военного коммунизма исключал любой индивидуализм. Конституция СССР 1924 года не урегулировала защиту частной жизни человека. Защита персональных данных, сведений о частной жизни, права на переписку на тот момент не могла стать каким-то основанием для отступления от идеологии коммунизма. Но история не стоит на месте, и вскоре этому аспекту человеческих интересов было уделено внимание. В Конституции СССР 1936 года уже появился раздел, полностью посвященный правам и свободам гражданина. В ней появились неприкосновенность личности, неприкосновенность жилища и тайна переписки (ст. 127-128).

В части развития теоретической концепции принятие Конституции в таком виде стало серьезным достижением российской правовой науки, однако на практике – это была формальность. Право на тайну телефонных переговоров было полностью исключено принятием одного из приказов НКВД, обязывающего стенографировать все без исключения телефонные разговоры сотрудников посольств и международных организаций. Кроме того, была введена обязательная цензура всей переписки, если адресат находился в другой стране. В годы Великой Отечественной войны проблема защиты частной жизни и тайны корреспонденции не имела значения.

1950-60-е годы в СССР стали периодом оттепели. После того, как был ратифицирован Пакт о гражданских и политических правах 1966 года, с учетом его положений была разработана новая Конституция 1966 года, уже в полной мере отразившая складывающуюся практику защиты информационных прав, в том числе и права на защиту персональных данных. Уважение личности было провозглашено в качестве важной обязанности, возлагаемой на государственные органы и должностные лица. Гражданам было предоставлено право на неприкосновенность личности; жилища; тайны переписки, телефонных переговоров и телеграфных сообщений.

Неприкосновенность частной жизни как самостоятельная ценность, включающая в себя и право на защиту персональных данных, впервые вошла в российское законодательство в 1991 году. В 1995 году был разработан и принят Закон «Об информатизации и информации», который отнес персональные данные к охраняемой законом конфиденциальной информации.

В 1999 году на уровне Ассамблеи стран СНГ был принят модельный закон о защите персональных данных, который должен был стать основой национального законодательства.

В Казахстане персональные данные регулируются Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». Под «персональными данными» понимаются сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе. Обработка персональных данных – это действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных.

Персональные данные по доступности подразделяются на общедоступные и ограниченного доступа. Общедоступными персональными данными являются персональные данные или сведения, на которые в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта.

Сведения о субъекте, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, исключаются из общедоступных источников персональных данных в течение одного рабочего

дня по требованию субъекта или его законного представителя либо по решению суда или иных уполномоченных государственных органов.

С 1 июля 2024 года оператор персональных данных обязан в течение одного рабочего дня с момента обнаружения нарушения безопасности персональных данных уведомить уполномоченный орган о таком нарушении с указанием контактных данных лица, ответственного за организацию обработки персональных данных (при наличии).

Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» устанавливает следующие обязанности для операторов данных, то есть юридических лиц и индивидуальных предпринимателей, которые каким-либо образом собирают и обрабатывают персональные данные:

утверждать перечень персональных данных, который необходим для бизнес-процессов;

утверждать документы, определяющие политику в отношении сбора, обработки и защиты персональных данных;

принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для защиты персональных данных;

предоставлять по запросу уполномоченного органа в рамках рассмотрения обращений физических и юридических лиц информацию о способах и процедурах, используемых для обеспечения соблюдения требований закона;

принимать меры по уничтожению персональных данных в случае достижения цели их сбора и обработки;

представлять доказательство о получении согласия субъекта на сбор и обработку его персональных данных в случаях, предусмотренных законодательством Республики Казахстан;

по обращению субъекта сообщать информацию, относящуюся к нему, в законные сроки; а в случае отказа в предоставлении информации предоставить мотивированный ответ.

другие обязанности, установленные ст. 25 Закона.

Нарушение законодательства в сфере персональных данных влечет административную ответственность (ст. 79 КоАП РК) и уголовную ответственность (ст. 147 УК РК).

ЛЕКЦИЯ 2. ПРИВАТНОСТЬ И ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ: МЕЖДУНАРОДНЫЕ ПОДХОДЫ

В русском языке понятие «приватность» идентично выражению «неприкосновенность частной и личной жизни». То есть, частная и личная жизнь – это и есть приватность.

По одной из дефиниций, приватность (англ. privacy) – это центральный регуляторный процесс, посредством которого персона или группа делает себя более или менее открытой и доступной для других, селективный контроль доступности человеческого «Я», синтез стремления быть в контакте и вне контакта с другими; это процесс установления межличностных границ, который, подобно клеточной мембране, открывает или закрывает субъекта для общения.

Примером приватности в литературе является роман Джорджа Оруэлла «1984», в котором было представлено антиутопическое видение мира, в котором больше не существует приватности, а постоянное наблюдение лишает человека всякого чувства личной автономии.

Многие авторы рассматривали приватность с точки зрения качества контактов. А. Бейтс считал, что это чувство персоны, что другие могут быть отстранены от чего-то, что касается только его, и признают это право. Ф.С. Чапин понимал приватность как уровень способности быть самим собой и избегать давления со стороны других, А. Кира – как избегание общения и внедрения посредством визуальных, аудиальных и других каналов и их сочетаний.

Другие исследователи базой приватности считали контроль открытости-закрытости. Так, А.Ф. Уэстин полагал, что это право индивида решать, какая информация и при каких условиях может быть передана другим людям, А. Рапапорт – это способность индивидуума контролировать взаимодействие и располагать средствами предотвращения нежелательных контактов и достижения желательного взаимодействия.

А. Зиммель считал сущностью приватности контроль над стимулами, поступающими от других, и способность быть сепаратным от других, Е. Шилс – контроль над движением информации сквозь границы между отдельными людьми, а также между человеком и группой или между группами, Х.М. Прошанский – максимизацию свободы выбора поведения и контроля за своей активностью. Таким образом, основой приватности оказываются либо категории, описывающие социальную динамику, либо качества контроля, свободы и ответственности, то есть субъектные свойства личности.

Приватность как проявление свободного выбора всегда характеризуется двумя пунктами: это желаемая как состояние идеального уровня взаимодействия и достигнутая как актуальный уровень контактов.

Люди всегда нуждались в уединении. Проблема уединения прослеживалась в трудах Сократа и других греческих философов, когда проводится различие между «внешним» и «внутренним», между публичным и частным, между обществом и одиночеством. Различие между общественным и

частным имеет корни в древнегреческой философии. Аристотель, например, рассматривал общественное как пространство свободы и постоянства, где люди могли дистанцироваться от забот частной жизни. Римляне рассматривали общественную сферу как место, где человеческий потенциал мог по-настоящему расцвести. Частная жизнь иногда рассматривалась как антисоциальное поведение. Всегда существовал своего рода конфликт между «субъективным желанием уединения и изоляции и объективной потребностью зависеть от других».

Со временем концепция приватности превратилась из второстепенной по отношению к общественной жизни в жизненно важный аспект индивидуальности. Руссо рассматривал приватность как отступление от социального давления, как в семье, так и в обществе в целом. Ханна Арендт утверждала, что приватность необходима для личной идентичности и осуществления политических прав, хотя именно через взаимодействие с другими мы получаем ощущение нашей собственной реальности и общего мира вокруг нас.

Особое понятие «приватности» появилось в США. Из-за расстояния между усадьбами физическая приватность стала характеристикой повседневной жизни, а сам дом стал основным местом приватности.

Потребность в приватности никогда не может быть абсолютной и должна быть сбалансирована с другими потребностями, например, с необходимостью борьбы с терроризмом, преступностью и мошенничеством.

В самом общем виде частная жизнь связана с самыми интимными аспектами бытия человека. На протяжении всей истории частная жизнь связана с домом, семейной жизнью и перепиской. С XIV по XVIII век люди обращались в суд за подслушивание или вскрытие и чтение личных писем. С конца XIX века акцент сместился в сторону личной информации с тем же намерением контролировать собственную информацию.

Первые дела, переданные в суд, были связаны с вторжениями в дом, в частности, с подслушиванием. Центр информации об электронной конфиденциальности (EPIC) отмечал, что в 1361 году Закон о мировых судьях в Англии предусматривал арест подглядывающие и подслушивающие. В 1765 году британский лорд Кэмден, отменяя ордер на проникновение в дом и изъятие бумаг, написал: «Мы можем с уверенностью сказать, что в этой стране нет закона, оправдывающего обвиняемых в том, что они сделали; если бы он был, это разрушило бы все удобства общества, поскольку бумаги часто являются самой дорогой собственностью, которую может иметь любой человек». Закон о нарушении права собственности и конституционная защита от необоснованного обыска и изъятия в Соединенных Штатах, сформулированные в Четвертой поправке, были истолкованы как защита от официальных и неофициальных вторжений.

Четвертая поправка сосредоточена на запрете необоснованного обыска и изъятия. Она обусловлена двумя проблемами: чтобы собственность граждан была защищена от изъятия правительством и чтобы дома и личность человека

были защищены от несанкционированных и произвольных обысков. Эта поправка является часто используемой, но все еще неясной концепцией «разумного ожидания конфиденциальности». Четырнадцатая поправка гарантирует надлежащую правовую процедуру и неразглашение личной информации. Поскольку эта формулировка больше соответствует информационному измерению компьютерного века, то ученые рассматривают ее в связи с защитой данных.

Помимо дома, личная почта рассматривалась как часть частной жизни, нуждающаяся в особой защите. Задолго до того, как эта защита стала общепринятой, в частности, благодаря использованию телеграфа, известны первые случаи вторжения в личную почту. Например, в 1624 году плантация Плимут была местом, которое впервые упоминается как зафиксированное вторжение в личную жизнь. Губернатор Уильям Брэдфорд узнал о заговоре против руководства небольшой колонии. Он перехватил несколько компрометирующих писем, написанных двумя новичками и отправленных друзьям в Англию. Двое мужчин отрицали заговор, губернатор предъявил письма и попросил их прочитать их содержимое вслух. Мужчины выразили возмущение тем, что их личная переписка была перехвачена, но не стали подчиняться, поскольку у них не было законных оснований для этого.

Любопытство всегда было врагом частной жизни и является слабостью, которая стимулировала вторжение в частную жизнь и на которой газеты эксплуатировали частную жизнь личности на коммерческой основе. В 1873 году появились первые жалобы на журналистов, которые использовали методы интервьюирования. Например, президент Кливленд выражал недовольство тем, как пресса обращалась с ним время от времени, особенно когда некоторые журналисты следовали за ним и его невестой во время их свадебного путешествия в 1886 году. В конце 19-го века главным врагом частной жизни является любопытство, проявляемое некоторыми людьми к делам других людей.

Право на неприкосновенность частной сферы как юридическая категория зародилось в США. В английском языке все стороны частной жизни обозначаются единым термином «privacy», который не имеет эквивалента в русском языке. Одна из первых попыток сформулировать понятие «privacy» была предпринята в 1890 г. известными американскими юристами Сэмюэлем Уорреном и Луисом Брандейсом, которые определили его как право быть оставленным в покое или право быть предоставленным самому себе («the right to be alone»). Существует легенда, что создание статьи напрямую связано с одним случаем, который произошёл с Брандайсем. Однажды к нему домой пришел посетитель. Пока дворецкий звал хозяина, гость достал фотокамеру Kodak, делающую мгновенные снимки, и сфотографировал гостиную. Брандайс был глубоко поражен случившимся. Он чувствовал себя некомфортно: появилось ощущение, что у него украли личную вещь. Но, будучи юристом, он понимал, что нарушения прав человека не произошло.

В своей статье «Право на приватность» в Гарвардском правовом журнале они утверждали, что приватность подвергается опасности со стороны новых

изобретений и методов ведения бизнеса, и обосновывали необходимость создания специального «права приватности». Авторы заявляют, что «мгновенные фотографии и газетное предпринимательство вторглись в священные пределы частной и домашней жизни», и стремятся «рассмотреть, предоставляет ли существующее право принцип, который можно было бы надлежащим образом использовать для защиты частной жизни личности».

Классический пример вторжения в частную жизнь – использование без согласия фотографии человека для продвижения продукта. Первоначальным испытанием было дело Роберсон против Rochester Folding Box Co., которое потрясло юридический мир Нью-Йорка. Местная мукомольная компания решила использовать фотографию Эбигейл Рочестер, очаровательной и привлекательной девушки того времени, для продвижения своего продукта. По этой причине был использован блестящий слоган «Мука семьи» , который вместе с фотографией был размещен в многочисленных магазинах, на складах и в салонах. Эбигейл заявила о «праве на частную жизнь» и подала иск на сумму 15 000 долларов. Нью-йоркский суд отклонил иск решением 4-3, заявив, что ее иск не имеет права на том основании, что общему праву еще неизвестно, что именно было нарушено.

Это решение вызвало большое удивление и оказало сильное влияние на последующие судебные разбирательства, в частности, три года спустя было рассмотрено дело Pavesich против New England Life Insurance Co. В этом судебном деле фотография Паоло Павесича была использован без его согласия страховой компанией для рекламы. На фотографии был изображен здоровый мужчина – Павесич, который действительно купил полис страхования жизни, в отличие от больного человека, который этого не сделал и, предположительно, не мог сделать такую «бесценную» покупку для своей будущей безопасности. Под фотографией Павесича была надпись: «В свой здоровый и продуктивный период жизни я купил страховку в New England Life Insurance Co. в Бостоне, Массачусетс, и сегодня моя семейная жизнь защищена». На самом деле Павесич никогда не покупал такую страховку жизни и не делал никаких заявлений, как процитировано. Он нашел рекламу неприятной и подал иск на возмещение ущерба в размере 25 000 долларов. В этом случае право на неприкосновенность частной жизни было единогласно принято. Суд постановил, что страховая компания должна возместить ущерб за вторжение в частную жизнь Павесича. Это был значимый прецедент с точки зрения несанкционированного использования фотографии отдельного лица и защиты данного аспекта личной жизни.

Чрезвычайно важным и часто цитируемым делом было дело Олмстеда против Соединенных Штатов 1928 года. В этом деле оборудование для прослушивания телефонных разговоров использовалось полицией в качестве способа получения доказательств. Жалоба не была принята 5 из 9 судей, поскольку не было фактического проникновения в дома и не было изъято ничего осязаемого. Таким образом, поправка об обыске и выемке не могла быть применена. Однако более важным, чем решение, было несогласие судьи

Брандейса, соавтора статьи «Право на приватность» в Гарвардском правовом журнале. По его мнению, это дело показало, что была нарушена частная жизнь человека, то есть «право быть оставленным в покое как самое всеобъемлющее из прав и право, которое больше всего ценят цивилизованные люди».

Рассуждения Брандейса были приняты лишь сорок лет спустя в деле Кац против Соединенных Штатов. Федеральные власти использовали электронные подслушивающие устройства, прикрепленные к внешней стороне телефонной будки, которой пользовался Чарльзом Катцом, которого власти подозревали в нарушении законов об азартных играх. Несмотря на то, что собственность не была захвачена, суд постановил, что этот метод сбора доказательств нарушает права Катца, предусмотренные Четвертой поправкой. По мнению суда, конституция защищает все, что стремится сохранить как частное. Самое примечательное в этом деле – это интерпретация того, что является частным в значении Четвертой поправки. По мнению судьи Харлана, частное можно определить как фактическое субъективное ожидание индивидуума в отношении частной жизни и в той степени, в которой это ожидание было тем, что общество готово признать «разумным». С тех пор это толкование использовалось во многих случаях, связанных с домами, бизнесом, запечатанным багажом и посылками. В то же время его также часто критикуют и считают имеющим ограниченную ценность, поскольку оно ограничивается вмешательством правительства в частную жизнь и не применяется к объектам, контролируемым третьими лицами, таким как, например, банковские записи.

В 1965 г. в деле Griswold против Connecticut судья Верховного суда США Дуглас вывел право на приватности из первых пяти поправок к Конституции США, признав, что эти поправки «охраняют различные аспекты неприкосновенности частной жизни». Широко известны его слова, которые он произнес, резюмируя решение суда: «Мы имеем дело с правом на неприкосновенность частной жизни, которое старше, чем Билль о правах». В рамках дело рассматривался вопрос о защите Конституцией права на неприкосновенность частной жизни супругов от ограничений штата на возможность получения парой консультаций по использованию противозачаточных средств. В решении суд указал, что Конституция явно не защищает общее право на неприкосновенность частной жизни, различные гарантии в Билле о правах создают полутени или зоны, которые устанавливают право на неприкосновенность частной жизни. Вместе Первая, Третья, Четвертая и Девятая поправки создают право на неприкосновенность частной жизни в супружеских отношениях.

На свет продолжали появляться публикации о приватности. Они достигли кульминации в 1962 году в рамках проекта «Влияние науки и технологий на конфиденциальность». Проект разрабатывался между 1962 и 1966 годами Специальным комитетом по науке и праву Ассоциации адвокатов города Нью-Йорка. Директором по исследованиям был Алан Вестин, который опубликовал подробные сведения о результатах в «Columbia Law Review» и в своей книге «Конфиденциальность и свобода» и заложил прочную основу для последующего

обсуждения. Почти во всех публикациях того периода в отношении частной жизни используются три слова: свобода, контроль и самоопределение. Понятие конфиденциальности определяется почти так же, как это было в 1891 году Уорреном и Брандейсом. Конфиденциальность описывается как право быть оставленным в покое и право каждого человека определять в обычных обстоятельствах, какими будут его или ее мысли, чувства и эмоции при общении с другими. Из-за прогресса в области технологий конфиденциальность становится все более важной проблемой. Эти характеристики конфиденциальности повторяются и разрабатываются многочисленными авторами в начале 1960-х годов.

В своей работе «Приватность и свобода» Алан Уэстин подводит итоги обсуждения и определяет приватность на основе всех этих пунктов. «Приватность – это притязание отдельных лиц, групп или учреждений самостоятельно определять, когда, как и в какой степени информация о них передается другим. Рассматриваемая с точки зрения отношения отдельного лица к социальному участию, приватность – это добровольное и временное удаление человека от общества в целом с помощью физических или психологических средств, либо в состоянии уединения или близости в небольшой группе, либо, когда речь идет о более крупных группах, в состоянии анонимности или сдержанности».

Выделялось 4 функции приватности:

– потребность в личной автономии, которая жизненно важна для развития индивидуальности и осознания индивидуального выбора в жизни любого человека. Она поддерживает нормальное психологическое функционирование, стабильные межличностные отношения и личностное развитие.

– приватность как форма эмоционального освобождения. Она поддерживает здоровое функционирование, предоставляя необходимые возможности расслабиться, быть самим собой, уйти от стрессов повседневной жизни и выразить гнев, разочарование, горе или другие сильные эмоции без страха последствий или насмешек. Последствия отказа от таких возможностей могут быть от возросшего напряжения и недальновидного выражения до самоубийства и психического срыва.

– приватность влияет на самооценку и принятые решения. Людям необходимо пространство и время для обработки информации, которая поступает к ним в огромном количестве. Уединение дает человеку возможность рассмотреть альтернативы и последствия, чтобы действовать максимально последовательно и уместно.

– потребность в ограниченном и защищенном общении, что особенно важно в городской жизни с ее скоростью и постоянными физическими и психологическими столкновениями. Ценность приватности признает, что людям нужны возможности делиться конфиденциальной информацией со своей семьей, друзьями и близкими.

В конце 1970-х годов понятие приватности было скорректировано с учетом появления телекоммуникации. Людей стала пугать не столько обработка данных, а распространение их среди неизвестных получателей.

Широкое распространение компьютеров произвело революцию в хранении и обработке данных, что привело к созданию электронных баз данных, которые могли хранить огромные объемы личной информации. Это вызвало опасения относительно потенциального злоупотребления и масштабных нарушений конфиденциальности.

На раннем этапе внедрения Интернета концепция «конфиденциальности» была вторичной по отношению к фокусу на «безопасности». Поскольку первые пользователи Интернета привыкли запоминать пароли и использовать электронную почту, компаниям пришлось изобретать новые способы предотвращения мошенничества и кражи данных. Для обычного пользователя конфиденциальность и безопасность были одним и тем же, так как не было идеи использования данных за пределами их явного назначения, не говоря уже о продаже рекламодателям.

Все изменилось с появлением таких компаний, как Google, которые разработали способ использования пользовательских данных для повышения релевантности результатов поиска и эффективности интернет-рекламы. Бизнес-модель Google позволяла пользователям получать выгоду от бесплатной и очень полезной поисковой системы и других приложений, в то время как рекламодатели могли получать выгоду от улучшенного таргетинга рекламы, основанного на их поисковых запросах и поведении. Эта модель стала чаще использоваться в таких социальных сетях как Facebook и Twitter.

К концу 1970-х годов достижения в области телекоммуникаций добавили новое измерение к этим проблемам. Слияние вычислений и телекоммуникаций, известное как телематика, сделало возможными инновации (такие как телеобразование и телемедицина), но также увеличило риски, в частности, возможность распространения конфиденциальных данных неизвестным получателям.

В этот период такие исследователи, как Эндрю Яо (многосторонние вычисления) и Дэвид Чаум (слепые подписи и т. д.), разработали основы технологий повышения конфиденциальности. Одновременно появились движения, ориентированные на конфиденциальность. Начиная с конца 1980-х годов, движение шифропанк выступало за широкое использование надежного шифрования и технологий повышения конфиденциальности для защиты личной конфиденциальности и сопротивления государственному или корпоративному надзору (до этого шифрование в основном использовалось правительствами).

В 1991 году Фил Циммерман выпустил Pretty Good Privacy (PGP) – новаторское программное обеспечение для шифрования, которое позволяло людям защищать свои сообщения от несанкционированного доступа. Хотя правительство США изначально оспаривало PGP, оно стало краеугольным камнем защиты конфиденциальности и шифрования, оказав влияние на глобальный сдвиг в принятии безопасных коммуникационных технологий.

В то же время правительства и организации начали формализовать защиту конфиденциальности через законодательство и международные соглашения. Например, в 1974 был издан Закон США о конфиденциальности, который установил правила сбора, хранения, использования и распространения личной информации федеральными агентствами. В 1977 ФРГ приняла Федеральный закон о защите данных, который стал одним из первых всеобъемлющих законов о конфиденциальности данных.

Хотя правовые рамки были необходимы и важны, критики утверждали, что слишком большая фокусировка на регулировании, ввиду чего упускались из виду общественные и технологические решения проблем конфиденциальности.

В 2008 году появилась технология блокчейн, предлагающая децентрализованный подход к финансовым транзакциям и цифровой идентификации. Цель состояла в том, чтобы отойти от централизованных систем, которые стали уязвимы для наблюдения и утечек данных. Несмотря на то, что связь между блокчейном и конфиденциальностью не является простой (присущая блокчейну неизменность противоречит «праву быть забытым»), такие технологии, как доказательства с нулевым разглашением, успешно используются для согласования конфиденциальности с прозрачностью, которую обеспечивает блокчейн.

В настоящее время выделяется новый термин – «цифровая конфиденциальность». Концепция цифровой конфиденциальности относится к праву и возможности человека решать, как его личная информация собирается, используется и передается в цифровом мире. Она отражает желание человека перемещаться по цифровому ландшафту без страха несанкционированного сбора, неправильного использования или распространения личной информации – это его интернет-конфиденциальность.

Важность цифровой конфиденциальности отражается в различных областях. Во-первых, она расширяет возможности отдельных лиц, предоставляя им контроль над своей информацией и свободу взаимодействовать с цифровым миром на своих условиях. Во-вторых, она помогает предотвращать киберпреступность, такую как кража личных данных, мошенничество и преследование. В-третьих, она играет решающую роль в поддержании свободного и открытого общества, защищая от необоснованного вторжения и слежки со стороны государственных и корпоративных структур.

Одной из наиболее распространенных угроз цифровой конфиденциальности являются кибератаки. Целью этих атак является компрометация личной информации людей, часто с использованием сложных методов обхода мер безопасности. Кибербезопасность, относящаяся к мерам, применяемым для защиты от таких атак, становится критически важным факторов в поддержании цифровой конфиденциальности.

Утечки данных – это особый тип кибератак. Они происходят, когда неавторизованные лица получают доступ к базе данных, содержащей персональные данные. Компрометация персональной информации во время утечек данных может иметь серьезные последствия, начиная от кражи личных

данных и заканчивая финансовыми потерями. Утечки особенно разрушительны, поскольку они могут включать незаконное раскрытие огромных объемов данных.

Одной из распространенных угроз цифровой конфиденциальности являются атаки социальной инженерии, которые эксплуатируют человеческую психологию, а не технологические уязвимости. Эти атаки манипулируют людьми, заставляя их раскрывать конфиденциальную информацию или вести себя таким образом, который ставит под угрозу их цифровую конфиденциальность. Примерами социальной инженерии являются фишинговые письма, маскирующиеся под заслуживающие доверия сущности, и предлоги, когда злоумышленники фабрикуют сценарии, чтобы обмануть своих жертв.

Кроме того, технологии отслеживания представляют собой существенные проблемы для цифровой конфиденциальности. Эти технологии, включая файлы cookie, трекеры и маяки, отслеживают онлайн-активность пользователей с пугающей степенью детализации. Веб-сайты используют такие технологии для сбора различных данных – от посещаемых вами страниц до используемого вами устройства – для различных целей, включая целевую рекламу и улучшение пользовательского опыта. Однако эти методы могут нарушать конфиденциальность пользователей, поскольку они могут использоваться без явного знания или согласия пользователей.

Как видно из литературы по этой теме, можно выделить два измерения приватности: реляционное и информационное. Первое касается отношений человека с другими людьми, например, контроля того, кто может войти в домашнюю среду или кому разрешено прикасаться к телу. Эти аспекты иногда описываются как территориальная приватность и телесная приватность. Информационное измерение связано со сбором, хранением и обработкой (персональных) данных.

Общим для обоих измерений приватности является необходимость сохранять контроль над личным пространством, телом и информацией о себе; однако очевидно, что в определенных ситуациях потеря контроля еще важнее, например, когда люди теряют сознание из-за несчастного случая.

В литературе выделяют следующие виды приватности:

(1) Телесная приватность:

Это приватность связана с телом. Ношение одежды с целью скрыть отдельные части тела, необходимость использования санитарных комнат для удовлетворения физиологических потребностей, защита от нежелательных прикосновений и насилия – всё это относится к телесной приватности. Примером нарушения телесной приватности служат сканеры в аэропорту. Первые их модели нарушали право людей на приватность, поскольку показывали тело человека. Пассажирам это крайне не нравилось: люди начали протестовать и смогли добиться изменений. Теперь сканеры показывают не тело, а лишь его очертания, и подсвечивают предметы, вызывающие подозрение.

(2) Пространственная приватность:

Пространственная приватность касается территории, которая считается своим личным пространством. Это может быть дом, квартира, личный шкафчик или автомобиль. Никто не имеет права вторгаться в личное пространство человека. Это гарантировано не только законодательством государств, но и Всеобщей декларацией прав человека. Ярким примером нарушения пространственной приватности стала игра Pokemon Go. С помощью камеры и режима дополненной реальности пользователи должны были следовать указаниям игры и искать покемонов. Кроме 100 миллионов скачиваний в Google Play и Apple Store разработчики получили также бессчетное количество жалоб. Игра не учитывала границ частной собственности граждан и предлагала игрокам искать покемонов на территории частных домов, в муниципальных зданиях, храмах и т.д. Из-за многочисленных жалоб людей, которым надоели бегающие по их участкам искатели покемонов, проект пришлось закрыть.

(3) Коммуникационная приватность:

Она защищает тайну почтовой связи, телефонных разговоров, электронных переписок и других способов общения. Пытаясь ее сохранить, мы переходим на шепот, вкладываем письма в конверты, пишем в социальных сетях личные сообщения и т.д. Пример нарушения – скандал Facebook. Журналисты Bloomberg выяснили, что компания нанимала подрядчиков для расшифровки голосовых сообщений пользователей. После того, как на компанию получила множество исков, Facebook был вынужден прекратить расшифровку и принести извинения своим пользователям.

(4) Информационная приватность:

Она связана с понятиями чести, достоинства и их влиянием на жизнь. Люди формируют отношение к друг другу на базе того, что им известно о друг друге. Часто один факт из жизни может поменять отношение, сказаться на положении в обществе. С развитием технологий люди становятся заложниками информации, которая уже была собрана ранее. Например, при подготовке резюме создается образ для HR-менеджеров: рассудительный, образованный, интеллектуальный человек. Однако HR-специалист изучит не только резюме, но и информацию из открытых источников. Например, там он нашел ссылку на форум, где кандидат принимал участие и высказывал неоднозначное мнение 10 или 15 лет назад. Таким образом, прошлые ошибки повлияли на настоящее, так как остался «цифровой след». С развитием технологий у новых поколений фактически исчезло право на ошибку, ведь вся информация попадает в интернет.

Согласно статье европейского исследователя Майкла Фридевальда, различают 7 аспектов приватности:

1. Приватность индивида подразумевает право скрывать физиологические характеристики своего организма, например, генетический код и биометрические характеристики.

2. Приватность образа действий включает в себя такую чувствительную информацию, как сексуальные предпочтения и склонности, политическую деятельность, религиозные практики.

3. Приватность коммуникаций стремится сделать невозможным контроль коммуникации, а именно изучение чужой почты, использование подслушивающих устройств и направленных микрофонов, прослушивание или запись коммуникаций по телефону или беспроводным каналам связи, доступ к сообщениям электронной почты.

4. Приватность данных и изображений подразумевает гарантию того, что данные одного человека не становятся автоматически доступными другим людям и организациям, и что люди «осуществляют основной контроль над своими данными и их использованием».

5. Приватность мыслей и чувств. У людей есть право не делиться своими мыслями или чувствами, или же высказать их. У людей есть право думать так, как им угодно.

6. Приватность месторасположения означает, что у людей есть право передвигаться в общественных местах не будучи идентифицированными, не подвергаясь слежке или мониторингу.

7. Приватность ассоциаций, в том числе приватность групп, связана с правом людей общаться с теми, с кем они хотят, не подвергаясь мониторингу.

ЛЕКЦИЯ 3. ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ЕВРОПЕЙСКОМ СОЮЗЕ: ПОНЯТИЕ И СОДЕРЖАНИЕ

В ЕС предусмотрено специальное регулирование защиты персональных данных. До разработки GDPR действовало несколько актов:

- Директива ЕС по защите данных 95/46/ЕС3 как основополагающий документ, который, однако, не имел прямого действия. Каждое государство-член ЕС имел право на разработку собственного национального законодательства о защите персональных данных.

- Директива по защите данных полиции и уголовного правосудия.

- Рамочное соглашение 2008/977/JHA5, которое не вносило значительных изменений в общую конструкцию защиты данных в Европе и скорее был подготовительным этапом в принятии GDPR.

GDPR применяется к обработке персональных данных, осуществляемой полностью или частично с помощью автоматизированных средств, а также к неавтоматизированной обработке персональных данных, формирующих часть системы данных либо предназначающихся, чтобы стать частью системы данных. Обработка персональных данных в быту и личной жизни не обязывает соблюдать GDPR. Понятие «автоматизированные средствами» обозначает компьютеры, смартфоны, ноутбуки, сервера, «умные» часы т.п. Если же процесс обработки осуществляется в уме или на бумаге, то соблюдать GDPR не требуется, за исключением случаев, если обрабатываемые личные данные представляются в систему, то есть делается возможным быстрый и эффективный поиск конкретного лица и сведений о нем.

Например, таблички с именами жильцов в ФРГ не «обязывают» соблюдать GDPR. Домовладельцы вешают их рядом со звонками в квартиры у двери подъезда. В данном случае данные не собраны в каталог или систему.

GDPR применяется к обработке персональных данных в контексте деятельности организационной единицы контролёра или процессора в ЕС, независимо от того, производится обработка в ЕС или нет.

Например, прецедент CJEU, Google Spain SL/Agencia española de protección de datos. «В свете этой цели Директивы 95/46 и формулировки Статьи 4(1)(a) следует признать, что обработка персональных данных для целей обслуживания поисковой системы, такой как Google Search, которая управляется предприятием, имеющим местонахождение в третьем государстве, но имеющим предприятие в государстве-члене ЕС, осуществляется «в контексте деятельности» этого предприятия, если последняя направлена на продвижение и продажу в этом государстве-члене ЕС рекламных площадей, предлагаемых поисковой системой, что служит для обеспечения прибыльности услуг, предлагаемых этой системой. При таких обстоятельствах деятельность оператора поисковой системы и деятельность его заведения, расположенного в соответствующем государстве-члене, неразрывно связаны, поскольку деятельность, связанная с рекламным пространством, является средством обеспечения экономической выгоды рассматриваемой поисковой системы, а эта система в то же время является средством, позволяющим осуществлять эту деятельность.

GDPR применяется к обработке персональных данных субъектов данных, находящихся в Союзе, контролёром или процессором, не имеющими организационной единицы в ЕС, если процессы обработки данных касаются:

(a) предложения товаров и услуг субъектам данных, находящимся в Союзе, независимо от того, требуется ли от них оплата, или нет, либо

(b) мониторинга их поведения, если такое поведение происходит в Союзе.

GDPR применяются к обработке персональных данных контролёром, не имеющим организационной единицы в ЕС, но имеющим организационную единицу в том месте, где согласно международному публичному праву действует законодательство государства-члена.

Применяется GDPR в данных ситуациях.

1. Белорусское мобильное приложение обрабатывает данные о геолокации белорусских и иностранных граждан, находящихся в ЕС.

2. Белорусский сайт знакомств собирает контактные данные всех своих пользователей. На сайте зарегистрированы также американцы и европейцы, приезжающие в Беларусь и желающие познакомиться с местными девушками.

Рассмотрим несколько ключевых терминов из GDPR, которые важны для понимания порядка его применения.

(1) «Персональные данные» – это любая информация, относящаяся к «субъекту данных», то есть идентифицированному или поддающемуся идентификации физическому лицу; поддающееся идентификации физическое лицо – это лицо, которое можно прямо или косвенно идентифицировать, в

частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор, либо на один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица.

Так, выделяется в конструкции персональных данных 4 «несущих» блока: «любая информация», «относящаяся к», «идентифицированному или идентифицируемому», «физическому лицу». Данные, «относящиеся к» субъекту, включают в себя не только информацию о самом субъекте, но и о принадлежащих ему или иным образом связанных с ним объектах, питомцах. Таким образом, данными, «относящимися к» субъекту, являются не только номер телефона, автомобиля, компьютера, банковской карты, фитнес-трекера, чипа питомца, но и иные характеристики этих объектов и животных: цена, износ, серийные номера, поломки, диагнозы, результаты анализов и т.д. Также выделяет три элемента, каждый из которых, независимо от наличия других, может сделать любую информацию «относящейся к» субъекту – это содержание, цель и результат.

Информация может относиться к субъекту по своему содержанию, если она о конкретном физическом лице, например, результаты тестов на экзамене, номер телефона конкретного лица, профиль определенного пользователя в социальных сетях.

Информация может относиться к субъекту также по цели, если она используется или, вероятнее всего, будет использована в целях оценки, влияния на статус или поведение субъекта, проявления определенного рода отношения к субъекту. Например, список посещенных сотрудниками компании интернет страниц в корпоративной сети, может быть использован для целей мониторинга эффективности использования рабочего времени каждым сотрудником, или для блокировки определенных страниц определенным сотрудникам.

Информация может относиться к субъекту персональных данных, даже в отсутствие признаков «содержания» и «цели», если есть признак результата: если обработка данных, вероятнее всего, повлияет на права и интересы субъекта, например, даже если слегка изменит отношение окружающих к нему, заставит выделять его среди остальных в сообществе. Например, информация о том, что дедушка школьника получил премию Дарвина, может вызвать насмешки и издевательства со стороны сверстников. Эти три элемента относимости данных к субъекту применяются каждый в отдельности, но, если присутствует хотя бы один элемент, нет надобности выявлять остальные два – данные точно относятся к субъекту.

(2) «Идентифицированному или идентифицируемому» – имеет квалифицирующее значение для определения информации, относящейся к субъектам. Определяет лицо как идентифицируемое, если оно еще не идентифицировано, но его возможно идентифицировать прямо, например, по фамилии (если это позволяет выделить субъекта из группы) или косвенно – по номеру паспорта, телефона или комбинации предпочтений, позволяющих

выделить субъекта из группы (это может быть возраст, внешний вид, обладание специальным объектом или навыком и т.д.).

Гипотетическая вероятность идентификации субъекта не делает информацию персональными данными. Если возможность идентифицировать субъекта отсутствует или ничтожно мала, данные не могут считаться персональными. Даже если, по мнению контролера, идеи идентифицировать субъекта не было, но идентификация возможна при сопоставлении с другой базой данных, например, в рамках межведомственного обмена данными, получения данных от сотовых контролеров, с дорожных камер видеонаблюдения, либо в рамках интеграции систем, то соблюдение GDPR обязательно.

Необходимо определить какие разумные усилия контролер или любое третье лицо должны будут приложить для идентификации конкретных субъектов: затраты денежных средств на такие усилия; временные и человеческие ресурсы; наличие технологии, позволяющей выполнить идентификацию без особых усилий и затрат; подразумеваемая (а не декларируемая цель) и построение обработки; какие выгоды может извлечь контролер или любое другое третье лицо; продолжительность хранения данных и потенциальное развитие технологий для идентификации в этот период.

В каждом конкретном случае необходимо определять наличие возможности и прилагаемые ресурсы контролера для идентификации субъектов по номеру телефона. Если возможность есть, или цель и контекст обработки предполагает идентификацию субъекта, то номер телефона является персональными данными.

(3) «Обработка» – это любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными с использованием средств автоматизации или без использования таких средств, включая сбор, запись, организацию, структурирование, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение.

В определении содержатся примеры действий над персональными данными.

В определении отсутствует упоминание цели. Однако, когда статья GDPR гласит, что кто-то должен выполнить что-то в отношении «обработки», то под обработкой понимаются действия (операции), объединенные одной целью. На практике обработки зачастую связаны с процессами в организации, например, маркетинговая рассылка, уведомление о работе сайта и т.п. Поэтому один вид обработки над одними и теми же данными, например, сбор email-адреса в веб-форме, может быть частью сразу нескольких обработок (процессов). Например: регистрация на сервисе с помощью email, уведомление о работе сервиса по email, маркетинговая коммуникация через тот же email – три разных обработки над одними и теми же данными, в которых присутствует операция сбора email-адреса.

(4) «Контролёр» – это любое физическое или юридическое лицо, государственный орган, учреждение или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных; контролёр или критерии для его определения могут быть установлены законодательством Союза или государства-члена в случаях когда, цели и средства этой обработки определяются законодательством Союза или государства-члена.

В качестве примера может быть несколько ситуаций. IT-компания предоставляет свое программное обеспечение и проводит анализ данных для обработки ежедневных записей о посещаемости фитнес-клуба за ежегодную плату. В случае предоставления программного обеспечения компания не является контролером, но в случае анализа данных она является процессором для школы.

Покупатели магазина заказывают товары с доставкой на дом. Доставкой занимается отдельная компания, которая является процессором для магазина.

Маркетинговая компания рассылает рекламные ваучеры клиентам парикмахерской от имени парикмахера. Маркетинговая компания является процессором для парикмахерской.

Организация использует облачный сервис для хранения и анализа своих данных. Организация остается контролером, а поставщик облачных услуг - процессором.

(5) «Процессор» – это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает персональные данные от имени и по поручению контролёра;

На практике контролер определяет цель в рамках задач, поставленных законодательством, и основные элементы средств, в то время как процессор играет роль исполнителя. Другими словами, «действовать от имени контролера означает, что процессор служит интересам контролера при выполнении конкретной и что он, таким образом, следует инструкциям контролера, по крайней мере, в отношении, по крайней мере, цели и основных элементов средств. Основная обязанность по соблюдению требований лежит на контролере.

(6) «Согласие» субъекта данных – это добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных;

Как и в белорусском законодательстве, в ст. 5 GDPR установлены принципы обработки персональных данных: lawfulness, fairness and transparency; purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.

(a) обрабатываться законно, справедливо и прозрачно для субъекта данных.

Пример прозрачности: разработка политики конфиденциальности простым и понятным языком, которая находится в доступном месте.

Пример законности: Реализуя принцип законности, банк, вводя новую маркетинговую услугу понимает, что он не может использовать «необходимое для заключения договора основание» для той части обработки, которая предполагает сбор персональных данных. Тот факт, что эта конкретная обработка представляет собой риск того, что субъект данных станет менее вовлеченным в процесс обработки своих данных, также является значимым фактором при оценке законности самой обработки. Банк приходит к выводу, что эта часть обработки должна опираться на согласие.

Пример справедливой обработки: Контролер управляет поисковой системой, которая обрабатывает в основном личные данные пользователей. Контролеру выгодно иметь большой объем персональных данных и иметь возможность использовать их для целевой рекламы. Поэтому контролер хочет повлиять на субъектов данных, чтобы они разрешили обширный сбор и использование своих персональных данных. Контролер не может представлять варианты обработки таким образом, чтобы затруднить субъектам данных воздержаться от передачи своих данных, или затруднить субъектам данных изменение настроек конфиденциальности и ограничение обработки.

(b) собираться для конкретных, отчетливых и законных целей и не обрабатываться в последующем несовместимым с этими целями образом; дальнейшая обработка для архивных целей в публичном интересе, в целях исторических или научных исследований или для статистических целей, в соответствии со ст. 89(1), не считается несовместимой с начальными целями.

Пример ограничения цели: Контролер обрабатывает персональные данные своих клиентов. Цель обработки - исполнение договора, т. е. возможность доставить товар по нужному адресу и получить оплату. Допустимо хранение таких персональных данных, как история покупок, имя, адрес, адрес электронной почты и номер телефона. Например, контролер рассматривает возможность приобретения продукта Customer Relationship Management (CRM), который собирает все данные о клиентах, такие как продажи, маркетинг и обслуживание клиентов, в одном месте. Продукт дает возможность хранить все телефонные звонки, действия, документы, электронные письма и маркетинговые кампании, чтобы получить 360-градусное представление о клиенте. В конечном итоге CRM автоматически анализирует покупательскую способность клиентов, используя общедоступную информацию. Цель такого анализа - более точное нацеливание рекламы, но он не является частью первоначальной законной цели обработки. Чтобы соответствовать принципу ограничения целей, контролер требует от поставщика продукта сопоставить различные действия по обработке персональных данных с целями, важными для контролера. Еще одно требование заключается в том, что продукт должен быть способен отмечать, какой вид деятельности по обработке персональных данных не соответствует законным целям контролера.

(c) быть адекватным и релевантным тому, что необходимо касательно целей, для достижения которых они обрабатываются, а также ограничены этим.

Пример минимизации данных: Книжный магазин хочет увеличить свой доход за счет продажи книг через Интернет. Владелец книжного магазина создает стандартную форму для оформления заказа, в которой запрашивается дата рождения, номер телефона и домашний адрес. Обязательное заполнение этих данных не соответствует анализируемому принципу. Однако заполнение даты рождения и номера телефона субъекта данных не являются необходимым для покупки товара. Это означает, что они не могут быть обязательными полями в веб-форме для заказа товара. Более того, бывают ситуации, когда адрес не нужен. Например, при заказе электронной книги покупатель может скачать продукт, и его адрес не нужно обрабатывать в интернет-магазине.

(d) быть точными и при необходимости поддерживаться в актуальном состоянии; необходимо принять все разумные меры, чтобы персональные данные, которые являются неточными в свете целей, для которых они обрабатываются, были немедленно удалены или уточнены.

Пример точности: Банк хочет использовать искусственный интеллект для составления профиля клиентов, подающих заявки на получение банковских кредитов, в качестве основы для принятия решений. При разработке решения должны определяться средства обработки и учитываться защита данных по проекту при выборе искусственного интеллекта и при принятии решения о том, как его обучать. При определении способа обучения контролер должен иметь точные данные для достижения точных результатов. Поэтому он должен убедиться, что данные, используемые для обучения, точны.

Учитывая, что у контролера есть правовая основа для обучения с использованием персональных данных большого числа своих существующих клиентов, он выбирает репрезентативный пул клиентов, чтобы избежать предвзятости. Данные о клиентах собираются из их собственных систем, в которых собираются данные об истории платежей существующих клиентов, банковских операциях, задолженности по кредитным картам, проводятся новые проверки кредитоспособности, а также собираются данные из государственных реестров, к использованию которых они имеют законный доступ. Чтобы обеспечить максимальную точность данных, используемых для обучения, контролер собирает данные только из источников с корректной и актуальной информацией.

Когда искусственный интеллект полностью обучен и работает, банк использует его результаты в качестве части оценки кредитов, но при этом его решение не должно зависеть только от решения искусственного интеллекта.

(e) храниться в форме, которая позволяет идентифицировать субъектов данных не дольше, чем это необходимо для целей, для которых эти данные обрабатываются. Они могут храниться в течение более длительного периода, до тех пор, пока они будут обрабатываться исключительно для архивных целей в публичном интересе, в целях исторических или научных исследований, или статистических целях в соответствии со ст. 89(1), при условии, что будут реализованы соответствующие технические и организационные меры, предусмотренные GDPR в целях защиты прав и свобод субъекта данных.

Пример ограничения хранения: Контролер собирает персональные данные, если целью обработки является администрирование членства с субъектом данных, после прекращения членства персональные данные должны быть удалены. Контролер устанавливает внутреннюю процедуру хранения и удаления данных. В соответствии с ней работники должны вручную удалять персональные данные после окончания срока хранения. Работник следует процедуре регулярного удаления и исправления данных с любых устройств, из резервных копий, журналов, электронной почты и других соответствующих носителей. Чтобы сделать удаление более эффективным, контролер вместо этого внедряет автоматическую систему для автоматического и более регулярного удаления данных. Система настроена таким образом, чтобы следовать заданной процедуре удаления данных, которая затем происходит через заранее определенный регулярный интервал, чтобы удалить персональные данные со всех носителей компании. Контролер регулярно проверяет и тестирует политику хранения данных.

(f) обрабатываться способом, обеспечивающим соответствующую безопасность персональных данных, включая защиту от несанкционированной или незаконной обработки, а также от случайной потери, уничтожения или повреждения, с помощью соответствующих технических и организационных мер.

Пример целостности и конфиденциальности: Контролер хочет извлечь персональные данные из медицинской базы данных на сервер компании. Компания оценила риск маршрутизации извлечений на сервер, доступный всем работникам компании, как высокий для прав и свобод субъектов данных. В компании есть только один отдел, которому необходимо обрабатывать эти данные о пациентах. Чтобы регулировать доступ и снизить возможный ущерб от вредоносного программного обеспечения, компания решает разделить сеть и установить контроль доступа к серверу и каталогу. Кроме того, они устанавливают мониторинг безопасности и систему обнаружения и предотвращения вторжений. Контролер активирует контроль доступа к серверу и изолирует его от обычного использования. Для контроля доступа и изменений устанавливается автоматизированная система аудита. При наступлении определенных событий, связанных с использованием сервера, создаются отчеты и автоматические оповещения. Эта мера безопасности гарантирует, что все пользователи будут иметь доступ по принципу «необходимо знать» и с соответствующим уровнем доступа. Ненадлежащее использование может быть быстро и легко распознано.

В ст. 6 GDPR как и в национальном законодательстве установлены основания обработки персональных данных.

(a) субъект персональных данных дал согласие на обработку своих персональных данных для одной или нескольких конкретных целей;

(b) обработка необходима для исполнения договора, в котором субъект данных является стороной, или для реализации по поручению субъекта данных шагов, предшествующих заключению договора;

(c) обработка необходима для выполнения правового обязательства, возложенного на контролёра;

(d) обработка необходима для защиты жизненно важных интересов субъекта данных или другого лица;

(e) обработка необходима для выполнения задачи в публичном интересе или в рамках осуществления государственной власти, доверенной контролёру;

(f) обработка необходима для целей, вытекающих из легитимных интересов, преследуемых контролёром или третьим лицом, за исключением случаев, когда преимущество над такими интересами имеют интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных, в частности, когда субъектом данных является ребенок.

Пример: для того, чтобы обработка данных основывалась на законном интересе, должны быть выполнены три совокупных условия, а именно

- преследование законного интереса контролером данных или третьей стороной или сторонами, которым раскрываются данные,

- необходимость обработки персональных данных для целей преследуемых законных интересов, и

- условие, что основные права и свободы субъекта данных, чьи данные требуют защиты, не имеют приоритета.

Если обработка осуществляется для иной цели, нежели той для которой были собраны персональные данные, не базируется на согласии субъекта данных или законодательстве ЕС или законодательстве государства-члена, являющихся в демократическом обществе необходимым и соразмерным средством гарантирования целей, упомянутых в ст. 23 (1) GDPR, контролёр, чтобы определить, согласуется ли обработка с другой целью, в той, для которой личные данные были первоначально собраны, должен учитывать в частности:

a) Любые отношения между целями, для которых были собраны личные данные, и целями дальнейшей предполагаемой обработки;

b) контекст, в котором были собраны персональные данные, в частности, отношения между субъектами данных и контролёром;

c) природу персональных данных: будут ли обрабатываться специальные категории персональных данных или персональные данные, касающиеся судимостей и правонарушений;

d) возможные последствия для субъектов данных от дальнейшей предполагаемой обработки;

e) существование надлежащих механизмов защиты, которые могут включать шифрование или псевдонимизацию.

При получении согласия контролер в момент его получения должен предоставить следующую информацию:

(a) наименование (имя) и контактные данные контролёра и, при необходимости, его представителя;

(b) контактные данные инспектора по защите персональных данных, если применимо;

(c) цели, для которых обрабатываются персональные данные, а также правовое основание для обработки;

(d) если обработка основывается на пункте (f) Статьи 6(1), легитимные интересы, преследуемые контролёром или третьим лицом;

(e) получатели или категории получателей персональных данных, если имеются;

(f) факт осуществления трансграничной передачи, наличия намерения передать персональные данные в третью страну или международную организацию, а также наличие или отсутствие решения Европейской Комиссии об адекватности, или в случае передачи согласно ст. 46 или 47 или согласно второму подпараграфу ст. 49(1) GDPR.

Дополнительно необходимо представить следующую информацию:

(a) срок хранения персональных данных, или если это не представляется возможным, критерии для определения такого срока;

(b) наличие права требовать от контролёра доступ к персональным данным и их исправления, удаления, ограничения обработки или возражение против обработки, а также право на переносимость данных;

(c) наличия права на отзыв согласия в любое время, несмотря на законность обработки, основанной на согласии до его отзыва;

(d) право подачи жалобы в надзорный орган;

(e) является ли предоставление персональных данных требованием, предусмотренным законодательством или договором, или требованием, которое необходимо для заключения договора, а также обязан ли субъект данных предоставлять персональные данные и возможные последствия непредставления указанных данных;

(f) наличие процесса автоматизированного принятия решения.

Если контролёр намерен в дальнейшем обрабатывать персональные данные в целях, отличных от тех, для которых персональные данные были собраны, до начала указанной обработки он должен предоставить субъекту данных информацию относительно иной цели.

Контролёр принимает соответствующие технические и организационные меры для того, чтобы обеспечить и быть в состоянии продемонстрировать, что обработка выполняется в соответствии с GDPR. При необходимости эти меры пересматриваются и обновляются.

Контролёр должен внедрять надлежащие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только персональные данные, обработка которых требуется для конкретной цели обработки. Оно распространяется на количество собранных персональных данных, степень их обработки, срок их хранения и их доступность. В частности, такие меры должны гарантировать, что персональные данные не будут доступны без вмешательства лица для неопределенного круга физических лиц по умолчанию.

Ограничение обработки персональных данных с точки зрения технических и организационных мер должно регулироваться с помощью политики

информационной безопасности и конфиденциальности вместе с задокументированными процедурами их принятия и соблюдения.

Первые шаги проектирования приватности:

Определить цели обработки и потребность бизнеса в данных.

Анонимизировать или псевдномизировать данные с помощью соответствующих техник, так как это позволяет снижать риски для индивидов.

Примерами техник могут быть:

– псевдонимизация. В ст. 4 GDPR под ней понимается обработка персональных данных, которая проводится таким образом, что персональные данные больше не могут быть связаны с конкретным субъектом данных без использования дополнительной информации, при условии, что дополнительная информация содержится отдельно, и к ней применяют технические и организационные меры обеспечения того, чтобы персональные данные не были связаны с идентифицированным или идентифицируемым физическим лицом. Пример может быть использование кодов или псевдонимов вместо настоящих имен при анализе данных пациентов в медицинском исследовании.

– добавление шума (Noise addition). Эта техника вводит в данные контролируемые случайные элементы, сохраняя их значение для авторизованных пользователей, но делая их нерасшифровываемыми для неавторизованных лиц без соответствующих ключей дешифрования. Процесс иногда включает шифрование данных, которое преобразует исходные данные в безопасный, закодированный формат с использованием уникального ключа шифрования. Расшифровка обращает этот процесс, разблокируя зашифрованные данные для авторизованных пользователей, удаляя добавленный шум.

– подмена (Substitution).

– дифференциальная приватность (Differential privacy). Он даёт возможность понять, оказывают ли персональные данные какое-то статистически значимое влияние на результат запроса. Например, в телефоне активирована функции сообщать об использовании определенного смайлика. Этот отчёт состоит из одного бита информации: 1 означает, что смайлик использовался, 0 – нет. Телефон может получать эти отчёты и вносить их в базу данных. В итоге телефон получает возможность узнать количество пользователей, которым нравится определённый смайлик. Простой процесс суммирования результатов и их публикации – это не обработке персональных данных в полном объеме, потому что арифметическая операция суммы значений в базе данных, которая содержит информацию, потенциально выдаст другой результат, чем суммирование значений из базы данных, где отсутствует переданная информация. Поэтому, хотя такие суммы выдадут немного информации о пользователе, но всё-таки часть персональных данных была обработана.

Для трех следующих техник необходимо три типа переменных:

(1) Идентификаторы (ключевые атрибуты): прямые идентификаторы, такие как имена, номера паспорта, адреса электронной почты и т. д. Эти

переменные в принципе не следует собирать вообще или удалять из набора данных, если они не нужны для исследовательского проекта.

(2) Квази-идентификаторы: косвенные идентификаторы, которые могут привести к идентификации при сочетании с другими квази-идентификаторами в наборе данных или внешней информацией. Это часто демографические переменные, такие как возраст, пол, место жительства и т. д., но также может быть что-то совершенно иное, например физические характеристики, временные метки и т. д. В целом, квази-идентификаторы обычно являются переменными, которые, вероятно, известны кому-то во внешнем мире.

(3) Чувствительные атрибуты: переменные интереса, которые должны быть защищены и которые не могут быть изменены, поскольку они являются основными переменными результата. Например, это может быть медицинское состояние в наборе данных здравоохранения или доход в финансовом наборе данных.

– K-анонимность (агрегация). Он предполагает обобщение и подавление атрибутов данных. Обобщение заменяет конкретные значения более широкими категориями, а подавление вообще удаляет определенные значения. Чтобы сделать набор данных k-анонимным, вы должны сначала определить, какие переменные в наборе данных являются идентификаторами, квази-идентификаторами и чувствительными атрибутами. Например, вместо отображения точного возраста набор данных может показывать возрастные диапазоны (например, 20–30, 31–40). Этот процесс гарантирует, что данные любого человека невозможно будет легко идентифицировать, поскольку они сливаются с более крупной группой похожих записей. Эффективность k-анонимности во многом зависит от выбора квази-идентификаторов и выбранного значения k.

– L-разнообразие (L-diversity). Это расширение k-анонимности, которое гарантирует наличие достаточной вариации в чувствительном атрибуте. L-разнообразие предполагает, что должно быть по крайней мере L различных значений для чувствительного атрибута на комбинацию квази-идентификаторов. Как и в случае k-анонимности, идеального значения L не существует , хотя обычно оно меньше или равно k и больше 1.

– T-близость (T-closeness). T-близость гарантирует, что распределение чувствительного атрибута в рамках обобщения квази-идентификатора близко к распределению чувствительного атрибута во всем наборе данных. Другими словами, она гарантирует, что чувствительный атрибут не будет смещен в сторону определенного значения в группе схожих лиц, что потенциально может быть использовано для повторной идентификации кого-либо. Например, если набор данных содержит информацию о возрасте (квази-идентификатор), поле (квази-идентификатор) и доходе (чувствительный атрибут), а t-близость применяется со значением t = 0,1, то для каждой комбинации возраста и пола распределение дохода должно быть в пределах 10% от распределения дохода во всем наборе данных.

ЛЕКЦИЯ 4. СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРАКТИКА ИСПОЛНЕНИЯ ГЕНЕРАЛЬНОГО РЕГЛАМЕНТА

В соответствии с GDPR у компаний должны быть разработаны ряд документов. Среди них можно назвать, например, Data Processing Agreement.

Data Processing Agreement (DPA) – это юридический документ, устанавливающий положения и условия, на которых третья сторона, например поставщик услуг или подрядчик, обрабатывает персональные данные от имени контролера/компании. DPA четко определяет права и обязанности каждой стороны, участвующей в соглашении. Он гарантирует, что обработчик данных реализует достаточные меры защиты данных при обработке персональных данных, переданных контролером, и что он соблюдает применимое законодательство. DPA сохраняет надзор за обработкой данных, даже если она делегирована поставщику услуг. Он четко определяет обязанности и права обеих сторон, устанавливает ограничения на хранение и обработку данных и предписывает реализацию необходимых технических и организационных мер для защиты данных.

DPA обеспечивает ясность в отношении характера и категорий обрабатываемых данных, целей обработки, обязанностей контролера и обработчиков, субобработки, прав на аудит, уведомлений о нарушениях, удаления и передачи данных, прав субъектов данных и многого другого.

Согласно ст. 28 GDPR обработка процессором регулируется договором или иным правовым актом ЕС, или национальным законодательством государства-члена, которое является обязательным для процессора и контролёра и устанавливает предмет и продолжительность обработки, характер и цель обработки, тип персональных данных, категории субъектов данных, обязательства и права контролёра.

Этот договор или иной правовой акт должны предусматривать, в частности, что процессор:

(a) обрабатывает персональные данные только на основании документированных распоряжений от контролёра, включая передачу персональных данных в третью страну или международную организацию, если только он не обязан делать это по праву Союза или государств-членов, которому подчиняется процессор; в таком случае процессор информирует контролёра об этих правовых требованиях до обработки, если этот закон не запрещает такое информирование по важным с точки зрения публичного интереса основаниям;

Контракт между организацией и клиентом должен включать, но не ограничиваться, целью и временными рамками, которые должны быть достигнуты услугой.

(b) гарантирует, что лица, уполномоченные обрабатывать персональные данные, связаны положением о конфиденциальности или находятся под соответствующим законодательно установленным обязательством о конфиденциальности;

Соглашение о конфиденциальности, является ли оно частью договора или отдельным, должно указывать продолжительность времени, в течение которого обязательства должны соблюдаться. Когда организация является процессором, соглашение о конфиденциальности в любой форме между организацией, ее сотрудниками и ее агентами должно обеспечивать соблюдение сотрудниками и агентами политики и процедур, касающихся обработки и защиты данных.

(c) принимает все необходимые меры в соответствии со ст. 32 GDPR;

(d) соблюдает условия, указанные в пар. 2 и 4, для привлечения иного процессора;

Организация должна привлекать субподрядчика к обработке персональных данных только в соответствии с контрактом с клиентом.

Если организация заключает с другой организацией субподряд на обработку персональных данных частично или полностью, необходимо получить письменное разрешение клиента до обработки персональных данных субподрядчиком. Это может быть сделано в виде соответствующих условий в контракте с клиентом или особого «разового» соглашения. Организация должна иметь письменный контракт с любым субподрядчиком, которого она привлекает от своего имени, и должна удостовериться, что их контракты с субподрядчиками предусматривают внедрение необходимых средств управления.

Контракт может определять обязанности каждой стороны по-разному, но чтобы соответствовать данному документу, все средства управления должны быть рассмотрены и включены в документируемую информацию.

(e) принимая во внимание характер обработки, по мере возможности содействует контролёру посредством соответствующих технических и организационных мер в выполнении его обязанности отвечать на запросы субъекта данных касательно осуществления его прав, упомянутых в Главе III GDPR;

(f) принимая во внимание характер обработки и информацию, находящуюся в распоряжении процессора, оказывает содействие контролёру в выполнении обязательств, изложенных в ст. 32-36 GDPR;

(g) по выбору контролёра, удаляет или возвращает все персональные данные контролёру после окончания оказания услуг по обработке, и удаляет существующие копии, если право Союза или государств-членов не требует хранения персональных данных;

Информация, необходимая клиенту, может включать информацию о том, допускает ли организация аудиторские проверки, проводимые клиентом или другим аудитором, которые уполномочены или иным образом согласованы с заказчиком, и способствуют ли они проведению аудитов.

(h) предоставляет контролёру всю необходимую информацию, чтобы продемонстрировать соблюдение обязательств, изложенных в настоящей статье, а также разрешает и вносит свой вклад в аудиты, в том числе проверки, проводимые контролёром или иным аудитором, назначенным контролёром.

Контролер данных принимает следующие решения:

- какая организация в первую очередь собирает данные и имеет для этого законные основания;
- с какой целью будут использованы персональные данные;
- нужно ли разглашать данные и если да, то кому именно;
- применяются ли права доступа субъектов и других лиц, а также есть ли исключения;
- как долго хранить данные и нужно ли менять их способом, который не предусмотрен правилами.

Оператор данных принимает следующие решения:

- какие методы используются, чтобы собирать и хранить персональные данные;
- как защищены данные;
- какие средства используются, чтобы передавать персональные данные от одной организации к другой;
- как происходит сбор персональных данных;
- какой метод применяется, чтобы обеспечить соблюдение графика хранения;
- как происходит удаление персональных данных.

В законодательстве не установлено содержание DPA, однако на практике он может включать следующее:

(1) Основные положения «введение и определения». В ней указываются наименования сторон. Определения чаще всего соответствуют стандартам GDPR. В качестве примеров может быть DPA, GDPR, персональные данные, субъект данных, утечка персональных данных. Перечень определений зависят от содержания DPA.

(2) «Общая информация» / «Сведения об обработке данных».

В этом разделе содержится информация про цели обработки (*например, для использования услуг процессора, таких как обработка заработной платы, платежные транзакции или услуги электронной почты*), предмет/характер/типы обрабатываемых данных, объем соглашения, продолжительность обработки, категории субъектов данных.

(3) «Обязанности процессора». Дополнительно должно быть указано контактное лицо со стороны процессора, с которым контролер может связаться. Процессор должен выполнять любые запросы контролера на исправление или удаление. Все персональные данные, обрабатываемые от имени контролера, должны быть удалены по окончании действия соглашения или по требованию контролера. Процессор должен принять соответствующие меры по защите данных. Любые персональные данные, предоставленные процессору, должны использоваться только для указанной цели.

Процессоры не могут хранить, продавать или передавать персональные данные, предоставленные в соответствии с настоящим соглашением, без разрешения контролера.

(4) «Обязанности и права контролера».

Контролер соблюдает все применимые к нему законы о защите данных. Он уполномочен разрешать процессору выполнять свои обязательства и осуществлять свои права. Любые дополнительные инструкции или изменения в DPA потребуют отдельного и предварительного письменного соглашения.

(5) «Технические и организационные меры безопасности».

(6) «Запросы субъектов данных». В этом разделе разъясняется обязанность процессора отвечать на прямой запрос субъекта данных или контролера для осуществления прав на основании GDPR.

(7) «Права на аудит». Этот пункт оставляет за собой право проводить аудиты и получать подтверждение соответствие процессора. Процессор имеет право устанавливать любые разумные ограничения в отношении аудита, такие как обязанность соблюдения конфиденциальности или временные ограничения.

(8) «Субпроцессоры». Это еще один важный пункт в DPA, который подтверждает, может ли быть назначен субпроцессор. Он также определяет, что все субпроцессоры будут иметь те же обязанности, что и процессор, включая реализацию мер безопасности.

(9) «Передача данных». В этом разделе указывается, что передача данных будет осуществляться за пределы государств-членов ЕС. Она должна осуществляться в соответствии с решением о достаточности или стандартными договорными условиями между экспортером и импортером данных. Это гарантирует, что данные субъекта будут надежно защищены даже в случае передачи в третьи страны.

(10) «Удаление или возврат полученных персональных данных». Этот раздел определяет, что происходит с персональными данными после истечения срока действия или прекращения действия DPA.

За несоблюдение требований GDPR установлена ответственность. Каждый надзорный орган должен располагать следующими корректирующими полномочиями:

(a) выдавать предупреждения контролёру или процессору о том, что запланированная обработка данных может нарушать положения Регламента;

(b) делать предупреждения контролёру или процессору, если обработка данных нарушила положения Регламента;

(c) потребовать от контролёра или процессора удовлетворения запроса субъекта данных относительно осуществления его прав согласно Регламенту;

(d) потребовать, при необходимости, от контролёра или процессора приведения процесса обработки данных в соответствие с положениями Регламента в установленном порядке и в установленный срок;

(e) потребовать, чтобы контролёр сообщил субъекту данных о нарушении безопасности персональных данных;

(f) наложить временное или окончательное ограничение на обработку данных, включая запрет обработки;

(g) потребовать исправления или уничтожения персональных данных, или ограничения обработки, а также уведомления об указанных действиях получателей, которым были раскрыты персональные данные.

(h) отозвать сертификат, или потребовать от сертификационного органа отзыва сертификата, или потребовать, чтобы сертификационный орган не выдавал сертификат, если требования для сертификации не выполняются или больше не выполняются;

(i) наложить административный штраф в дополнение к мерам, указанным в этой части, или вместо них, в зависимости от обстоятельств каждого отдельного случая;

(j) потребовать приостановить передачу данных получателю в третьей стране или международной организации.

В качестве примеров реализации привлечения к ответственности можно назвать следующие кейсы.

Одним из самых больших штрафов был штраф компании Meta Platforms Ireland Ltd (материнская компания Facebook и Instagram) от Комиссии по защите данных Ирландии в 2023 году в размере 1,2 млрд. евро за передачу данных в США. Основания получения штрафа – это передача персональных данных европейских пользователей Facebook в Соединенные Штаты без достаточной защиты, а также недостаточность мер защиты конфиденциальности детей. В результате расследования было установлено, что компания сознательно игнорировала решение Суда Правосудия Европейского Союза (CJEU) о недостаточности применения Стандартных контрактных условий (SCC) как надежного инструмента для передачи персональных данных в США и продолжала их использовать, тем самым, делая персональные данные объектом доступа и контроля со стороны разведывательных органов США.

Еще один из самых больших штрафов в размере 746 млн евро был наложен на Amazon Europe Национальной комиссией по защите данных Люксембурга (CNPD). Надзорный орган установил, что интернет-магазин не получал согласия пользователей перед сохранением рекламных файлов cookie. Штраф в размере 406 млн. евро также был наложен на компанию Instagram за нарушение конфиденциальности детей.

Часто размер штрафа составляется из нескольких отдельных, назначенных за разные нарушения. Если надзорный орган одновременно узнает о нескольких независимых нарушениях, за каждое из них назначают отдельный штраф, который рассчитывается индивидуально.

В ст. 83 GDPR указано, что каждый надзорный орган должен гарантировать, что наложение административного штрафа за нарушения GDPR, в каждом индивидуальном случае является эффективным, соразмерным и сдерживающим. Административные штрафы накладываются в зависимости от обстоятельств каждого индивидуального случая. При решении вопроса о наложении административного взыскания и установлении его размера, в каждом индивидуальном случае необходимо принимать во внимание:

(a) характер, тяжесть и продолжительность нарушения с учетом характера, объема или цели обработки, количества пострадавших субъектов данных и размера причиненного им вреда;

Например, Facebook допустил утечку личной информации 533 млн пользователей, которые могли стать субъектами мошенничества, рассылки спама, фишинга, смишинга, и риски были высокими. Нарушение продолжалось дольше года. Поэтому надзорный орган посчитал такой ущерб значительным и определил штраф в размере 256 млн евро.

(b) преднамеренный или непреднамеренный характер нарушения;

В деле Facebook надзорный орган решил, что отсутствие технических и организационных мер в IT-системе социальной сети было небрежностью.

(c) любые действия, предпринятые контролёром или процессором для уменьшения ущерба, причиненного субъектами данных;

Facebook сразу предпринял меры и снизил вероятность дальнейшего массового парсинга личных данных пользователей.

(d) степень ответственности контролёра или процессора, учитывая предпринятые ими технические и организационные меры согласно ст. 25 и 32 GDPR;

(e) любые относящиеся предыдущие нарушения со стороны контролёра или процессора;

В деле Facebook установлено, что аналогичных нарушений не было, и этот фактор стал смягчающим.

(f) степень сотрудничества с надзорным органом в целях устранения нарушения и смягчения возможных негативных последствий нарушения;

(g) категории персональных данных, пострадавших в результате нарушения;

Категории персональных данных, которые стали общедоступными через платформу Facebook, включали мобильные номера телефонов, имена, пол, местонахождение, род занятий и семейное положение пользователей. Эта личная информация по своему характеру несет риск нарушения прав субъектов данных, например риск мошенничества. Парсеры могли объединить те данные, которые стали общедоступными по вине социальной сети, и те, которые были размещены пользователями в открытых аккаунтах. Это увеличивает риски мошенничества и учитывается надзорным органом как отягчающий фактор.

(h) каким образом надзорный орган узнал о нарушении, в частности, уведомил ли контролёр или процессор о нарушении и, если уведомил, то в какой степени;

(i) исполнение мер, упомянутых в статье 58(2), по тому же самому делу, если таковые ранее применялись в отношении контролёра или процессора;

(j) соблюдение утвержденных кодексов поведения или утвержденных механизмов сертификации;

(k) любые другие отягчающие или смягчающие факторы, применимые к обстоятельствам дела, такие как приобретенные прямо или косвенно благодаря нарушению финансовые выгоды, или предотвращенные убытки.

Если в пределах одной и той же обработки или же нескольких связанных друг с другом операций обработки контролёр или процессор умышленно или по неосторожности нарушает несколько положений GDPR, общая сумма

административного штрафа не должна превышать сумму штрафа за наиболее серьезное нарушение. Нарушение GDPR влечет административный штраф в размере до 10 000 000 Евро, а в случае субъекта хозяйствования – до 2% от общего годового мирового оборота за предыдущий финансовый год, в зависимости от того, что выше:

(a) обязанностей контролёра и процессора, упомянутых в ст. 8 (согласие ребенка), 11 (судимости и правонарушения), 25 -39 (взаимодействие контролера и процессора), 42 и 43 GDPR (сертификация);

(b) обязанностей сертифицирующего лица, упомянутых в ст. 42 и 43 GDPR;

(c) обязанностей контролирующего органа в соответствии со статьей 41(4) GDPR.

Нарушение следующих положений подлежит согласно пар. 2 административному штрафу в размере до 20 000 000 Евро, а в случае субъекта хозяйствования – до 4% от общего годового мирового оборота за предыдущий финансовый год, в зависимости от того, что выше:

(a) основных принципов обработки, в том числе условий согласия в соответствии со ст. 5, 6, 7 и 9 GDPR;

(b) прав субъектов данных согласно ст. 12-22 GDPR;

(c) передачи персональных данных получателю в третьей стране или международной организации согласно ст. 44-49 GDPR;

(d) любых обязательств согласно законодательству государства-члена, принятому в соответствии с гл. IX;

(e) невыполнение предписания, временного или постоянного ограничения на обработку либо на приостановку передачи данных, изданного надзорным органом или неспособность обеспечить доступ в нарушение ст. 58(1).

Невыполнение предписания надзорного органа, о котором говорится в ст. 58 (2), подлежит административному штрафу в размере до 20 000 000 Евро, а в случае субъекта хозяйствования – до 4% от общего годового мирового оборота за предыдущий финансовый год, в зависимости от того, что выше.

Каждое государство-член может установить правила о том, могут ли накладываться и, если да, то в какой степени, административные штрафы на государственные органы и агентства, созданные в этом государстве-члене.

Санкции (в том числе административные штрафы) должны налагаться за любое нарушение GDPR, в дополнение или вместо соответствующих мер, налагаемых надзорным органом согласно GDPR. В случае если нарушение незначительное или если наложение штрафа несоразмерно нарушению физического лица, вместо штрафа может быть объявлен выговор. При его наложении следует принимать во внимание характер, тяжесть и продолжительность нарушения, преднамеренный характер нарушения, меры, принятые для смягчения нанесенного ущерба, степень ответственности или любые другие ранее совершенные нарушения, способ, посредством которого надзорному органу стало известно о нарушении, соблюдение мер, принятых в отношении контролёра или процессора, соблюдение кодексов поведения, а также любые иные отягчающие или смягчающие вину обстоятельства.

Когда административные штрафы налагаются на физических лиц, которые не являются субъектами хозяйствования, надзорный орган при определении размера штрафа должен принять во внимание общий уровень дохода лица в государстве-члене, а также его материальное положение.

Правовая система Дании и Эстонии не предусматривает административных штрафов. Эти нормы об административных штрафах могут применяться таким образом, что в Дании штраф налагается компетентными национальными судами в качестве уголовной санкции, в Эстонии штраф налагается надзорным органом в рамках процедуры по делам о менее тяжких преступлениях (мисдиминор), при условии, что применение норм в указанных государствах-членах имеет воздействие, равноценное применению административных штрафов, налагаемых надзорными органами. Вследствие этого компетентные национальные суды должны учитывать рекомендации надзорного органа, инициировавшего наложение штрафа.

Еще несколько примеров штрафов. Комиссия по защите данных применила штраф к китайской компании TikTok на сумму 345 милл. евро после того, как в ходе расследования выяснилось, что платформа незаконно обрабатывала персональные данные детей и делала их публичными через открытые профили пользователей и видеоролики. Кроме всего прочего, функционал, предназначенный для того, чтобы позволить родителям контролировать активность своих детей, имел недостаточные меры проверки, которые были легко обойти, а политика конфиденциальности и практика обработки данных TikTok были слишком сложными и запутанными для молодых пользователей, не предоставляя им значительного контроля над своими данными.

Французский контролирующий орган (CNIL) принял решение о применении штрафных санкций к компании CRITEO, специализирующейся на «поведенческом ретаргетинге», который заключается в отслеживании активности пользователей Интернета с целью показа персонализированной рекламы. Компания не соблюдала положений GDPR в части получения согласия на обработку персональных данных и возможности его отзыва (ст. 7(1), (3), 17(1) GDPR), требований предоставления информации о обработке персональных данных в понятной форме (ст. 12 и 13 GDPR) и реализации права на получение доступа к персональным данным (ст. 15(1) GDPR). Общая сумма штрафа составила 40 млн. евро.

В начале 2023 года Комиссия по защите данных Ирландии оштрафовала WhatsApp на 5,5 миллиона евро. Штраф был наложен после жалобы субъекта данных на то, как приложение просило пользователей согласиться с его обновленными условиями обслуживания после вступления в силу GDPR. В случае отказа они больше не смогут получить доступ к услуге, и соответствующий субъект данных утверждал, что пользователи были вынуждены дать согласие на обработку их персональных данных. В результате расследования было установлено, что компания WhatsApp не предоставляла пользователям право выбора при принятии обновленных условий, а

предоставляла их как неподлежащее обсуждению условие для дальнейшего использования своих услуг, фактически заставляя пользователей соглашаться на расширенную практику обмена данными. Это нарушило требование GDPR о свободно предоставленном информированном согласии. Кроме того, было установлено, что условия обслуживания и политика конфиденциальности были признаны слишком сложными и длинными, так как они не предоставили пользователям четкую и понятную информацию о последствиях принятия новых положений об обмене данными.

В 2023 году Шведское агентство по защите данных оштрафовало веб-плеер цифровой музыки и подкастов Spotify на сумму 5,4 миллиона долларов за нарушение правил прозрачности, установленных GDPR. В результате расследования было выявлено, что Spotify отвечает на запросы доступа к данным, не информируя клиентов о том, как компания использует их данные. В пресс-релизе агентства по конфиденциальности указывается, что Spotify должен быть «точнее» в раскрытии данных и сделать так, чтобы клиенты, запрашивающие доступ, имели возможность понять, как Spotify использует их данные. И хотя выявленные недочеты в целом считаются незначительными, в свете количества зарегистрированных пользователей и оборота Spotify, агентство применило штраф именно в таком размере против Spotify.

ЛЕКЦИЯ 5. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ БЕЛАРУСЬ

История регулирования персональных данных была до принятия Закона «О защите персональных данных». Основные нормативные правовые акты в сфере защиты персональных данных были Закон Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации», Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных», приказы Оперативно-аналитического центра при Президенте Республики Беларусь, иные акты законодательства.

История развития персональных данных может включать несколько этапов.

1 этап. Охрана отдельных категорий персональных данных осуществлялась в рамках тайны переписки и информации о частной жизни.

На первоначальных этапах развития государственности на белорусских землях вопросам защиты личной информации особого внимания не уделялось. Первые упоминания об отдельных аспектах данного права появляются в Конституции БССР 1937 года в виде закрепления права граждан на тайну переписки. В ст. 54 Конституции БССР 1978 года предусматривалось, что личная жизнь граждан, тайна переписки, телефонных переговоров и телеграфных сообщений охраняется законом.

Конституция 1994 года в ст. 28 предусматривала, что каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от

посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

КоАП 1984 года, действовавший в это время, не предусматривал ответственности за незаконные действия с персональными данными или информацией о частной жизни. В целом вопрос о защите личных данных с учетом решаемых на этом историческом этапе задач в государстве не находился среди приоритетных.

2 этап. Регламентация действий с личной информацией в рамках законодательства об информатизации и отраслевых актов, регулирующих функционирование отдельных информационных ресурсов.

Важным моментом в развитии рассматриваемого института законодательства стало принятие Закона Республики Беларусь от 06.09.1995 г. № 3850-XII «Об информатизации». Хотя в Законе отсутствовал термин «персональные данные», однако был термин «информация о гражданах». В ст. 12 устанавливалось, что органы государственной власти, физические и юридические лица в пределах своей компетенции собирают, обрабатывают, хранят документированную информацию о гражданах и используют ее для выполнения возложенных на них функций и задач. В соответствии со ст. 21 физическим и юридическим лицам предоставлялись права: (1) на доступ к документированной информации о них; (2) на уточнение этой документированной информации в целях обеспечения ее полноты и точности; (3) оспаривать эту документированную информацию в установленном законодательством порядке; (4) знать, кто и в каких целях накапливает или использует документированную информацию о них.

В КоАП 2003 года по-прежнему отсутствовали нормы об ответственности за нарушения, связанные с персональными данными или информацией о частной жизни. В КоАП в ст. 22.13 предусматривалась ответственность за разглашение коммерческой или иной тайны.

Фактически первым белорусским законодательным актом, в котором упоминались персональные данные, стала Инструкция Министерства внешних экономических связей Республики Беларусь от 25 сентября 1992 г. № 06/14 «О порядке использования туристических ордеров/ваучеров предприятиями и организациями Республики Беларусь». На уровне законодательного акта рассматриваемый термин впервые целенаправленно употреблен в Указе Президента Республики Беларусь от 6 апреля 1999 г. № 195 «О некоторых вопросах информатизации в Республике Беларусь». Данным Указом была утверждена концепция государственной политики в области информатизации, которой предусматривалось, что для органов государственного управления в сфере информатизации приоритетными являются ряд направлений деятельности, в том числе защита персональных данных.

В Законе «Об информации, информатизации и защите информации» информация о частной жизни физического лица и персональные данные были отнесены к информации, распространение и (или) предоставление которой ограничено, хотя самого определения персональных данных не содержалось.

Предусматривалось, что никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами.

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими должны были осуществляться с согласия данного физического лица, если иное не установлено законодательными актами. Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь. Последующая передача персональных данных разрешалась только с согласия физического лица, к которому они относились, либо в соответствии с законодательными актами.

Такие меры должны были приниматься до уничтожения персональных данных, либо до их обезличивания, либо до получения согласия физического лица, к которому эти данные относились, на их разглашение.

В Законе «О регистре населения» персональные данные физических лиц определялись как совокупность основных и дополнительных персональных данных, а также данных о реквизитах документов, подтверждающих основные и дополнительные персональные данные конкретных физических лиц. К основным персональным данным отнесены, например, (1) идентификационный номер; (2) фамилия, собственное имя, отчество; (3) пол; (4) число, месяц, год рождения; (5) место рождения; (6) цифровой фотопортрет; (7) данные о гражданстве (подданстве).

Несмотря на отсутствие четких признаков персональных данных, многие на практике восприняли это положение законодательства как определение персональных данных. НЦЗПД полагает, что данная норма в силу узости своего содержания не могла выступать в качестве обозначения «персональных данных». На данном этапе в законодательных актах постепенно начинают появляться нормы, связанные с обработкой персональных данных.

4 января 2014 г. в Закон «Об информации, информатизации и защите информации» включено дополнение, в котором впервые предпринята попытка дать универсальное определение персональных данных. Под персональными данными было предложено понимать основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. Определение стало не соответствовать термину в Законе «О регистре населения», отнеся к персональным данным любую информацию, которая позволяет идентифицировать лицо.

Но наряду с плюсами указанное определение сохраняло и очевидные недостатки. Использование словосочетания «позволяющие идентифицировать лицо», исходя из складывавшейся практики его применения, оставляло за

рамками рассматриваемого понятия случаи, когда сами по себе данные лицо не идентифицируют, но вместе с иной имеющейся информацией позволяют его идентифицировать. Иными словами, все варианты косвенной идентификации оказались вне рамок правовой защиты. С принятием данного Закона стало возможным обрабатывать персональные данные не просто с согласия лица, а лишь с согласия в письменном виде, что, видимо, было призвано повысить защищенность прав граждан.

В 2018 году в ст. 22.13 КоАП внесены изменения, в соответствии с которыми установлена ответственность за умышленное незаконное разглашение персональных данных лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью.

3 этап. Формирование комплексного института законодательства о персональных данных.

Данный этап можно обозначить как принятие Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (Закон).

В 2022 году в новой редакции Конституции наряду с правом на защиту частной жизни предусмотрено и право на защиту персональных данных. Тем самым, фактически, признан самостоятельный характер данного права по отношению к праву на защиту частной жизни.

Новая редакция КоАП, принятая в 2021 году, предусмотрела ст. 23.7, устанавливающую ответственность за нарушение законодательства о персональных данных. В ней закреплена ответственность как для физического, так и для юридического лица, а максимальный размер штрафа в случае незаконного распространения персональных данных составляет 200 базовых величин.

В 2021 году Уголовный кодекс дополнен двумя самостоятельными составами (ст. 203-1 и 203-2), предусматривающими ответственность за незаконные действия в отношении персональных данных и за несоблюдение мер обеспечения их защиты.

Упоминание персональных данных невозможно без упоминания Закона «Об информации, информатизации и защите информации». В ст. 18 указано, что никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами.

Сбор, обработка, хранение, предоставление, распространение информации о частной жизни физического лица, а также пользование ею и обработка персональных данных осуществляются с согласия данного физического лица, если иное не установлено законодательными актами.

Важно, что в ст. 3 Закона в случае, если законодательным актом, устанавливающим правовой режим охраняемой законом тайны, предусматриваются особенности обработки персональных данных, входящих в

состав охраняемой законом тайны, применяются положения этого законодательного акта, что закрепляет разграничение применения Закона и Закона «Об информации, информатизации и защите информации». Если не применяется Закон, то будет применяться Закон «Об информации, информатизации и защите информации».

Взаимодействие рассматриваемых правовых режимов можно представить в следующем виде:

когда законодательным актом, устанавливающим правовой режим охраняемой законом тайны, и принятыми в его развитие актами конкретный вопрос не регулируется – применяются положения Закона.

когда законодательным актом, устанавливающим правовой режим охраняемой законом тайны, и принятыми в его развитие актами предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, – применяются положения Закона «Об информации, информатизации и защите информации».

Особенности обработки персональных данных имеют место в том случае, когда Закон и Закона «Об информации, информатизации и защите информации», устанавливающий правовой режим охраняемой законом тайны, а также принятые в его развитие акты по-разному регулируют один и тот же вопрос.

Это, например, могут быть: различный круг оснований для обработки персональных данных; различный круг органов и организаций, которые имеют право на получение персональных данных; различные подходы к объему персональных данных, необходимых для достижения определенной цели; различные требования к форме и содержанию согласия на обработку персональных данных; различные подходы к срокам хранения персональных данных.

Так, постановлением Правления Национального банка Республики Беларусь от 22 июня 2018 г. № 291 «О формировании кредитных историй и предоставлении кредитных отчетов» утверждена форма согласия на предоставление кредитного отчета, содержание которой существенно отличается по сравнению с требованиями ст. 5 Закона (не предусматривается предоставление всей информации, указанной в данной статье, и др.). Поскольку рассматриваемое постановление принято в развитие законодательного акта, устанавливающего правовой режим охраняемой законом тайны (Банковского кодекса Республики Беларусь), подлежат применению нормы данного постановления, а не положения ст. 5 Закона.

Появление отдельного Закона, посвященного защите персональных данных, и увеличение числа нормативных правовых актов, регулирующих различные аспекты обработки персональных данных, обусловили необходимость внесения в Единый правовой классификатор Республики Беларусь, утвержденный Указом Президента Республики Беларусь от 4 января 1999 г. № 1, самостоятельной позиции 10.03.08.05 «Персональные данные и их защита». Уполномоченный орган по защите прав субъектов персональных данных – Национальный центр защиты персональных данных Республики

Беларусь (НЦЗПД), который был создан Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты. Его возглавляет директор, который назначается на должность и освобождается от должности Президентом Республики Беларусь по представлению начальника Оперативно-аналитического центра при Президенте Республики Беларусь.

Основными задачами Национального центра защиты персональных данных являются:

принятие мер по защите прав субъектов персональных данных при обработке их персональных данных;

организация обучения по вопросам защиты персональных данных.

НЦЗПД выполняет следующие функции:

– осуществляет контроль за обработкой персональных данных операторами (уполномоченными лицами);

– рассматривает жалобы субъектов персональных данных по вопросам обработки персональных данных;

– определяет перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

– выдает разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, а также определяет порядок выдачи таких разрешений;

– вносит предложения о совершенствовании законодательства о персональных данных, участвует в подготовке проектов актов законодательства о персональных данных;

– дает разъяснения по вопросам применения законодательства о персональных данных, проводит иную разъяснительную работу о законодательстве о персональных данных;

– определяет случаи, когда не требуется уведомления Национального центра защиты персональных данных о нарушениях систем защиты персональных данных;

– устанавливает классификацию содержащих персональные данные информационных ресурсов (систем) в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных;

– участвует в работе международных организаций по вопросам защиты персональных данных;

– осуществляет сотрудничество с органами (организациями) по защите прав субъектов персональных данных в иностранных государствах;

– ежегодно не позднее 15 марта публикует в средствах массовой информации отчет о своей деятельности;

– реализует образовательные программы дополнительного образования взрослых в соответствии с законодательством об образовании;

– осуществляет иные полномочия, предусмотренные законодательством о персональных данных.

НЦЗПД имеет право:

– при осуществлении контроля запрашивать и получать на безвозмездной основе от государственных органов, юридических лиц Республики Беларусь, иных организаций и физических лиц информацию, необходимую для определения законности действий (бездействия) операторов (уполномоченных лиц) по обработке персональных данных (в том числе персональные данные физических лиц без их согласия). Информация представляется в течение 10 календарных дней со дня поступления запроса;

– при осуществлении контроля безвозмездно пользоваться информационными ресурсами (системами), в том числе иметь к ним доступ, включая удаленный, получать из них сведения, в том числе содержащие банковскую, коммерческую, профессиональную и иную охраняемую законом тайну, а также персональные данные физических лиц без их согласия, за исключением информационных ресурсов (систем), содержащих государственные секреты, на основании письменных запросов, запросов в виде электронных документов либо соглашений (договоров), заключенных с собственниками (владельцами) информационных ресурсов (систем);

– безвозмездно пользоваться информационными и (или) электронными услугами, оказываемыми государственными органами, юридическими лицами Республики Беларусь и иными организациями, на основании соглашений (договоров), заключенных с субъектами, оказывающими такие услуги;

– проводить в отношении операторов (уполномоченных лиц) при обработке ими персональных данных проверки на предмет соблюдения законодательства о персональных данных;

– требовать от операторов (уполномоченных лиц) изменения, блокирования или удаления недостоверных или полученных незаконным путем персональных данных, устранения иных нарушений законодательства о персональных данных;

– требовать от операторов (уполномоченных лиц) прекращения обработки персональных данных, если иными способами невозможно обеспечить защиту прав субъектов персональных данных;

– принимать по вопросам, входящим в его компетенцию, решения, обязательные для исполнения государственными органами, юридическими лицами Республики Беларусь, иными организациями и физическими лицами, осуществляющими деятельность по обработке персональных данных;

– привлекать работников государственных органов, иных государственных организаций по согласованию с их руководителями, а также физических лиц на договорной основе для решения вопросов, относящихся к компетенции Национального центра защиты персональных данных;

– проводить на договорной основе добровольный аудит соблюдения операторами (уполномоченными лицами) требований законодательства о персональных данных;

– использовать государственные средства связи и коммуникации;

– организовывать и осуществлять международное сотрудничество по вопросам, входящим в его компетенцию;

– заключать в пределах своей компетенции договоры с государственными органами, юридическими лицами Республики Беларусь, иными организациями и физическими лицами, а также с органами и организациями иностранных государств, международными организациями и межгосударственными образованиями;

– заниматься приносящей доходы деятельностью;

– осуществлять иную не запрещенную законодательством деятельность, направленную на реализацию своих основных задач и функций.

В целях оказания НЦЗПД содействия в реализации возложенных на него функций при нем создается на общественных началах консультативный совет. Персональный состав консультативного совета, порядок его организации и функционирования устанавливаются директором НЦЗПД.

НЦЗПД вправе осуществлять контроль в форме плановых, внеплановых и камеральных проверок:

Камеральные проверки проводятся по месту своего нахождения посредством изучения, анализа и оценки (1) информации, размещенной в средствах массовой информации и глобальной компьютерной сети Интернет; (2) документов и иной информации, в том числе полученной от оператора (уполномоченного лица) по запросу НЦЗПД. Они проводятся без выдачи предписания на их проведение и уведомления об этом оператора (уполномоченного лица). По результатам такой проверки оператору (уполномоченному лицу) могут быть направлены рекомендации об устранении выявленных нарушений законодательства о персональных данных.

Плановые проверки проводятся в соответствии с планом проверок соблюдения законодательства о персональных данных, ежегодно утверждаемым директором НЦЗПД, размещаемом на официальном сайте в глобальной компьютерной сети Интернет не позднее 30 декабря года, предшествующего году проведения проверки. Плановые проверки одного и того же оператора (уполномоченного лица) проводятся с периодичностью не чаще одного раза в два года. Операторы (уполномоченные лица), имеющие положительное заключение НЦЗПД по итогам проведения добровольного аудита соблюдения требований законодательства о персональных данных, не подлежат плановым проверкам в течение 5 лет со дня получения соответствующего заключения.

Внеплановые проверки проводятся без включения в план проверок. Они могут назначаться директором Национального центра защиты персональных данных при наличии сведений, в том числе полученных от организации или физического лица, жалоб субъектов персональных данных, свидетельствующих о совершаемом (совершенном) нарушении требований законодательства о персональных данных. Анонимная информация не является основанием для назначения внеплановых проверок.

Срок проведения плановой и внеплановой проверки не может превышать 20 рабочих дней. Указанный срок может быть продлен директором однократно

не более чем на 10 рабочих дней. Для проведения проверки формируется комиссия по проверке и выдается предписание на ее проведение с указанием наименования оператора (уполномоченного лица), вида проверки (плановая или внеплановая), даты начала проверки, сроков ее проведения, состава комиссии, вопросов, подлежащих проверке. О назначении плановой проверки оператор (уполномоченное лицо) письменно уведомляется не позднее 10 рабочих дней до начала ее проведения. Уведомление должно содержать сведения о дате начала проверки, сроках ее проведения, составе комиссии, а также о вопросах, подлежащих проверке.

Проверочные мероприятия в рамках плановой или внеплановой проверки проводятся, как правило, в присутствии представителей проверяемого оператора (уполномоченного лица). В ходе плановой или внеплановой проверки оцениваются меры, принятые оператором (уполномоченным лицом) для обеспечения защиты персональных данных, а также их достаточность для защиты персональных данных. Методы и способы осуществления проверки руководитель комиссии определяет самостоятельно.

По результатам плановой или внеплановой проверки составляется акт в двух экземплярах, в котором должны быть отражены (1) соответствие (несоответствие) принятых оператором (уполномоченным лицом) мер по обеспечению защиты персональных данных требованиям законодательства о персональных данных; (2) экспертная оценка комиссией достаточности принятых оператором (уполномоченным лицом) мер для защиты персональных данных; (3) выявленные нарушения законодательства о персональных данных либо вывод об отсутствии таких нарушений.

Акт плановой или внеплановой проверки составляется в течение 10 рабочих дней со дня ее окончания и подписывается всеми членами комиссии. В течение 3 рабочих дней после составления акта первый его экземпляр направляется проверяемому оператору (уполномоченному лицу) или вручается его уполномоченному представителю, второй – остается в НЦЗПД.

В случае выявления по результатам плановой или внеплановой проверки нарушений законодательства о персональных данных, отраженных в акте плановой или внеплановой проверки, директор НЦЗПД в течение 10 рабочих дней со дня окончания проверки выносит письменное требование (предписание) об устранении выявленных нарушений и (или) приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе) с указанием конкретных действий, которые должны быть приостановлены (прекращены), и устанавливает срок такого устранения и (или) приостановления (прекращения), не превышающий 6 месяцев.

Требование (предписание) составляется в двух экземплярах. Первый экземпляр в течение 3 рабочих дней после его составления направляется проверенному оператору (уполномоченному лицу) или вручается его уполномоченному представителю, второй – остается в НЦЗПД.

О выполнении письменного требования (предписания) об устранении выявленных нарушений оператор (уполномоченное лицо) в сроки,

установленные в этом требовании (предписании), письменно сообщает в НЦЗПД с приложением подтверждающих документов, а также предоставляет возможность удостовериться (в том числе на месте) в устранении нарушений (при необходимости).

При наличии объективных обстоятельств, не позволивших устранить нарушения, указанные в письменном требовании (предписании), в установленные в нем сроки, по заявлению оператора (уполномоченного лица), поданному не позднее 3 рабочих дней до дня истечения этих сроков и отражающему соответствующие обстоятельства, сроки могут быть продлены. Решение о продлении указанных сроков или об отказе в этом принимается не позднее 2 рабочих дней со дня поступления заявления, о чем оператор (уполномоченное лицо) уведомляется в письменной форме в течение 2 рабочих дней со дня принятия решения.

Решение о возобновлении обработки персональных данных в соответствующих информационных ресурсах (системах) принимается директором НЦЗПД в течение 10 рабочих дней после устранения нарушений, послуживших основанием для вынесения письменного требования (предписания) о приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе), о чем оператор (уполномоченное лицо) уведомляется в письменной форме в течение 2 рабочих дней со дня принятия такого решения.

При наличии возражений по акту плановой или внеплановой проверки руководитель оператора (уполномоченного лица) или иной его уполномоченный представитель не позднее 15 рабочих дней со дня поступления акта оператору (уполномоченному лицу) или вручения его уполномоченному представителю представляет в НЦЗПД письменные возражения по его содержанию.

Обоснованность доводов, изложенных в возражениях, рассматривается не позднее 10 рабочих дней со дня их поступления. Результаты рассмотрения возражений отражаются в письменном заключении, которое направляется оператору (уполномоченному лицу) или вручается его уполномоченному представителю.

В случае признания возражений обоснованными составляется новый акт проверки и при необходимости отменяется (изменяется) соответствующее письменное требование (предписание).

Вынесенное по результатам плановой или внеплановой проверки письменное требование (предписание) об устранении нарушений и (или) приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе), а также действия (бездействие) проверяющих могут быть обжалованы оператором (уполномоченным лицом) в судебном порядке.

Субъекты персональных данных, полагающие, что их права, свободы и законные интересы нарушены при обработке персональных данных, вправе направить в НЦЗПД жалобу по вопросам обработки персональных данных. Она может быть направлена на действия (бездействие), которые непосредственно

затрагивают права, свободы и законные интересы субъекта персональных данных, подающего жалобу, в течение 3 месяцев со дня, когда о них стало известно лицу, направившему жалобу. Она подается в письменной форме или в виде электронного документа и должна содержать (1) фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания); (2) изложение сути жалобы с указанием действий (бездействия), которыми нарушаются права, свободы и законные интересы субъекта персональных данных; (3) информацию о принятых мерах по восстановлению нарушенных прав, свобод и законных интересов субъекта персональных данных (в том числе обращение к оператору (уполномоченному лицу), в суд, органы прокуратуры или иные государственные органы) или об отсутствии таких мер; (4) личную подпись субъекта персональных данных в случае направления жалобы в письменной форме. К жалобе прилагаются документы и иные материалы (в том числе фотографии, графические изображения экрана (скриншоты), подтверждающие нарушение прав, свобод и законных интересов субъекта персональных данных, подающего жалобу (при их наличии).

Жалоба оставляется без рассмотрения по существу, если она:

– не соответствует требованиям к ней;

– рассмотрена, рассматривается или подлежит рассмотрению в соответствии с законодательством о конституционном судопроизводстве, гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса, либо если в соответствии с законодательными актами установлен иной порядок подачи и рассмотрения такой жалобы.

Решение об оставлении жалобы без рассмотрения по существу принимается НЦЗПД в течение 10 рабочих дней со дня, следующего за днем ее регистрации, с уведомлением об этом субъекта персональных данных, подавшего жалобу, и указанием причин принятого решения. Они рассматриваются не позднее 1 месяца со дня, следующего за днем их регистрации. В случае, если жалоба требует дополнительного изучения и проверки, срок может быть продлен не более чем на 1 месяц с уведомлением об этом субъекта персональных данных, подавшего жалобу.

Если содержащиеся в жалобе сведения о нарушениях при обработке персональных данных подтверждаются, НЦЗПД принимает необходимые меры по защите нарушенных прав, свобод и законных интересов субъекта персональных данных, подавшего жалобу, и уведомляет его об этом. В случае, если содержащиеся в жалобе сведения о нарушениях при обработке персональных данных не подтверждаются, НЦЗПД оставляет такую жалобу без удовлетворения и информирует об этом субъекта персональных данных, подавшего жалобу, с разъяснением порядка обжалования такого решения. Принятые по результатам рассмотрения жалоб решения могут быть обжалованы в судебном порядке.

В случае поступления повторных жалоб, не содержащих новых обстоятельств, имеющих значение для их рассмотрения по существу, по таким жалобам с соответствующим субъектом персональных данных прекращается переписка с уведомлением его об этом. При поступлении повторных жалоб по вопросам, по которым с субъектом персональных данных прекращена переписка, такие жалобы рассмотрению не подлежат (без уведомления субъекта персональных данных).

В Указе указаны дополнительные обязанности. Собственники (владельцы) информационных систем и владельцы критически важных объектов информатизации, а также организации, осуществляющие лицензируемую деятельность по технической и (или) криптографической защите информации, обеспечивают:

– обучение в НЦЗПД не реже 1 раза в 3 года своих работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации;

– ежегодное до 15 ноября представление НЦЗПД информации о количестве работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, для повышения их квалификации.

Операторы (уполномоченные лица) организуют не реже одного раза в 5 лет прохождение обучения по вопросам защиты персональных данных лицами, ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных, в том числе:

– категориями лиц, определенными Оперативно-аналитическим центром при Президенте Республики Беларусь, – в НЦЗПД по образовательной программе повышения квалификации руководящих работников и специалистов;

– иными лицами:

в учреждениях образования, а также в иных организациях, которым предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов, по образовательной программе повышения квалификации руководящих работников и специалистов;

в других организациях по образовательной программе обучающих курсов (лекториев, тематических семинаров, практикумов, тренингов, офицерских курсов и иных видов обучающих курсов);

у оператора (уполномоченного лица) путем изучения установленных требований в области защиты персональных данных и проверки им знаний по вопросам защиты персональных данных (в форме собеседования, опроса, тестирования и других формах контроля знаний).

Операторы (уполномоченные лица) ежегодно до 15 ноября обеспечивают представление НЦЗПД информации о количестве лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных, а

также лиц, непосредственно осуществляющих обработку персональных данных, которым необходимо пройти обучение в НЦЗПД;

Обязанности операторов, являющихся государственными органами, юридическими лицами Республики Беларусь, иными организациями, устанавливают и поддерживают в актуальном состоянии:

а) перечень информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых они являются;

б) категории персональных данных, подлежащих включению в такие ресурсы (системы):

общедоступные персональные данные;

специальные персональные данные (кроме биометрических и генетических персональных данных);

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными;

в) перечень уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами;

г) срок хранения обрабатываемых персональных данных;

Операторы обязаны вносить в создаваемый НЦЗПД государственный информационный ресурс «Реестр операторов персональных данных» сведения об информационных ресурсах (системах), содержащих персональные данные, а также обеспечивать актуализацию соответствующих сведений.

Согласно Приказу НЦЗПД от 15.11.2021 № 12 «О классификации информационных ресурсов (систем)» информационные ресурсы (системы), содержащие персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных подразделяются на информационные ресурсы (системы), содержащие:

общедоступные персональные данные;

специальные персональные данные (кроме биометрических и генетических персональных данных);

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными.

Согласно Приказу НЦЗПД от 15.11.2021 № 13 «Об уведомлении о нарушениях систем защиты персональных данных» уведомление о нарушениях систем защиты персональных данных направляется оператором в НЦЗПД при нарушении систем защиты персональных данных.

Уведомление не направляется, если нарушение систем защиты не наступило следующих последствий:

– незаконному распространению, предоставлению персональных данных;

– изменению, блокированию либо удалению персональных данных без возможности восстановления доступа к ним.

– уведомление направляется оператором незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, в письменной форме или в виде электронного документа;

Уведомление излагается на белорусском или русском языке и содержит следующее:

– фамилию, собственное имя, отчество (если таковое имеется), адрес места жительства (места пребывания) оператора (физического лица) или полное наименование и место нахождения оператора (государственного органа, юридического лица Республики Беларусь, иной организации), а также номер телефона, адрес электронной почты (при наличии) оператора;

– фамилию, собственное имя, отчество (если таковое имеется), должность лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных оператора либо наименование соответствующего структурного подразделения (в отношении государственного органа, юридического лица Республики Беларусь, иной организации), его номер телефона и адрес электронной почты (при наличии);

– дату и время нарушения системы защиты персональных данных;

– дату и время, когда стало известно о произошедшем нарушении системы защиты персональных данных;

– описание нарушения системы защиты персональных данных;

– примерное количество субъектов персональных данных, затронутых нарушением;

– вероятные неблагоприятные последствия нарушения системы защиты персональных данных (потеря контроля над персональными данными, их хищение, нарушение прав и свобод субъектов персональных данных, чести, достоинства или деловой репутации, наступление убытков, разглашение охраняемой законом тайны, наступление иного существенного имущественного или иного вреда у субъектов персональных данных);

– меры, принятые или предлагаемые оператором для устранения нарушения системы защиты персональных данных;

– изменение или отзыв уведомления направляются по правилам, как направлялось само уведомление.

ЛЕКЦИЯ 6. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Анализ белорусского законодательства следует начать с понятия «персональных данных», закрепленного в ст. 1 Закона. «Персональные данные» – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано. Закон не предусматривает ограничений или требований к носителям информации для признания ее персональными данными: письменный или электронный носитель, видеоизображение, видеозапись.

В литературе есть два подхода: узкий и широкий.

Согласно узкому подходу, к персональным данным относиться только та информация, которая сама по себе достаточна для идентификации лица и обязательным должно быть фамилия, имя, отчество. Ввиду формирования большого количества баз данных, позволяющих сопоставлять и связывать воедино разрозненные блоки информации, выводится из-под правовой защиты множество ситуаций, связанных с обработкой личной информации.

Широкий подход – открытый перечень и отнесение максимально всех данных. Сторонники данного подхода отмечают, что при желании к персональным данным можно отнести практически любые сведения.

Таким образом, отмечается, что сужение определения делает его понятным и определенным, но выводит из-под правовой защиты многие бизнес-процессы, порожденные развитием информационных технологий (профилирование, прямой маркетинг и др.). Чрезмерное расширение может привести к созданию механизма всеобъемлющего регулирования всего имеющегося объема информации.

Для упрощения применения и нахождения баланса между широким и узким пониманием в Законе установлены признаки персональных данных: (1) это информация; (2) относимость к лицу; (3) возможность идентификации лица.

Информация относится к лицу, когда эта информация:

1) о каком-то лице (например, фото лица, история его болезни, обстоятельства рождения, место работы и др.);

2) не о самом лице, но она может быть использована для его оценки или влияния на поведение, реализации его прав и обязанностей (например, сведения GPS, определяющие место нахождения транспортного средства, могут быть использованы для оценки маршрута водителя, история звонков с рабочего телефона – для оценки использования средств связи нанимателя с работником в личных целях). Рассматриваемый признак исключает отнесение к персональным данным информации, когда такая информация является случайной по отношению к цели ее обработки и не может оказать влияния на субъекта персональных данных. Например, случайное изображение на фотографии, иллюстрирующей открытие нового магазина, транспортных средств с различимыми номерами. В данном случае целью обработки является не оценка владельца транспортного средства или оказание на него определенного влияния.

Соответственно, такие данные не должны признаваться персональными данными.

Иная ситуация, когда на специальном интернет-ресурсе размещаются фотографии автомобилей с различимыми номерами, которые демонстрируют нарушение автовладельцами правил дорожного движения (так называемые «доски позора»). Целью размещения таких фото как раз и является привлечение внимания к допущенному нарушению, оказание влияния на лицо в целях недопущения последующих нарушений. Кроме того, соответствующие данные могут использоваться и правоохранительными органами для привлечения владельца транспортного средства к ответственности. Поэтому в этом случае размещение фотографии транспортного средства следует рассматривать как обработку персональных данных. При решении вопроса о том, относится ли информация к конкретному лицу, следует учитывать различные обстоятельства, в том числе содержание информации, цель обработки и возможное влияние обработки на конкретного субъекта.

Не вся информация, которая касается лица или может оказать на него влияние, будет считаться персональными данными, а лишь та, на основании которой лицо идентифицировано или может быть идентифицировано. Идентифицированным является лицо, личность которого известна, которое однозначно выделено среди других лиц (мы на него указали, к нему можно обратиться, мы уже контактировали с данным лицом, знаем его и др.). Наиболее распространенным вариантом такой ситуации на сегодняшний день является указание ФИО лица в совокупности с другими данными, которые однозначно выделяют лицо среди других лиц. Например, Ковалев Михаил Александрович, который приходил на личный прием 15.02.2022 в 10.30 по вопросу незаконной перепланировки жилого помещения, или Ковалев Михаил, который проживает по адресу: г. Минск, ул. Руссиянова, 3-24. Но даже если неизвестно ФИО лица, то информация о нем может относиться к персональным данным как информация о физическом лице, которое может быть идентифицировано.

Физическое лицо, которое может быть идентифицировано, – физическое лицо, которое может быть прямо или косвенно определено, в частности, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности. Формулировка Закона предусматривает отнесение к персональным данным информации о лице, которое может быть определено прямо или косвенно.

Физическое лицо, которое может быть прямо определено, – это лицо, личность которого можно установить на основании той информации, которую мы рассматриваем, без использования дополнительных сведений. Например, заведующий кафедрой криминалистики юридического факультета БГУ, менеджер ООО «Астра» и номер его телефона, одинокий пенсионер, проживающий по адресу: ул. Никифорова, д. 18, кв. 47, лучший бомбардир

футбольного клуба «Минск» в 2020–2021 г., электрик Сергей Валерьевич из ЖЭС-110 и др.

Физическое лицо, которое может быть косвенно определено, – это лицо, личность которого нельзя установить на основании той информации, которую мы рассматриваем, но это можно сделать путем объединения имеющейся информации с иными сведениями, которыми мы располагаем или которые могут быть получены из других источников.

Например, в большинстве случаев имя и фамилия не являются уникальными (например, фамилию и имя Артем Иванов могут носить несколько десятков или даже сотен человек), то для определения конкретного лица может потребоваться получение дополнительной информации, например, даты и места рождения, номера телефона, адреса электронной почты и др.

Вместе с тем, знание места рождения, чаще всего, недостаточно для идентификации лица и может потребоваться дополнительная информация (например, место работы). Когда мы говорим о возможности получения дополнительной информации, речь идет о легальной возможности. При этом для признания сведений персональными данными реальная идентификация не требуется. Достаточно возможности идентификации.

Если идентификация лица зависит от объединения нескольких блоков информации, каждый из таких блоков в отдельности должен рассматриваться как персональные данные. Закон предусматривает ряд идентификаторов, наличие которых может свидетельствовать о возможности прямого или косвенного определения лица: ФИО, дата рождения, идентификационный номер, один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Так, например, к признакам, характерным для физической идентичности, могут относиться пол, рост, вес, цвет волос, состояние здоровья (например, дефект речи, инвалидность, фотографии, звукозаписи голосов и др.).

Об экономической идентичности может свидетельствовать владение транспортным средством, объектами недвижимости, уровень заработной платы, номер кредитной карточки и др.

Социальная идентичность может характеризоваться посредством ссылок на вероисповедание, национальность, политические взгляды, социальные связи, высказывания и комментарии, сексуальную ориентацию

Можно выделить и дополнительные сведения, которые используются для прямого или косвенного определения лица: номер телефона, почтовый адрес, адрес электронной почты, номер паспорта и дата его выдачи, история посещения сайтов, поисковые запросы, IP-адрес, идентификатор файла cookie и др.

Важно учитывать, что вопрос об отнесении сведений к персональным данным должен решаться в отношении конкретной ситуации. Информация, которая позволяет идентифицировать человека в одном контексте, может не идентифицировать человека в другом контексте. Например, имя Михаил Ковалев является весьма распространенным. Таких данных вполне достаточно

для идентификации лица в небольшом коллективе, например, классе или даже в школе, но явно недостаточно для идентификации лица среди всего населения города или страны. Когда информация публикуется в открытых источниках (например, открытая страница в социальных сетях), доступ к ней может получить любой человек.

В Законе закреплены категории персональных данных.

Под биометрическими персональными данными понимается информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое). В качестве примера могут быть отпечатки пальцев рук, ладоней, радужная оболочка глаза и иные подобные характеристики человека являются неповторимыми, по ним можно однозначно идентифицировать личность.

В качестве признаков можно отнести следующее:

информация должна характеризовать физиологические и биологические особенности человека (отпечатки пальцев рук, ладоней и другое);

информация используется для уникальной идентификации соответствующего лица, что предполагает наличие специальных технических средств, обеспечивающих уникальное сопоставление отпечатков пальцев и другого с имеющимся в базе образцом.

На практике весьма распространенной ошибкой является, например, отнесение к биометрическим персональным данным ксерокопий или отсканированных копий страниц паспортов, удостоверений с фотографиями. Так как не осуществляется уникальная идентификация субъекта (как правило, происходит просто визуальное сопоставление фотографии на документе и лица, предъявившего такой документ), то оснований для отнесения фотоизображений к биометрическим персональным данным нет. Иная ситуация, например, когда работнику выдается пропуск и при прохождении проходной с использованием специального программного обеспечения осуществляется распознавание лица посетителя и сопоставление его с образцом, сохраненным в базе данных. В такой ситуации имеет место обработка биометрических персональных данных.

В качестве биометрических персональных данных может использоваться голос.

Следующей категорией являются генетические персональные данные – информация, относящаяся к наследуемым либо приобретенным генетическим характеристикам человека, которая содержит уникальные данные о его физиологии либо здоровье и может быть выявлена, в частности, при исследовании его биологического образца. Они являются разновидностью специальных персональных данных, обработка которых может осуществляться лишь с согласия лица или по основаниям, предусмотренным ст. 8 Закона.

Информацией, содержащей генетические персональные данные, располагают организации здравоохранения, имеющие в своем составе специализированные лаборатории, осуществляющие молекулярно-генетические, цитогенетические (кариотипирование), молекулярно-

цитогенетические исследования. Объектом такого исследования является молекула ДНК (РНК).

Важно, сведения о состоянии здоровья пациента, содержащиеся в биологических образцах (кровь, слюна и т.д.), медико-генетических заключениях, медицинских справках о состоянии здоровья, которые содержат информацию о физиологии и здоровье человека, не обладают уникальностью и не относятся к генетическим персональным данным.

Еще одна категория – это общедоступные персональные данные. Под ними понимаются персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов. Выделение в отдельную категорию обусловлено возможностью фактически любого лица получить доступ к таким данным. Обработка таких персональных данных может быть на основании абз. 19 ст. 6 Закона без получения согласия субъекта персональных данных.

Закон выделяет два вида общедоступных персональных данных:

– распространенные самим субъектом персональных данных;

– с его согласия.

Для признания персональных данных общедоступными необходимо сочетание двух признаков:

– факт распространения данных, то есть действий, направленных на ознакомление с персональными данными неопределенного круга лиц, например, размещение информации на странице в LinkedIn.

– данные должны быть распространены самим субъектом или с его согласия. При использовании таких персональных данных следует фиксировать факт и источник получения таких данных. В конечном итоге использование оператором находящихся в свободном доступе данных всегда несет в себе элемент риска, поскольку именно на операторе в конечном итоге лежит бремя доказывания законности обработки персональных данных.

– распространенные в соответствии с требованиями законодательных актов. Для данного основания также необходимо сочетание двух признаков:

– распространение персональных данных;

– наличие законодательного акта, в соответствии с которым осуществляется распространение.

Например, Избирательным кодексом Республики Беларусь предусматривается опубликование деклараций о доходах кандидатов в Президенты Республики Беларусь. Законом Республики Беларусь «Об информации, информатизации и защите информации» закреплена необходимость указания на сайте государственного органа (организации) информации о руководителе, заместителе руководителя (должность, ФИО, номер служебного телефона).

Отдельная категория персональных данных – это специальные, касающиеся расовой либо национальной принадлежности, политических взглядов, членства в профессиональных союзах, религиозных или других убеждений, здоровья или половой жизни, привлечения к административной или

уголовной ответственности, а также биометрические и генетические персональные данные.

Закон выделяет две категории субъектов, которые обрабатывают персональные данные, – это оператор и уполномоченное лицо. От статуса зависит определение правовых оснований обработки, обязанности лиц, осуществляющих обработку персональных данных, в том числе перед субъектами персональных данных и уполномоченным органом по защите прав субъектов персональных данных, ответственность за нарушение Закона, а также правильная организация сотрудничества с другими организациями и физическими лицами, осуществляющими обработку персональных данных.

Определение статуса лица, осуществляющего обработку персональных данных, должно осуществляться в каждом конкретном случае с учетом анализа всех обстоятельств, связанных с обработкой персональных данных. При этом в смежных правоотношениях одно и то же лицо может выступать как оператор или уполномоченное лицо.

Оператор – это государственный орган, юридическое лицо Беларуси, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных.

Оператору присущи следующие признаки:

1. Статус.

В качестве оператора может выступать как организация, в том числе государственный орган, так и физическое лицо, осуществляющее обработку персональных данных, связанную с профессиональной или предпринимательской деятельностью, независимо от наличия либо отсутствия коммерческой выгоды от обработки персональных данных, а также от объема обрабатываемых персональных данных.

Физическое лицо признается оператором в случаях, когда такое лицо осуществляет обработку персональных данных в связи со своей деятельностью в качестве:

– индивидуального предпринимателя;

– лица, осуществляющего деятельность, направленную на получение прибыли, но не имеющего статуса индивидуального предпринимателя (ремесленник, адвокат, нотариус, лицо, осуществляющее деятельность по оказанию услуг в сфере агроэкотуризма, или иные виды деятельности, которые не относятся к предпринимательской деятельности в соответствии с ч. 4 п. 1 ст. 1 ГК).

Физические лица, осуществляющие обработку персональных данных в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью, не являются операторами, поскольку в соответствии с абз. 2 п. 2 ст. 2 Закона на такие отношения действие Закона не распространяется.

Например, физическое лицо осуществляет сбор персональных данных своих родственников для составления «генеалогического дерева» в личных

целях. Такая деятельность осуществляется для личного использования, не связана с профессиональной или предпринимательской деятельностью и, соответственно, действие Закона на нее не распространяется.

Физическое лицо ведет свою страницу в социальной сети, не монетизирует ее и размещает на ней фото- и видеоизображения, отражающие происходящие в его личной жизни события (фото с совместных мероприятий и др.). Такая деятельность не является профессиональной или предпринимательской деятельностью и, соответственно, действие Закона на нее не распространяется.

Неприменение Закона к обработке персональных данных в процессе исключительно личного, семейного, домашнего и иного подобного их использования не означает возможности бесконтрольного использования персональных данных других лиц. В данной ситуации будут применяться положения ч. 2 ст. 18 Закона «Об информации, информатизации и защите информации», согласно которой сбор, обработка, хранение, предоставление, распространение информации о частной жизни физического лица, а также пользование ею и обработка персональных данных осуществляются с согласия данного физического лица, если иное не установлено законодательными актами. При этом, если Закон не подлежит применению, то получение согласия осуществляется в любой форме, в том числе и устной, без необходимости предоставления информации, предусмотренной ст. 5 Закона;

2. Оператор организует и (или) осуществляет обработку персональных данных.

В качестве примера может быть наниматель при обработке персональных данных своих работников; учреждение образования при оказании образовательных услуг обучающимся; учреждение здравоохранения при оказании медицинской помощи пациентам; организация торговли при обработке персональных данных покупателей при реализации им товаров; страховщик по отношению к застрахованным лицам.

Использование союза «и (или)» предусматривает три варианта действия оператора.

В первой ситуации оператор определяет ключевые параметры обработки персональных данных (цели и сроки, объем обрабатываемых данных, круг лиц, которым предоставляются персональные данные). При этом непосредственно все действия по обработке персональных данных осуществляет уполномоченное лицо.

Во второй ситуации оператор не только организует, но и осуществляет обработку персональных данных (например, сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление и т.п.).

Например, организация занимается продажей мебели и ведет базу данных клиентов для осуществления рекламной рассылки. В данном случае организация как оператор самостоятельно организует и осуществляет сбор сведений у клиентов (например, при заключении договоров), вносит соответствующие

сведения в базу данных, пользуется такой базой, осуществляет при необходимости удаление персональных данных клиентов.

В третьей ситуации оператор осуществляет только обработку персональных данных. Как правило, в качестве таких операторов выступают государственные органы и иные организации, которые осуществляют обработку персональных данных для реализации возложенных на них государственно-властных полномочий или иных публичных функций. Ключевые параметры такой обработки определяются законодательством и соответствующие органы и организации не могут их изменить.

Например, исполкомы первичного уровня являются операторами, осуществляющими обработку данных, при ведении учета личных подсобных хозяйств граждан в пределах своей компетенции, а объем обрабатываемых персональных данных, цели и порядок такой обработки определяются законодательством (в частности, форма похозяйственных книг установлена постановлением Совета Министров Республики Беларусь от 15 октября 2005 г. № 1273 «Об организации ведения похозяйственного учета»).

Оператор может организовывать и (или) осуществлять обработку персональных данных как самостоятельно, так и совместно с иными операторами. Лица, совместно организующие и (или) осуществляющие обработку персональных данных, – сооператоры. Типичным примером сооператорства является ведение (использование) общей базы данных несколькими операторами (программы лояльности, базы данных кандидатов на работу и др.).

Само по себе наличие взаимной выгоды (например, коммерческой), возникающей в результате деятельности, связанной с обработкой персональных данных, не приводит к сооператорству. Если юридическое лицо, участвующее в обработке персональных данных, не преследует собственных целей в отношении деятельности по обработке персональных данных, а просто получает оплату за оказанные услуги, оно действует как уполномоченное лицо, а не как совместный оператор. В Законе не определены правовые основания для обработки персональных данных между сооператорами.

На каждого из сооператора возлагаются все обязанности, предусмотренные Законом в отношении операторов, и каждый из них самостоятельно несет полную ответственность за несоблюдение его требований.

В этой связи при организации и осуществлении совместной обработки персональных данных принципиально важным является распределение между такими операторами функций в совместной обработке.

Прозрачность такого распределения обеспечивается, как правило, посредством заключения между совместными операторами соответствующего соглашения (договора), в котором будут, в частности, отражены:

– цели обработки;

– персональные данные, которые подлежат обработке;

– права и обязанности каждого из операторов в отношении обработки персональных данных;

– порядок рассмотрения заявлений субъектов персональных данных, направленных в соответствии со ст. 14 Закона (например, рассмотрение заявлений субъектов персональных данных (подготовка проектов ответов), осуществляется одним из сооператоров независимо от того, кому они адресованы, или же каждый оператор самостоятельно рассматривает адресованные ему заявления субъектов персональных данных). В любом случае ответ на заявление направляется субъекту персональных данных тем оператором, к которому поступило заявление.

Для обеспечения принципа прозрачности обработки персональных данных (п. 6 ст. 4 Закона) информация о совместной обработке персональных данных отражается в документе, определяющем политику каждого оператора в отношении обработки персональных данных. При этом в отношении обработки персональных данных для реализации конкретного бизнес-процесса (например, участие в программах лояльности торговой сети, ведение базы данных кандидатов на работу) совместными операторами может быть подготовлен общий такой документ.

Если основанием для обработки персональных данных сооператорами является согласие, то субъект персональных данных выражает его для достижения конкретной цели всем сооператорам. Такое согласие может собирать один из сооператоров в отношении всех сооператоров. В случае несогласия с участием в обработке персональных данных конкретного оператора, субъект персональных данных отказывает в даче согласия всем сооператорам. При этом каждый из них несет самостоятельное бремя доказывания получения согласия субъекта персональных данных в отношении себя.

Еще один субъект – это субъект персональных данных, под которым понимается физическое лицо, в отношении которого осуществляется обработка персональных данных.

Закон не устанавливает для признания лица субъектом персональных данных, то есть любое физическое лицо признается таковым независимо от возраста, гражданства, занимаемой должности и др.

Индивидуальный предприниматель является субъектом персональных данных.

По общему правилу, умершие не признаются субъектами персональных данных. Тем не менее, Закон хоть и ограниченно, но регулирует обработку персональных данных таких лиц. Так, если отсутствуют правовые основания для обработки персональных данных умершего, то их обработка возможна с согласия одного из наследников, близких родственников или иных лиц, указанных в ч. 1 п. 9 ст. 5 Закона. В этом случае указанные лица пользуются правами субъекта персональных данных.

Последний субъект – это уполномоченное лицо, под которым понимается государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося

оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах.

Основные признаки уполномоченного лица следующие:

1. Статус.

Уполномоченным лицом может являться организация (государственный орган, юридическое лицо Республики Беларусь, иная организация) и физическое лицо, в том числе индивидуальный предприниматель.

Уполномоченное лицо должно быть отдельным юридическим или физическим лицом по отношению к оператору, независимо от признания его аффилированным, зависимым или дочерним.

Важно, что работники оператора не могут рассматриваться как самостоятельные операторы или уполномоченные лица. Оператором в данном случае выступает наниматель, у которого работник работает по трудовому договору.

Если с физическим лицом заключен гражданско-правовой договор, то его статус определяется в каждом конкретном случае. Если такое лицо осуществляет обработку персональных данных под контролем оператора и с использованием принадлежащих оператору информационных ресурсов, то его по аналогии с работниками оператора следует рассматривать как «часть» оператора.

2. Уполномоченное лицо осуществляет обработку персональных данных от имени оператора или в его интересах.

Например, организация продает товары через Интернет, предлагая доставку товара курьером. С целью исполнения обязательств по доставке организацией запрашиваются у покупателя контактные данные, необходимые для доставки: адрес, имя и контактный телефон. Для доставки организация заключила договор с другой организацией, которая имеет будет доставлять товар. Организация-продавец передает собранные ею персональные данные покупателей в доставку. В данном случае организация-продавец определила цель обработки (доставка товара), лиц, чьи персональные данные будут обрабатываться (покупатели), и перечень обрабатываемых персональных данных (адрес, имя и контактный телефон). В свою очередь, организация-доставщик, используя собранные персональные данные, от имени организации-продавца доставила товар. Организация-продавец – оператор, организация-доставщик – уполномоченное лицо.

Классическим примером является передача ведения бухгалтерского или кадрового учета, системного администрирования локальной сети третьим лицам. В таком ситуации, организация – заказчик – это оператор, а исполнитель, то есть та, которая оказывает услуги, - исполнитель.

В одних случаях оператор определяет, какие персональные данные подлежат обработке, и предоставляет подробные указания (инструкции) по обработке, которым должно следовать уполномоченное лицо. Соответственно, уполномоченное лицо ограничено в том, какие действия оно может осуществлять с персональными данными.

В иных случаях (что чаще всего имеет место на практике) уполномоченные лица могут принимать свои собственные повседневные оперативные решения, использовать свои знания и навыки, чтобы решить, как выполнять определенные действия в интересах оператора (например, выбор конкретного типа аппаратного или программного обеспечения для обработки персональных данных, в том числе для обеспечения защиты информации).

Тем не менее, уполномоченные лица не могут определять ключевые параметры обработки персональных данных (о целях и сроках обработки, объеме обрабатываемых персональных данных, передаче персональных данных третьим лицам). При этом передача уполномоченным лицом персональных данных третьим лицам в силу требований законодательных актов не может рассматриваться как определение ключевых параметров обработки.

Распространенным примером является также выстраивание отношений «оператор-оператор». Например, при заключении договора поставки и продавец, и покупатель, передавая персональные данные своих представителей, являются самостоятельными операторами, что не накладывает на них дополнительных обязательств.

Прекращения взаимоотношений между оператором и уполномоченным лицам влечет необходимость прекратить обработку соответствующих персональных данных (такие данные передаются оператору либо удаляются (блокируются). Порядок подтверждения передачи, удаления или блокирования персональных данных целесообразно определить в договоре между оператором и уполномоченным лицом и впоследствии оформить акт или отчет. В качестве исключения удаления (блокирования) могут требования бухгалтерского учета или в сфере архивного дела и делопроизводства.

В сфере защиты персональных данных, основной термин – это обработка персональных данных, под которой понимается любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.

Разновидностями обработки в Законе названы (перечень является открытым)

- сбор;
- систематизация;
- хранение;
- изменение;
- использование;
- обезличивание;
- блокирование;
- распространение;
- предоставление;
- удаление.

Справочно:

В GDPR обработка определяется как любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными с использованием средств автоматизации или без использования таких средств, включая сбор, запись, организацию, структурирование, накопление, хранение, адаптацию или изменение, загрузку, просмотр, использование, раскрытие посредством передачи, распространение или иной вид предоставления доступа, сопоставление или комбинирование, сокращение, удаление или уничтожение.

Даже простое хранение информации на жестком диске компьютера является обработкой таких данных.

Обработка персональных данных должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами. В случае обработки персональных данных без согласия субъекта персональных данных цели обработки персональных данных устанавливаются Законом и иными законодательными актами.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее заявленных законных целей. Не допускается обработка персональных данных, не совместимая с первоначально заявленными целями их обработки.

В случае необходимости изменения первоначально заявленных целей обработки персональных данных оператор обязан получить согласие субъекта персональных данных на обработку его персональных в соответствии с измененными целями обработки персональных данных при отсутствии иных оснований для такой обработки, предусмотренных настоящим Законом и иными законодательными актами.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям их обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

Обработка персональных данных должна носить прозрачный характер. В этих целях субъекту персональных данных в случаях, предусмотренных настоящим Законом, предоставляется соответствующая информация, касающаяся обработки его персональных данных.

Оператор обязан принимать меры по обеспечению достоверности обрабатываемых им персональных данных, при необходимости обновлять их.

Хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных.

В Законе закрепляются принципы к обработке персональных данных:

– Законность.

Обработка должна осуществляться в соответствии с Законом и иными актами законодательства (законность). Обработка предполагает выполнение оператором (уполномоченным лицом) всех обязанностей, которые на него возлагаются Законом. Требование законности обработки также означает, что оператор должен учитывать не только требования самого Закона, но и положения отраслевого законодательства, регулирующие конкретный вид обработки.

– Соразмерность и справедливость.

Обработка должна быть соразмерна заявленным целям и обеспечивать на всех этапах обработки справедливое соотношение интересов всех заинтересованных лиц. Соразмерность означает, когда без обработки запрашиваемых персональных данных не может быть достигнута цель или ее достижение будет затруднено. Сканирование радужной оболочки глаз при входе в организацию (при отсутствии специфических обстоятельств, требующих от организации применения повышенных мер безопасности) для целей учета прихода и ухода с работы сложно признать соразмерной мерой, поскольку данная цель может быть достигнута иными способами (с помощью карточки, наличия охранника и др.).

Справедливость обработки также означает недопустимость злоупотребления сложившейся ситуацией (монопольным положением оператора, отсутствием у субъекта возможности ознакомиться с информацией и др.).

– Наличие правового основания.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами. Таким образом, в качестве общего правила обработки указывается на необходимость получения согласия субъекта персональных данных. Иные основания рассматриваются лишь как возможные исключения из него.

– ограничение цели.

Для соблюдения данного принципа есть несколько характеристик целей обработки:

конкретность (не допускается указание абстрактных или общих целей, которые не определяют пределов обработки и не позволяют субъекту персональных данных понять, для чего будут обрабатываться его персональные данные (например, «совершенствование деятельности организации»; «разработка новых услуг»; «достижение общественно значимых целей», «реализация устава»);

заявленность цели до момента начала обработки (оператор не может подбирать цель постфактум, после начала и, тем более, окончания обработки);

законность (недопустимость обработки персональных данных для осуществления противозаконной деятельности (например, осуществления мошеннических действий, преследования лица и др.).

Следует отличать измененные цели от совместимых целей. Измененная цель – это новая цель, которая не охватывается первоначальной, не вытекает из

нее. Совместимая цель – конкретизация (уточнение) первоначальной цели. В этой связи не должна рассматриваться как новая цель ее новая формулировка, не меняющая существа обработки, либо цель, конкретизирующая первоначальную.

Например, если первоначальная цель – это «заключение и исполнение договора», то цель – «отправка напоминаний о необходимости оплаты» может обоснованно рассматриваться как конкретизация первоначальной цели.

В свою очередь, отправка страховой компанией информации нанимателю о наличии задолженности работника за оказанные страховые услуги не может расцениваться как действия в целях исполнения договора страхования, а должна признаваться новой целью обработки персональных данных, требующей самостоятельного правового основания.

– Запрет избыточности.

На практике довольно распространенным нарушением данного требования является ситуация, когда имеет место обработка с «запасом», «на всякий случай».

Разновидностями данного нарушения могут быть ситуации, например, запрос информации о родственниках у кандидата на работу, когда это не предусмотрено законодательством, никак не влияет на оценку профессиональных качеств такого лица.

– Прозрачность.

Требование прозрачности обработки распространяется на весь период обработки персональных данных. Прозрачность обработки персональных данных обеспечивается при получении данных либо от самого субъекта, либо от третьих лиц; при коммуникации с субъектом персональных данных, например, по вопросу реализации его прав.

Ключевое значение для обеспечения прозрачности обработки имеет форма представления информации субъекту. Информацию следует излагать простым, ясным и доступным языком. Следует избегать абстрактных или неоднозначных формулировок, не позволяющих субъекту понять суть и параметры обработки персональных данных, в частности таких слов, как «может», «вероятно», «некоторый», «часто», «допускается».

– Ограничение хранения.

На практике предусмотрено два подхода к хранению персональных данных:

если срок хранения определен в законодательном акте (акте законодательства, принятом в развитие законодательного акта), то данные могут храниться в течение этого срока. В данном случае происходит своеобразная трансформация правового основания обработки (например, вместо исполнения договора правовым основанием становится необходимость выполнения обязанностей, предусмотренных законодательным актом).

если срок хранения не определен в акте законодательства, то он определяется самим оператором. В такой ситуации можно храниться не дольше, чем это необходимо для достижения цели обработки.

В этой связи следует отметить, что хранение персональных данных без правового основания, в том числе, если такие данные более не требуются для достижения заявленной цели, является разновидностью незаконной обработки персональных данных и влечет административную ответственность по ч. 1 ст. 23.7 КоАП.

Срок хранения персональных данных на практике может определяться по-разному. Это может быть:

конкретная календарная дата (например, до 1 января 2026 г.);

период времени с момента наступления определенного события (1 год с момента дачи согласия);

комбинация различных критериев (1 год с момента использования личного кабинета).

Использование фразы «до отзыва согласия» не соответствует требованиям Закона.

Вместе с тем, если данные будут анонимизированы (иными словами, идентифицирующие субъекта данные будут удалены), то такие данные не будут являться персональными и препятствий для их хранения не будет.

– Достоверность.

Требование достоверности обрабатываемых данных направлено на недопущение нарушений прав и свобод физических лиц в связи с обработкой устаревшей или недействительной информации.

Данное требование обеспечивается предоставлением субъекту персональных данных права на изменение персональных данных и права требовать прекращения их обработки и (или) удаления. Оператор обязан осуществлять изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных также по требованию Национального центра защиты персональных данных. Кроме того, актами законодательства может предусматриваться периодическая актуализация обрабатываемых персональных данных.

Одним из видов обработки является блокирование персональных данных, то есть прекращение доступа к персональным данным без их удаления. Блокирование персональных данных при наличии возможности их удаления может привести к незаконному хранению таких данных и применению соответствующих мер ответственности.

В отличие от удаления персональных данных, когда либо сам носитель данных уничтожается, либо данные необратимо стираются или иным образом удаляются (без возможности их восстановления), при блокировании персональные данные сохраняются. При этом администратором ресурса (системы) ограничивается доступ к таким данным и в дальнейшем они просто хранятся без возможности их использования.

Следующий вид обработки – это обезличивание персональных данных, то есть невозможность без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

В Беларуси методы обезличивания персональных данных предусмотрены в приложении 5 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному Приказом № 66. К ним отнесены введение идентификаторов, изменение состава, декомпозиция, перестановка, зашифрование.

В сфере медицины действует постановление Министерства здравоохранения Республики Беларусь от 28 мая 2021 г. № 64 «Об утверждении Инструкции о порядке обезличивания персональных данных лиц, которым оказывается медицинская помощь». Регулятор предусмотрел три метода обезличивания: введение идентификаторов, замена состава, декомпозиция.

Конкретный метод обезличивания выбирается оператором в зависимости от целей обработки персональных данных. Методы обезличивания могут применяться каждый по отдельности или комбинироваться друг с другом. При этом важно, чтобы обезличивание могло обеспечивать не только защиту таких данных, но и возможность их обработки. Как правило, чем больше степень обезличивания данных, тем меньше их ценность для анализа. Кроме того, обезличивание должно быть обратимым, иначе это будут уже анонимные данные с совершенно иным правовым режимом.

Довольно распространенным среди правоприменителей является мнение о том, что получившийся в результате обезличивания результат – это не персональные данные. Однако это не так.

Например, в 2006 году сервис потокового кино опубликовал набор данных, содержащий 10 млн. рейтингов фильмов, сделанных 500 000 клиентами, утверждая, что они были анонимными, но позже обнаружил, что злоумышленнику потребуется лишь немного знаний о подписчике, чтобы иметь возможность идентифицировать запись этого подписчика в наборе данных

В этой связи не соответствует Закону подход, при котором со ссылкой на п. 8 ст. 4 Закона (хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных) после достижения цели обработки персональные данные обезличиваются и продолжают храниться.

Указанная норма не может применяться, если в рассматриваемой ситуации сохраняется возможность идентификации лица. Вместе с тем, если будет исключена возможность идентификации лица, то такие данные становятся анонимными и могут продолжать храниться, а также использоваться для любых целей по сравнению с теми, для которых они были получены.

Следует учитывать, что применение обезличивания, к сожалению, не влияет на классификацию информационных ресурсов (систем), в которых обрабатываются персональные данные и, соответственно, не изменяет (понижает) требования к технической защите таких ресурсов. Так, если речь идет о специальных персональных данных, то к такому ресурсу (системе) будут

применяться требования к ресурсу (системе) 3-спец или 4-спец в зависимости от подключения к открытым каналам передачи данных. В этой связи на сегодняшний день для организации нет серьезных стимулов к внедрению обезличивания, хотя в целом, как уже отмечалось, это весьма эффективный инструмент снижения рисков при обработке персональных данных.

Важный этап обработки персональных данных – удаление, в результате которых становится невозможным восстановить персональные данные в информационных ресурсах (системах), содержащих персональные данные, и (или) в результате которых уничтожаются материальные носители персональных данных.

Механизм удаления во многом зависит от того, в каком виде и в каких документах содержатся персональные данные

НЦЗПД предлагает следующие варианты действий:

1. Удаление персональных данных, содержащихся в документах, включенных в номенклатуру дел с установленными сроками хранения.

1.1. Удаление персональных данных, содержащихся в документах на бумажных носителях.

После составления акта отобранные к уничтожению документы и дела передаются организациям, ведающим заготовкой вторичного сырья. Вместе с тем в целях обеспечения защиты персональных данных документы на бумажных носителях, содержащие специальные персональные данные, иные персональные данные, распространение которых создает высокий риск для прав и свобод физических лиц (круг таких данных определяется самим оператором), целесообразно передавать организациям, ведающим заготовкой вторичного сырья после предварительного измельчения.

1.2. Удаление персональных данных, содержащихся в документах в электронном виде (за исключением удаления из систем хранения данных, иного серверного оборудования).

1.3. Удаление персональных данных, содержащихся в электронных документах.

2. Удаление персональных данных из документов, не включенных в номенклатуру дел с установленными сроками хранения.

На персональных компьютерах, в общих сетевых ресурсах, на бумажных носителях у работников могут накапливаться материалы, послужившие основанием для разработки документов, а также их копии, проекты писем и др. В целях эффективного выполнения оператором своих обязанностей по удалению персональных данных после уничтожения документов и дел с истекшими сроками хранения подлежат удалению (уничтожению) и эти материалы, и копии, и проекты.

Порядок удаления (уничтожения) таких материалов определяет оператор.

Проведение проверок своевременного удаления (уничтожения) документов, материалов к ним, их копий и проектов целесообразно возлагать на лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных.

3. Удаление персональных данных, содержащихся в информационных системах (ресурсах).

В соответствии с Законом оператор обязан удалить персональные данные при отсутствии правовых оснований для их обработки. Данное требование распространяется в том числе и на ситуации, когда персональные данные содержатся в информационных ресурсах (системах) соответствующего оператора (например, локальной вычислительной сети, интернет-сайте, бухгалтерской информационной системе, системе электронного документооборота, системе видеонаблюдения и др.).

Порядок удаления информации из информационных систем (ресурсов) в законодательстве не определен, за исключением отдельных государственных информационных систем (ресурсов). В этой связи в целях выполнения соответствующей обязанности оператору следует самостоятельно разработать порядок удаления персональных данных. Он может быть предусмотрен в отдельном локальном правовом акте, локальном акте, определяющем порядок функционирования такой информационной системы (ресурса), в политике информационной безопасности.

Законодательством не предусматривается в этих случаях обязательное составление акта об удалении на бумажном носителе. Так, в случае автоматического удаления персональных данных из информационной системы (ресурса) достаточно указать сроки хранения этой информации. В частности, в системах видеонаблюдения запись видеоизображения осуществляется в циклическом режиме, когда самые старые записи заменяются новыми.

В иных случаях целесообразно создавать лог-файлы и настраивать их ведение таким образом, чтобы в эти файлы вносились записи об удалении персональных данных, но без информации, позволяющей идентифицировать физических лиц (например, запись сведений о дате удаления и объеме удаленных сведений).

Составлять акт об удалении персональных данных целесообразно в случаях разового удаления персональных данных, например удаления на основании заявления субъекта персональных данных, на основании требования Центра, в иных случаях, когда необходимо подтвердить факт совершения этого действия.

Из информационных систем (ресурсов) персональные данные следует удалять таким образом, чтобы их невозможно было восстановить обычному пользователю. Например, простое «перемещение в корзину» не является надлежащим выполнением обязанности по удалению персональных данных. При этом сама по себе возможность применения специальных технических средств по восстановлению информации не может рассматриваться как свидетельство невыполнения оператором обязанности по удалению персональных данных.

Законом (ч. 2 п. 2 ст. 13) предусматривается, что при отсутствии технической возможности удаления персональных данных оператор обязан

принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование.

В контексте Закона данная мера является альтернативой удалению, когда удаление по техническим причинам невозможно (например, может нарушить работу всей системы). По своим последствиям блокирование является равнозначным удалению и должно исключать использование, предоставление, распространение персональных данных и др.

ЛЕКЦИЯ 7. ПРАВОВЫЕ ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Одним из самостоятельных правовых оснований обработки персональных данных является согласие субъекта персональных данных. Оно не является универсальным или обязательным условием для обработки персональных данных, то есть обработка на основании ст. 6 и 8 Закона не требует получения согласия. В этой связи получение согласия при наличии иных оснований рассматривается как избыточная обработка персональных данных. Одним из критериев, свидетельствующих о неправомерности обработки персональных данных на основании согласия, может являться, в частности, тот факт, что отзыв согласия не допускается или не влечет прекращения обработки персональных данных.

Согласно ст. 5 согласие должно обладать следующими характеристиками: (i) свободное, (ii) однозначное, (iii) информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных

Согласие является свободным, когда субъект самостоятельно, исходя из своего внутреннего убеждения, выражает свою волю в отношении обработки персональных данных. Данное требование предполагает недопустимость понуждения субъекта к даче такого согласия под угрозой наступления неблагоприятных для него последствий.

(i) Свободное согласие. Это означает, что субъект персональных данных обладает реальным выбором давать свое согласие либо его согласие является вынужденным, например, в силу связанности согласия с достижением иной, желаемой для него цели.

Например, заказ и доставка товара в интернет-магазине не может быть реализована, пока субъект не даст согласие на использование адреса электронной почты для осуществления рекламной рассылки. В данной ситуации обработка персональных данных в целях получения рекламных сообщений не является необходимой для заключения договора розничной купли-продажи. Согласие не является свободным, следовательно, это нарушение Закона.

Нарушение принципа свободного согласия также в ситуации, когда одно согласие получается для достижения нескольких самостоятельных целей (например, для осуществления рекламной рассылки, а также для передачи данных организациям-партнерам). Для каждой цели должно получаться отдельное согласие, если оно используется в качестве правового основания

обработки персональных данных. Главный принцип – «одна цель – одно согласие». При этом субъект персональных данных вправе давать свое согласие исключительно на те цели, которые посчитает нужными. Для реализации требований к свободному согласию оператору необходимо предоставить субъекту персональных данных право выбора конкретных целей обработки персональных данных, с которыми он согласен, а также указать категории персональных данных, обрабатываемые применительно к каждой цели.

Цели обработки персональных данных могут разделяться, например, на «чек-боксы», в которых субъект персональных данных может выразить свое согласие путем проставления отметки (галочки) или подписи.

Согласие не может рассматриваться как свободное при очевидной зависимости между оператором и субъектом персональных данных. В этой связи за редкими исключениями не рассматривается как свободное согласие между нанимателем и работником (кандидатом на работу).

(ii) Однозначное согласие. Оно дается путем совершения четкого намеренного действия. Соответствующая информация должна быть воспринята субъектом персональных данных и отражать его действительные намерения. Факт дачи согласия не должен быть предметом допущений, а должен следовать из конкретных действий субъекта, свидетельствующих об этом. Молчание или бездействие субъекта персональных данных, даже если такое поведение в соответствии с изданными оператором документами, определяющими политику в отношении обработки персональных данных, будет признаваться согласием, не будет удовлетворять критерию однозначности согласия.

В этой связи не соответствуют критерию однозначности, например, следующие модели получения согласия:

«оставаясь на линии, Вы тем самым даете согласие на обработку персональных данных»; «продолжая пользоваться сайтом, Вы даете согласие на обработку персональных данных».

(iii) Информированное согласие. При получении согласия от субъекта персональных данных необходимо представлять всю необходимую и достоверную информацию о целях обработки, об обрабатываемых данных, операторе и иных лицах, которые будут осуществлять обработку персональных данных, сроке обработки и другой необходимой информации (п. 5 ст. 5 Закона). Информация должна быть представлена простым и ясным языком в той же форме, что и форма получения согласия. Предоставляемая оператором информация должна позволять субъекту получить ответы на вопросы: кто, зачем, какие данные, каким образом и в течение какого срока будет обрабатывать.

Например, размещение информации по п. 5 ст. 5 Закона на корпоративном сайте в глобальной компьютерной сети Интернет не будет являться надлежащей формой предоставления такой информации, если согласие получается в письменной форме. Не будет являться «надлежащим» информированием и получение согласия путем ознакомления с политикой обработки персональных данных, содержащей описание нескольких бизнес-процессов. В последнем

случае оператор фактически перекладывает на субъекта бремя поиска соответствующего бизнес-процесса и выделение необходимой информации в тексте политики. Кроме того, политика обработки персональных данных может периодически меняться, что фактически приводило бы к одностороннему изменению содержания полученного согласия.

Согласно п. 2 ст. 5 Закона согласие субъекта персональных данных может быть получено в письменной форме, в виде электронного документа или в иной электронной форме.

Согласия в письменной форме представляет собой собственноручно подписанный субъектом персональных данных документ в любой форме (напечатан на компьютере или написан от руки), который подтверждает добровольное решение субъекта персональных данных передать оператору свою личную информацию для определенных целей. Например, в соответствии с ч. 1 п. 23 Указа Президента Республики Беларусь от 18 апреля 2019 г. № 148 «О цифровых банковских технологиях» для целей деятельности пользователей межбанковской системы идентификации документы, информация, включая заявку, заявление, согласие на обработку данных о клиентах, в том числе хранящихся в МСИ, считаются совершенными (предоставленными) в письменной форме, если:

они сформированы (предоставлены) в порядке, отвечающем требованиям п. 22 Указа Президента Республики Беларусь от 18 апреля 2019 г. № 148 «О цифровых банковских технологиях»;

соблюдены требования к защите информации и обработке персональных данных в соответствии с законодательством об информации, информатизации и защите информации, в том числе о персональных данных.

На практике часто используется механизм включения согласия в текст договора, например, договор на оказание медицинских услуг с одновременным получением согласия на получение рекламной рассылки. Это допустимо, в Законе нет ограничений. Однако в силу требований к согласию, то есть какая информация должна представляться при его получении, договор будет слишком громоздким. Более того, внесение изменений в информацию для получения согласия потребует заключения дополнительного соглашения к договору. Также возникнет вопрос о свободном согласии, так как заключение договора будет подразумевать дачу согласия на иные цели, которые не достигаются путем заключения договора. В этой связи лучше оформлять два отдельных документа: договор и согласие. Включение согласия в договор также может вызывать путаницу в основании обработки персональных данных, так как договор и согласие – это два отдельных основания.

Унифицированной формы для оформления согласия законодательно не предусмотрено. В качестве ориентира можно использовать образец согласия на обработку персональных данных, размещенный на официальном сайте НЦЗПД.

Согласно п. 3 ст. 5 Закона предусмотрено, что в иной электронной форме согласие субъекта персональных данных может быть получено посредством:

указания (выбора) субъектом персональных данных определенной информации (кода) после получения СМС-сообщения, сообщения на адрес электронной почты;

проставления субъектом персональных данных соответствующей отметки на интернет-ресурсе;

других способов, позволяющих установить факт получения согласия субъекта персональных данных.

То есть перечень способов открытый. Распространенным примером получения согласия в иной электронной форме является проставление субъектом персональных данных соответствующей отметки на интернет-ресурсе, разрешающей обработку персональных данных этого субъекта. В такой ситуации согласие все равно должно быть свободным, информированным и однозначным.

Законодательными актами может быть предусмотрена необходимость получения согласия субъекта персональных данных только в письменной форме или в виде электронного документа.

Так, например, требования в отношении оформления согласия на предоставление сведений о правонарушениях установлены Законом «О единой государственной системе регистрации и учета правонарушений» и принятым в его развитие постановлением Совета Министров Республики Беларусь от 20 июля 2007 г. № 909 «О функционировании единой государственной системы регистрации и учета правонарушений». При этом в приложении 20 установлена форма согласия физического лица (его законного представителя), в том числе индивидуального предпринимателя, на предоставление сведений о правонарушениях, хранящихся в едином государственном банке данных о правонарушениях.

В п. 5 ст. 5 Закона содержатся положения, определяющие объем предоставляемой информации и требования к ее изложению, для признания согласия информированным.

К этой информации относится:

наименование (фамилию, собственное имя, отчество (если таковое имеется)) и место нахождения (адрес места жительства (места пребывания)) оператора, получающего согласие субъекта персональных данных;

цели обработки персональных данных (Они должны быть конкретными, например, на получение маркетинговой рассылки. Не допускается получение общего согласия, например, для взаимодействия заказчика и исполнителя, в соответствии с уставными целями, улучшение деятельности организации, реализация законных прав оператора, реализация устава и др. и т.д. При указании нескольких целей у субъекта должна возможность на одну из целей);

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных (Например, имя, адрес электронной почты. Запрещено собирать персональные данные «с запасом», на всякий случай. Оператору следует по возможности минимизировать объем персональных данных, руководствуясь принципом недопущения избыточности обработки.);

срок, на который дается согласие субъекта персональных данных. (В качестве срока может быть указана конкретная дата (например, до 31.12.2025) или конкретный период времени (например, истечение срока программы лояльности) либо критерии, используемые для определения срока обработки (например, в течение 1 года после последней активации личного кабинета). Не допускается использование при определении сроков согласия таких формулировок, как «до отзыва согласия субъектом персональных данных», «сроки устанавливаются законодательством», так как они не соответствуют требованиям прозрачности обработки персональных данных. Срок действия согласия не допускается указывать свыше 3 лет, так как субъекту будет затруднительно контролировать обработку своих персональных данных. Если срок согласия различается для каждой цели, то его необходимо обозначить для каждой цели отдельно.) .

информацию об уполномоченных лицах в случае, если обработка персональных данных будет осуществляться такими лицами. (Необходимо указывать наименование и местонахождение конкретной организации. Если это сделать невозможно, то указывается категории лиц (например, организации, оказывающие оператору услуги по системному администрированию локальной сети; организации, осуществляющие доставку покупателю купленных у оператора товаров; организации, оказывающие оператору услуги по ведению бухгалтерского, кадрового учета) и место их нахождения (страна нахождения). Не допускается указание общих характеристик, например, «лица, с которыми оператор имеет договорные отношения», или открытого перечня, например, «иные лица».);

перечень действий с персональными данными, на совершение которых дается согласие субъекта персональных данных, общее описание используемых оператором способов обработки персональных данных. Должны быть указаны конкретные действия, например, сбор персональных данных для заключения договора с определением перечня необходимых персональных данных; внесение сведений в информационный ресурс; хранение персональных данных с указанием сроков и условий хранения; их актуализация путем сопоставления с дополнительной информацией и т.п. Если используется обезличивание, предоставления персональных данных третьим лицам, это должно быть указано в согласии.

иную информацию, необходимую для обеспечения прозрачности процесса обработки персональных данных. Например, правовые, организационные и технические меры для защиты персональных данных субъектов, применяемые оператором, если эта информация может оказать влияние на принятие решения субъектом персональных данных.

При этом ч. 2 п. 5 ст. 5 Закона предусмотрено, что информация должна быть предоставлена простым и ясным языком субъекту персональных данных в письменной либо электронной форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой ему информации. В этой связи информация, предоставляемая оператором до получения согласия субъекта

персональных данных, должна содержаться в виде отдельной выдержки из политики в отношении обработки персональных данных, условий пользования сайтом и т.д.

При наличии трансграничной передачи персональных данных, необходимо указывать государства, в которые будет осуществляться передача. В случае передачи в страны, где не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, необходимо отразить возможные риски такой передачи (абзац второй п. 1 ст. 9 Закона);

Для целей обеспечения информированного согласия не является надлежащим:

предоставление необходимой информации путем отсылки для самостоятельного ознакомления к сайту оператора при получении согласия на обработку персональных данных в письменной форме;

размещение необходимой информации, например на информационных стендах организации;

предоставление необходимой информации путем ознакомления с политикой оператора в отношении обработки персональных данных, содержащей описание нескольких бизнес-процессов, при получении согласия в иной электронной форме.

В п. 6 ст. 5 Закона предусмотрено, что субъект персональных данных при даче согласия оператору указывает свои фамилию, имя, отчество (если таковое имеется), дату рождения, идентификационный номер, а в случае отсутствия такого номера – номер документа, удостоверяющего его личность, за исключением случая, предусмотренного ч. 2 п. 6 ст. 5 Закона. В соответствии с ч. 2 п. 6 ст. 5 Закона, если цели обработки персональных данных не требуют обработки всей совокупности указанной информации, она не подлежит обработке оператором при получении согласия субъекта персональных данных.

Например, для регистрации личного кабинета на сайте и получения рекламной рассылки достаточно указать ФИО и адрес электронной почты, то указание идентификационного номера при получении согласия не требуется. Для целей рассмотрения резюме, регистрации в интернет-магазине указание паспортных данных и (или) идентификационного номера также является избыточным.

Обязанность доказывания получения согласия субъекта персональных данных возлагается на оператора. Механизм подтверждения получения согласия субъекта персональных данных определяется оператором самостоятельно.

Например, это может быть осуществлено с помощью технической информации, содержащейся в базе данных оператора. В случае получения согласия субъекта персональных данных в письменной форме или форме электронного документа необходимо вести учет полученных согласий, в том числе, в разных местах. В этой связи не является нарушением Закона, например, хранение согласий соответствующим подразделением, ответственным за реализацию конкретных бизнес-процессов.

Закон допускает получение одного согласия в отношении нескольких операторов, если они осуществляют совместную обработку персональных данных, то есть совместно определяют способы и цели обработки (”сооператорство“).

В случае признания субъекта персональных данных недееспособным или ограниченно дееспособным, а также до достижения им возраста 16 лет, за исключением вступления в брак до достижения возраста 16 лет, согласие на обработку его персональных данных дает один из его законных представителей.

Что касается возможности получить согласие субъекта персональных данных на обработку его персональных данных через представителя на основании доверенности, то данный подход не противоречит требованиям Закона.

В ст. 6 Закона установлен открытый перечень оснований, когда допускается обработка персональных данных без согласия субъекта персональных данных. Важно, что данные основания неприменимы при обработке специальных персональных данных. То есть согласие – это базовое основание для обработки персональных данных, но оно не является универсальным или обязательным условием для обработки персональных данных. При этом следует учитывать, что все правовые основания, включая согласие, имеют равную силу.

Все основания можно сгруппировать по следующим категориям:

оформление и реализация трудовых (служебных) отношений;

заключение и исполнение договора;

обработка персональных данных, указанных в документе, адресованном оператору;

защита жизни, здоровья или иных жизненно важных интересов человека;

обработка распространенных ранее персональных данных;

обработка обезличенных персональных данных для научных или иных исследовательских целей;

выполнение обязанностей (реализация полномочий), предусмотренных законодательными актами.

Некоторые основания – это частный случай для определенных организаций.

Основания, когда не требуется получения согласия на обработку персональных данных, следующие:

для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности;

Порядок ведения административного и уголовного процессов установлен Процессуально-исполнительным кодексом Республики Беларусь об административных правонарушениях от 06.01.2021 № 92-З (далее – ПИКоАП) и Уголовно-процессуальным кодексом Республики Беларусь от 16.07.1999 № 295-З (далее – УПК).

В соответствии с п. 10 ч. 1 ст. 1.10 КоАП, ст.ст. 3.1 и 3.30 ПИКоАП ведение административного процесса осуществляется судом и

уполномоченными на то органами и организациями (органами внутренних дел, административными комиссиями и др.). К органам, ведущим уголовный процесс, относятся органы уголовного преследования (органы дознания, следователи, прокуроры) и суд (п. 19 ст. 6 УПК).

При совершении процессуальных действий, предусмотренных ПИКоАП и УПК, соответствующие органы и организации вправе осуществлять обработку персональных данных.

Так, например, в соответствии со ст. 3.29 ПИКоАП должностные лица органов, ведущих административный процесс, применяют профилактические меры воздействия, составляют протоколы, рассматривают дела об административных правонарушениях, налагают предусмотренные КоАП административные взыскания. Указанные действия неразрывно связаны с обработкой персональных данных, для которой на основании рассматриваемого абзаца второго ст. 6 Закона получать согласие субъекта персональных данных не требуется.

Оперативно-розыскная деятельность регулируется Законом Республики Беларусь от 15.07.2015 №307-З «Об оперативно-розыскной деятельности».

Оперативно-розыскную деятельность осуществляют:

органы внутренних дел;

органы государственной безопасности;

органы пограничной службы;

Служба безопасности Президента Республики Беларусь;

Оперативно-аналитический центр при Президенте Республики Беларусь;

органы финансовых расследований Комитета государственного контроля;

таможенные органы;

разведывательные службы Вооруженных Сил Республики Беларусь.

Органы, осуществляющие оперативно-розыскную деятельность, при выполнении задач оперативно-розыскной деятельности, в частности, имеют право:

создавать и (или) использовать базы данных (учеты), информационные системы, средства негласного получения (фиксации) информации и иные средства в соответствии с указанным Законом и иными актами законодательства;

получать безвозмездно сведения из баз данных (учетов), информационных систем путем удаленного доступа и (или) на материальных носителях информации от организаций, которые являются собственниками этих баз данных (учетов), информационных систем, в случаях, установленных законодательными актами, и порядке, определенном законодательством;

собирать, обрабатывать, хранить и изучать сведения и документы, необходимые для выполнения задач оперативно-розыскной деятельности;

получать от граждан на безвозмездной или возмездной основе сведения, необходимые для выполнения задач оперативно-розыскной деятельности;

направлять в организации письменные запросы о внесении в базы данных (учеты), информационные системы, собственниками которых являются эти организации, изменений, необходимых для выполнения задач оперативно-розыскной деятельности;

для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов;

Данное основание охватывает фактически два случая обработки персональных данных:

осуществление правосудия;

исполнительное производство.

Законодательными актами предусмотрено, что правосудие осуществляется только судом.

Обязанности (полномочия) суда (судей) при осуществлении правосудия установлены, в частности Кодексом Республики Беларусь о судоустройстве и статусе судей, ПИКоАП, УПК, Кодекс гражданского судопроизводства Республики Беларусь от 11.03.2024 № 359-З и рядом иных законодательных актов.

Обработка персональных данных без согласия субъекта персональных данных также осуществляется для исполнения судебных постановлений и иных исполнительных документов.

Перечень исполнительных документов содержится в ст. 10 Закона Республики Беларусь «Об исполнительном производстве», согласно которой наряду с судебными постановлениями к ним, в частности, относятся:

исполнительные листы и судебные приказы, выданные судами;

определения суда о судебном приказе;

определения суда об обеспечении иска или об обеспечении исполнения решения, не обращенного к немедленному исполнению;

постановления суда, органа, ведущего административный процесс, в части имущественных взысканий по делам об административных правонарушениях;

постановления судебного исполнителя в случаях, установленных настоящим Законом;

исполнительные документы иностранных судов в случаях, предусмотренных международными договорами Республики Беларусь;

исполнительные надписи нотариусов, дипломатических агентов дипломатических представительств Республики Беларусь и консульских должностных лиц консульских учреждений Республики Беларусь о взыскании денежных сумм (задолженности);

постановления прокуроров о выселении в административном порядке;

удостоверения комиссий по трудовым спорам;

решения налоговых органов о взыскании налогов, сборов (пошлин), а также иных обязательных платежей в республиканский и местные бюджеты, контроль за правильностью исчисления, своевременностью и полнотой уплаты которых возложен на налоговые органы;

иные акты, если в силу законодательных актов они являются исполнительными документами и подлежат исполнению в порядке, установленном Законом.

Согласно ст. 63 Закона Республики Беларусь «Об исполнительном производстве» судебный исполнитель при исполнении исполнительных документов имеет право:

истребовать у должника сведения об имеющемся у него имуществе, источниках получения доходов, а также другие сведения, необходимые для исполнения исполнительного документа;

получать по находящимся в его производстве исполнительным документам от граждан, в том числе индивидуальных предпринимателей, должностных лиц государственных органов и иных организаций на безвозмездной основе необходимые материалы и (или) документы, информацию (за исключением первичных статистических данных), включая информацию, содержащую банковскую и (или) иную охраняемую законом тайну, с соблюдением требований, установленных законодательными актами;

получать по находящимся в его производстве исполнительным документам на безвозмездной основе без письменного согласия физических лиц сведения из информационных ресурсов и систем, содержащих персональные данные, а также иметь доступ, включая удаленный, к информационным ресурсам и системам, содержащим такие данные, по письменному запросу или на основании соглашения о предоставлении персональных данных государственными органами и (или) иными организациями, в том числе с использованием общегосударственной автоматизированной информационной системы;

Данное основание применимо и иными операторами, которые вовлечены в процесс исполнительного производства и на которых возложена обязанность по совершению определенных действий, связанных с исполнением исполнительного документа, или по воздержанию от совершения определенных действий (банками и (или) небанковскими кредитно-финансовыми организациями, организациями по государственной регистрации недвижимого имущества, прав на него и сделок с ним, третьими лицами, собственниками имущества (учредителями, участниками) должника - юридического лица и др.).

в целях осуществления контроля (надзора) в соответствии с законодательными актами;

Основным комплексным законодательным актом, регулирующим вопросы осуществления контроля (надзора), является Указ Президента Республики Беларусь от 16.10.2009 № 510 «О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь» (далее – Указ №510).

Государственный контроль (надзор) осуществляется в формах выборочных проверок, внеплановых проверок, мероприятий технического (технологического, поверочного) характера, а также мер профилактического и предупредительного характера.

Общественный контроль в форме проведения проверок вправе осуществлять профессиональные союзы, их организационные структуры, объединения таких союзов и их организационные структуры в случаях и порядке, установленных иными законодательными актами. Осуществление общественного контроля в форме проведения проверок другими организациями, а также физическими лицами запрещается.

Указом № 510 утвержден перечень контролирующих (надзорных) органов, уполномоченных проводить проверки в рамках государственного контроля, и сфер их контрольной (надзорной) деятельности, а также определены права и обязанности данных органов при осуществлении этой деятельности.

Наличие у контролирующих (надзорных) органов и профсоюзов соответствующих прав (полномочий), позволяющих осуществлять обработку персональных данных без согласия субъектов персональных данных, не освобождает их от обязанности соблюдать общие требования к обработке персональных данных, предусмотренные ст. 4 Закона, в том числе требования о соответствии содержания и объема обрабатываемых персональных данных заявленным целям их обработки и исключении избыточной обработки персональных данных.

Оператор, предоставляющий контролирующим органам информацию, при наличии сомнений может запрашивать дополнительную информацию на предмет соблюдения положений ст. 4 Закона, в частности, уточнения правовых оснований, целей и, соответственно, объема информации, необходимой для их достижения.

при реализации норм законодательства в области национальной безопасности, о борьбе с коррупцией, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения;

Это основание связано с реализацией публично значимых функций. В одних законодательных актах предусматривается конкретный перечень обрабатываемых персональных данных (например, круг сведений, подлежащих установлению при идентификации клиентов - физических лиц, осуществляющих финансовые операции), в то время как в других - перечень таких данных в самом акте не закрепляется и вытекает из сути осуществляемых действий.

при реализации норм законодательства о выборах, референдуме, об отзыве депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, депутата местного Совета депутатов;

Сбор подписей, подача деклараций кандидатами, изготовление информационных материалов о кандидатах, регистрация инициативных групп и иные процессы, предусмотренные Избирательным кодексом Республики Беларусь от 11.02.2000 № 370-З, связаны с обработкой персональных данных.

Особенностью обработки персональных данных при реализации этого законодательства является необходимость обеспечения, с одной стороны, прозрачности избирательного процесса, а с другой - тайны голосования избирателей. Так, избиратели должны понимать, за кого они голосуют, что

обуславливает необходимость распространения информации о кандидатах. В то же время информация о том, кто и за кого голосовал, является тайной и в этой связи должны быть исключены любые действия, связанные с ее нарушением.

для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в том числе профессионального пенсионного страхования;

Данное основание применяется органами Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь (далее - Фонд), на который Указом Президента Республики Беларусь от 16 января 2009 г. № 40 возложены функции организации и ведения индивидуального (персонифицированного) учета в системе государственного социального страхования сведений о физических лицах, на которых распространяется государственное социальное страхование (абзац пятый п. 8 Положения о Фонде социальной защиты населения Министерства труда и социальной защиты Республики Беларусь, утвержденного Указом).

При ведении индивидуального (персонифицированного) учета органы Фонда обрабатывают персональные данные. Они отражаются на индивидуальном лицевом счете застрахованного лица и определены ст. 6 Закона Республики Беларусь от 6 января 1999 г. №230-З «Об индивидуальном (персонифицированном) учете в системе государственного социального страхования» (далее - Закон «Об индивидуальном (персонифицированном) учете в системе государственного социального страхования»). Среди таких данных указывают, например, страховой номер; дату рождения; информацию о месте жительства и (или) месте пребывания; номер, дату выдачи документа, удостоверяющего личность, наименование государственного органа, выдавшего этот документ, либо номер, дату выдачи паспорта или иного документа, его заменяющего, предназначенного для выезда за границу и выданного соответствующим органом государства гражданской принадлежности либо обычного места жительства иностранного гражданина, лица без гражданства или международной организацией, наименование органа или международной организации, выдавших эти паспорт или иной документ; размер страховых взносов; периоды получения ежемесячной доплаты к заработной плате вместо профессионального пенсионного страхования.

Обработка этих персональных данных органами Фонда осуществляется без согласия субъектов персональных данных.

при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством;

для осуществления нотариальной деятельности;

В соответствии с п. 1 ст. 3 Закона Республики Беларусь от 18 июля 2004 г. № 305-З 2О нотариате и нотариальной деятельности» (далее - Закон о нотариате) под нотариальной деятельностью понимаются совершение от имени Республики Беларусь нотариусами, уполномоченными должностными

лицами, должностными лицами загранучреждений нотариальных действий, предусмотренных данным законом и иными законодательными актами, международными договорами Республики Беларусь, а также оказание нотариусами услуг правового и технического характера.

Таким образом, наряду с нотариусами обработку персональных данных на данном основании при осуществлении нотариальной деятельности могут осуществлять уполномоченные должностные лица местных исполнительных и распорядительных органов, а также загранучреждений.

Полномочия нотариусов определены в ст. 24 Закона о нотариате. Так, например, в соответствии с п. 1 данной статьи нотариусы вправе:

истребовать и получать от государственных органов, иных организаций, индивидуальных предпринимателей и нотариусов, в том числе из государственных информационных ресурсов (систем) в установленном законодательными актами порядке, сведения и (или) документы, необходимые для осуществления нотариальной деятельности;

составлять проекты сделок, доверенностей, согласий, отказов, заявлений и иных нотариальных документов;

изготавливать копии документов и выписки из них и др.

Пунктом 1 ст. 25 Закона о нотариате на нотариусов возложен ряд обязанностей, в том числе:

проверять действительность представляемых гражданами и юридическими лицами для совершения нотариальных действий сведений и (или) документов посредством получения информации из информационных ресурсов (систем) государственных органов и иных организаций, к которым нотариус имеет доступ в соответствии с законодательством и (или) на основании соглашений, заключенных Белорусской нотариальной палатой с собственниками (владельцами) информационных ресурсов (систем);

вносить в единую электронную систему учета нотариальных действий и наследственных дел сведения в порядке, установленном Советом Министров Республики Беларусь.

Истребование персональных данных из соответствующих информационных ресурсов (систем) государственных органов и иных организаций для проверки действительности представляемых нотариусу сведений и (или) документов, в том числе удостоверяющих личность, и их последующее внесение в единую электронную систему учета нотариальных действий и наследственных дел осуществляется без согласия субъекта персональных данных.

при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь;

Данные вопросы урегулированы Законом Республики Беларусь от 1 августа 2002 г. №136-З «О гражданстве Республики Беларусь» и Законом Республики Беларусь от 23 июня 2008 г. №354-З «О предоставлении иностранным гражданам и лицам без гражданства статуса беженца,

дополнительной защиты, убежища и временной защиты в Республике Беларусь», а также принятыми в их развитие иными нормативными правовыми актами.

Согласно ст. 28 Закона Республики Беларусь «О гражданстве Республики Беларусь» решения по вопросам гражданства Республики Беларусь принимаются Президентом Республики Беларусь, органами внутренних дел, органами дипломатической службы. В связи с этим они обрабатывают персональные данные, например, при приеме заявлений по вопросам гражданства Республики Беларусь, проверке фактов и документов, представленных в обоснование таких заявлений.

Необходимо отметить, что в формах заявлений, анкет, а также в документах и материалах, требуемых для рассмотрения вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь, содержатся как «обычные» персональные данные (фамилия, собственное имя, отчество, число, месяц, год и место рождения, семейное положение и состав семьи, сведения о близких родственниках с указанием их места жительства, трудовая деятельность, образование и т.п.), так и специальные персональные данные (о вероисповедании, национальности, политической или общественной деятельности, привлечении к административной или уголовной ответственности, результаты обязательной государственной дактилоскопической регистрации и обязательного медицинского освидетельствования и т.п.). В этой связи в большинстве случаев обработка персональных данных при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь, будет осуществляться одновременно на двух правовых основаниях, предусмотренных абзацем десятым ст. 6 и абзацем девятым п. 2 ст. 8 Закона;

в целях назначения и выплаты пенсий, ежемесячного денежного содержания отдельным категориям государственных служащих, пособий;

Данное основание применимо при обработке персональных данных государственными органами и иными организациями, осуществляющими назначение и выплату любых пенсий и пособий, предусмотренных законодательством. Например, органами по труду, занятости и социальной защите - при назначении и выплате пенсий в соответствии с Законом Республики Беларусь от 17 апреля 1992 г. № 1596-XII «О пенсионном обеспечении. В отдельных случаях вопрос о назначении трудовых и социальных пенсий решается комиссией по назначению пенсий, образуемой районным (городским) исполнительным и распорядительным органом, которая будет осуществлять обработку персональных данных также на указанном основании;

При этом необходимо учитывать, что при наличии специального правового основания для обработки персональных данных, включая специальные персональные данные, в процессе трудовой (служебной) деятельности

субъекта персональных данных в случаях, предусмотренных законодательством, обработка персональных данных работников нанимателями для целей назначения и выплаты им пособий, предусмотренных законодательством (например, пособия по временной нетрудоспособности, по беременности и родам, по уходу за ребенком в возрасте до трех лет и т.п.), будет осуществляться на основании абзаца восьмого ст. 6 и абзаца третьего п. 2 ст. 8 Закона.

для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;

Определения терминов «государственные статистические наблюдения» и «официальная статистическая информация» содержатся в Законе Республики Беларусь от 28 ноября 2004 г. № 345-З «О государственной статистике» (далее - Закон «О государственной статистике»).

Так, государственные статистические наблюдения - сбор первичных статистических данных, осуществляемый органами государственной статистики или государственными организациями, уполномоченными на ведение государственной статистики, в целях формирования официальной статистической информации.

Официальная статистическая информация - информация об экономическом, демографическом, социальном положении и о состоянии окружающей среды в Республике Беларусь, сформированная путем обработки первичных статистических и (или) административных данных, иной информации в соответствии с официальной статистической методологии.

Согласно ст. 17 Закона «О государственной статистике» органы государственной статистики ведут государственную статистику по формам централизованных государственных статистических наблюдений и указаниям по их заполнению и (или) с использованием административных данных, иной информации, а также в соответствии с методиками по формированию и расчету статистических показателей и инструкциями по организации и проведению государственных статистических наблюдений, утверждаемыми республиканским органом государственного управления в области государственной статистики, и (или) в соответствии с международными стандартами и рекомендациями в области статистики.

При этом под административными данными понимается документированная информация (за исключением первичных статистических данных), получаемая государственными органами и иными организациями в связи с осуществлением государственно-властных полномочий, административных процедур, контрольных (надзорных) и других функций, возложенных на них нормативными правовыми актами, и используемая для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации.

В соответствии со ст. 18 Закона «О государственной статистике» Государственные статистические наблюдения проводятся по формам централизованных и нецентрализованных государственных статистических

наблюдений. Государственные статистические наблюдения могут быть сплошными (проводимыми в отношении всех единиц наблюдаемой совокупности), выборочными (проводимыми в отношении отдельных единиц наблюдаемой совокупности) и комбинированными, систематическими (проводимыми на регулярной основе) и специальными (единовременные, переписи, обследования). Формами государственных статистических наблюдений являются государственная статистическая отчетность; анкета; вопросник; переписной лист; иные формы государственных статистических наблюдений.

Обработка персональных данных, содержащихся в административных данных, а также в формах централизованных государственных статистических наблюдений, осуществляется органами государственной статистики и государственными организациями, уполномоченными на ведение государственной статистики, без согласия субъектов персональных данных.

в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных;

Указанное правовое основание может быть применено при одновременном соблюдении следующих условий:

обработка персональных данных осуществляется в научных или иных исследовательских целях;

персональные данные обезличены.

Понятие «научных целей» не закреплено в Законе Республики Беларусь от 21.10.1996 №708-XIII «О научной деятельности». В ст. 1 Закона установлено, что научная деятельность – это творческая деятельность, направленная на получение новых знаний о природе, человеке, обществе, искусственно созданных объектах и на использование научных знаний для разработки новых способов их применения. Следовательно, научные цели – это те цели, которые направлены на получение новых знаний о природе, человеке, обществе, искусственно созданных объектах и на использование научных знаний для разработки новых способов их применения.

Например, оператор электросвязи передает персональные данные в обезличенном виде (номера телефонов абонентов, отобранных по обозначенным критериям (пол, возраст и др.) организациям, которые аккредитованы согласно постановлению Совета Министров Республики Беларусь от 8 ноября 2005 г. № 1240 «О некоторых вопросах проведения опросов общественного мнения, относящихся к республиканским референдумам, выборам и общественно-политической ситуации в стране, и об опубликовании их результатов в средствах массовой информации», для проведения исследований и опросов общественного мнения.

Понятие «исследовательских целей» в законодательстве не установлено.

при осуществлении учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением и возмещения расходов на электроэнергию, платы за другие услуги и возмещения налогов, а также при предоставлении льгот и взыскании задолженности по плате за

жилищно-коммунальные услуги, плате за пользование жилым помещением и возмещению расходов на электроэнергию;

В соответствии с п. 36 ст. 1 Жилищного кодекса Республики Беларусь к организациям, осуществляющим учет, расчет и начисление платы за жилищно-коммунальные услуги и платы за пользование жилым помещением, относят организации, оказывающие жилищно-коммунальные услуги и (или) осуществляющие функции учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением, возмещения расходов организаций, осуществляющих эксплуатацию жилищного фонда и (или) предоставляющих жилищно-коммунальные услуги, на электроэнергию, потребляемую на освещение вспомогательных помещений и работу оборудования в многоквартирных жилых домах, а также функции по начислению безналичных жилищных субсидий и взысканию задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением, возмещению расходов на электроэнергию.

Согласно подп. 1.1 п. 1 Указа Президента Республики Беларусь от 31 декабря 2015 г. №535 «О предоставлении жилищно-коммунальных услуг» начисление платы за жилищно-коммунальные услуги и платы за пользование жилыми помещениями в жилых домах товариществ собственников либо организаций застройщиков осуществляется с использованием единой общереспубликанской информационной системы по учету, расчету и начислению платы за жилищно-коммунальные услуги и платы за пользование жилым помещением, в том числе через уполномоченные местными исполнительными и распорядительными органами организации, осуществляющие учет, расчет и начисление платы за жилищно-коммунальные услуги и платы за пользование жилым помещением.

при получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

Это самое используемое на практике основание. Тип договора в Законе не указан, но такое основание не применяется в отношении трудовых договоров. Данное основание применимо, если субъект персональных данных является (будет являться) стороной по договору, заключенному (заключаемому) с оператором, оператор осуществляет обработку тех персональных данных физического лица, которые указаны в договоре либо получены в процессе его заключения (исполнения); оператор осуществляет обработку персональных данных физического лица только для целей совершения действий, установленных договором, то есть, когда обработка персональных данных является необходимой для оказания услуг, выполнения работ, совершения действий в отношении конкретного физического лица, и без обработки таких данных выполнение обязательств по договору невозможно или существенно затруднено.

Рассматриваемое основание применяется как в случае обработки персональных данных на основании заключенного договора, так и в случае

обработки персональных данных субъекта персональных данных на стадии заключения договора. При этом на возможность применения данного основания не влияет тот факт, что в итоге договор с субъектом персональных данных может быть не заключен.

Например, между оператором и субъектом персональных данных заключен договор купли-продажи, по которому оператор обязан осуществить доставку товаров. Для этой цели оператор может обрабатывать имя, фамилию, адрес места жительства и (или) номер телефона субъекта персональных данных.

Еще примерами могут быть оставление заявки на сайте с контактными данными гражданина для связи и уточнения условий оказания услуг, продажи товаров, обсуждения стоимости и др.; принятие условий пользовательского соглашения на сайте (публичного договора между владельцем интернет-ресурса и пользователем), например, посредством регистрации учетной записи на интернет-ресурсе.

Например, информирование (напоминание) субъекта персональных данных о сроках исполнения договора; осуществление гарантийного и постгарантийного обслуживания;

Не могут рассматриваться в качестве обработки для целей исполнения договора способы обработки, не являющиеся необходимыми для исполнения договора. Например, обработка оператором персональных данных субъекта персональных данных с целью направления ему информации рекламного характера.

В случае неисполнения одной из сторон условий договора другая сторона может осуществлять обработку персональных данных в целях защиты своих прав, например составления искового заявления в суд (абз. 20 ст. 6 Закона).

при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа;

Такое основание может быть применено, если:

документ адресован оператору;

документ подписан субъектом персональных данных (собственноручно либо с использованием электронной цифровой подписи или иных технических средств, компьютерных программ, информационных систем или информационных сетей, если такой способ подписания позволяет достоверно установить, что документ подписан субъектом персональных данных);

обработке подлежат те персональные данные, которые указаны в документе;

обработка осуществляется для целей, указанных в документе.

Примером обработки персональных данных на данном основании является подача работниками заявлений на оказание материальной помощи, частичное возмещение стоимости путевок в санаторно-курортные и оздоровительные учреждения, компенсацию стоимости подписки, абонементов и т.п.

Следует отметить, что указанное основание не применяется в случаях, когда в организацию поступает документ, подписанный субъектом персональных данных, но необходимость направления такого документа (заявления) вытекает из законодательных актов и (или) форма такого документа устанавливается законодательством. Кроме того, оно не применяется, если форма заявления и круг указываемых в нем персональных данных определяются оператором, иначе это даст возможность операторам "обходить" требования Закона.

в целях осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации, организации, осуществляющей издательскую деятельность, направленных на защиту общественного интереса, представляющего собой потребность общества в обнаружении и раскрытии информации об угрозах национальной безопасности, общественному порядку, здоровью населения и окружающей среде, информации, влияющей на выполнение своих обязанностей государственными должностными лицами, занимающими ответственное положение, общественными деятелями, за исключением случаев, предусмотренных гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса;

Данное основание может быть использовано в деятельности журналиста, средства массовой информации, а также организации, осуществляющей издательскую деятельность, и предназначено для установления баланса между правом на защиту персональных данных и правом на свободу журналисткой деятельности в части поиска информации. Обработка персональных данных этими лицами допускается без согласия субъектов персональных данных в случаях, когда имеется превалирование общественных интересов над личными правами.

Это основание неприменимо для блогеров независимо от того, какое количество подписчиков у них имеется, а также для информационных ресурсов, не зарегистрированных в качестве сетевого издания.

Это основание не применяется в случаях, когда обработка персональных данных не обусловлена защитой общественного интереса, например при осуществлении фото- и видеосъемок на праздниках, юбилеях, при обычных интервью и т.п. В подобных ситуациях обработка персональных данных должна осуществляться на ином правовом основании (например, на основании абзаца двадцатого ст. 6 Закона).

Основание не применяется к случаям обработки персональных данных, предусмотренным гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса.

для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

Данное основание имеет устоявшуюся узкую трактовку и применяется в очень редких ситуациях, когда имеется прямая угроза жизни, например при оказании неотложной медицинской помощи (когда лицо не в состоянии выразить согласие по причине болезненного, бессознательного состояния и т.п.), в гуманитарных целях (контроль эпидемий и их распространения и т.п.) или в чрезвычайных ситуациях гуманитарного характера (техногенные или природные катастрофы, стихийное бедствие и т.п.), в иных исключительных ситуациях.

Для его применения необходимо одновременное соблюдение двух условий:

обработка персональных данных необходима для целей защиты жизни, здоровья или иных жизненно важных интересов либо самого субъекта персональных данных, либо иных лиц;

получение согласия субъекта персональных данных на обработку персональных данных невозможно.

Например, субъект персональных данных поступает в тяжелом состоянии в больницу и не может дать согласие на обработку персональных данных. Работники больницы в целях защиты его жизни вправе осуществить обработку его медицинских и иных данных. Еще одним примером может быть установка в подъезде жилого дома в целях обеспечения сохранности имущества по решению более половины собственников квартир камеры видеонаблюдения. Обработка персональных данных субъектов персональных данных, чье видеоизображение попало в объектив камеры, не может осуществляться на основании рассматриваемой нормы, поскольку собственники остальных квартир, которые не выражали согласия или не принимали участие в опросе, и другие субъекты персональных данных не лишены юридической возможности дать согласие на обработку их персональных данных.

в отношении распространенных ранее персональных данных до момента заявления субъектом персональных данных требований о прекращении обработки распространенных персональных данных, а также об их удалении при отсутствии иных оснований для обработки персональных данных, предусмотренных настоящим Законом и иными законодательными актами;

Данное основание может быть применено только в отношении общедоступных персональных данных, которые ранее были распространены на законных основаниях (самим субъектом, с его согласия или в соответствии с требованиями законодательных актов), и не легитимирует обработку персональных данных, распространенных в результате совершения преступления или иного правонарушения. При этом оценка законности распространения общедоступных персональных данных с учетом риск-ориентированного подхода является обязанностью оператора, применяющего данное правовое основание для обработки. При наличии сомнений оператор может принимать дополнительные меры для уточнения факта законности распространения персональных данных.

Если субъект персональных данных заявил требование о прекращении обработки распространенных персональных данных, а также об их удалении,

их обработка должна быть прекращена, если у оператора не имеется иных оснований для обработки персональных данных, предусмотренных Законом или иными законодательными актами.

в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;

Обработку персональных данных по данному основанию могут осуществлять как государственные органы для выполнения своих задач и функций, так и иные организации при выполнении возложенных на них обязанностей (полномочий). Рассматриваемое основание как основание более общего порядка применяется при отсутствии конкретизирующего его основания в ст. 6 Закона. В этой связи, если обработка персональных данных подпадает под иное основание, предусмотренное ст. 6 Закона применительно к конкретной сфере деятельности, то оно не применяется;

в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

В Законе предусмотрена возможность обработки персональных данных по поручению оператора. В качестве такого субъекта выступает уполномоченное лицо – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах. Уполномоченное лицо может выступать в качестве такового на основании следующего:

– акта законодательства (например, согласно п. 2 Инструкции, утвержденной Постановлением Министерства образования Республики Беларусь от 16.04.2019 № 36 «О порядке формирования и ведения единой базы данных обучающихся в учреждениях образования Республики Беларусь» «база данных обучающихся является государственным информационным ресурсом, владельцем которого является Министерство образования, а оператором - учреждение «Главный информационно-аналитический центр Министерства образования Республики Беларусь»);

– решения государственного органа, являющегося оператором;

– договора с оператором.

Последнее основание наиболее часто используется на практике. Это может быть как самостоятельный договор, так и раздел / глава в действующем договоре (например, в договоре оказания бухгалтерских услуг), так как правоотношения «оператор-уполномоченное лицо» возникают в момент заключения основного договора.

В п. 1 ст. 7 Закона указаны пункты, которые должны содержаться в договоре между оператором и уполномоченным лицом:

цели обработки персональных данных;

В данном пункте необходимо указать цели, которые будут соответствовать целям, которые указаны субъекту персональных данных при обработке его персональных данных. В качестве примера может быть «подача данных в Фонд социальной защиты населения».

перечень действий, которые будут совершаться с персональными данными уполномоченным лицом;

В данном пункте целесообразно указать конкретные действия, например, «внесение персональных данных в 1С «Бухгалтерия», «актуализация персональных данных с учетом представление оператором обновленных персональных данных пользователей»).

обязанности по соблюдению конфиденциальности персональных данных;

меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона.

Как указывает НЦЗПД, в договоре также целесообразно предусмотреть:

условия о возможности привлечения уполномоченным лицом иных лиц для обработки персональных данных или о запрете таких действий;

механизм участия уполномоченного лица в выполнении оператором обязанностей перед субъектами персональных данных;

обязанность уполномоченного лица прекратить по окончании договора обработку соответствующих персональных данных и передать такие данные оператору либо удалить (блокировать) их.

Под трансграничной передачей персональных данных понимается передача персональных данных на территорию иностранного государства обязательно с территории Беларуси. Порядок трансграничной передачи персональных данных установлен ст. 9 Закона. Особенностью трансграничной передачи является «столкновение» двух юрисдикций: белорусской и иностранного государства, на территорию которого передаются персональные данные. Важно, что «транзит» через территорию иных государств без доступа к содержанию передаваемой информации и ее сохранения не является трансграничной передачей персональных данных. При этом не может рассматриваться как трансграничная передача персональных данных регистрация гражданином в социальной сети, на сайте, заказ билетов у зарубежной авиакомпании, покупка товаров в Aliexpress вне зависимости от мессенджера или вида поисковой системы.

Примерами трансграничной передачи могут быть использование облачной инфраструктуры для персональных данных, когда соответствующие серверы размещаются за пределами Беларуси; направление организацией, входящей в группу компаний, персональных данных работников материнской компании, расположенной в другой стране; хранение собранных данных клиентов на Google Диск, Яндекс Диск.

Размещение персональных данных на сайте, где иностранный пользователь может скачать персональные данные или их просмотреть, не является трансграничной передачей. Это будет рассматриваться как распространение и требует наличия надлежащего правового основания.

Порядок трансграничной передачи персональных данных определяется от категории государства, в которую они передаются: с надлежащим уровнем защиты прав субъектов персональных данных или без него. Категоризация определяется в приказе директора НЦЗПД от 15.11.2021 г. № 14 «О трансграничной передаче персональных данных» на основании признания государства стороной Конвенции о защите физических лиц при автоматизированной обработке персональных данных, принятой в г. Страсбурге 28 января 1981 года. На сегодняшний день 55 стран являются сторонами Конвенции о защите физических лиц при автоматизированной обработке персональных данных. В качестве еще одного критерия выступает членство в Евразийском экономическом союзе (далее – ЕАЭС). Например, Казахстан не является стороной Конвенции, но является членом ЕАЭС. При соблюдении одного из критериев, трансграничная передача персональных данных осуществляется без ограничений как иной вид обработки. Однако необходимо указывать в документах оператора информацию о трансграничной передаче персональных данных, в том числе с указанием в согласии на обработку персональных данных.

Трансграничная передача персональных данных запрещается, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных (например, США, Китай), за исключением случаев, когда:

– дано согласие субъекта персональных данных при условии, что субъект персональных данных проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты (*Это может быть реализовано как путем добавления дополнительной информации в согласие, либо получения отдельного согласия на трансграничную передачу. В качестве рисков может быть отсутствие (ограниченность) законодательства о персональных данных, фактическая неприменяемость такого законодательства на практике, отсутствие уполномоченного органа по защите прав субъектов персональных данных, отсутствие или ограниченность прав субъектов персональных данных, неопределенность оснований для обработки персональных данных, возможность широкого доступа к таким данным органов безопасности, отсутствие мер ответственности за нарушения в сфере обработки персональных данных, отсутствие обязательных требований о технической и криптографической защите информационных систем (ресурсов), содержащих персональные данные.)*;

– персональные данные получены на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором (*например, при заключении договора на оказание туристических услуг с субъектом персональных данных, по которому его персональные данные передаются иностранному отелю*);

– персональные данные могут быть получены любым лицом посредством направления запроса в случаях и порядке, предусмотренных законодательством

(*например, получение выписки из единого государственного регистра юридических лиц и индивидуальных предпринимателей*);

– такая передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь (*например, в рамках Соглашений в области образования*);

– такая передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения в соответствии с законодательством;

– получено соответствующее разрешение уполномоченного органа по защите прав субъектов персональных данных.

Порядок получения разрешения установлен приказом директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 «О трансграничной передаче персональных данных». В приказе установлено два вида разрешений: разрешение в силу определенного статуса оператора и на основании заявления. Разрешение в силу определенного статуса субъекта предусмотрено при размещении государственными органами, государственными организациями, а также хозяйственными обществами, в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами, информации о своей деятельности в глобальной компьютерной сети Интернет, а также в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами.

Для получения разрешения необходимо подать в НЦЗПД заявление с приложением проекта договора, которым оформляется трансграничная передача персональных данных, согласованный заявителем и получателем персональных данных, на дату, предшествующую дате подачи заявления, либо иной документ, в соответствии с которым предполагается осуществлять передачу персональных данных. Срок рассмотрения заявления – 30 дней со дня его регистрации. В ходе рассмотрения заявления и прилагаемых к нему документов изучается информация об уровне защиты прав субъектов персональных данных на территории иностранного государства. Разрешение выдается при условии обеспечения защиты прав субъектов персональных данных на уровне не ниже, чем это предусмотрено законодательством Республики Беларусь.

После получения разрешения не допускается внесение изменений в проект договора либо в иной документ, в соответствии с которым предполагается осуществлять передачу персональных данных, в части изменения целей обработки, категорий обрабатываемых персональных данных, срока хранения

получателем персональных данных. Изменение этих сведений после подписания договора подлежит согласованию с НЦЗПД в порядке, предусмотренном для выдачи разрешения.

В качестве оснований для отказа в выдаче разрешения можно назвать следующее:

– ликвидация (прекращение деятельности), смерть заявителя, получателя персональных данных;

– персональные данные обрабатываются в нарушение требований Закона;

– представленные документы и (или) сведения не позволяют сделать вывод о надлежащей защите прав субъектов персональных данных, в том числе когда правовые, организационные и технические меры, принимаемые получателем персональных данных, не являются достаточными для обеспечения защиты прав субъектов персональных данных на уровне не ниже, чем это предусмотрено законодательством Республики Беларусь.

Разрешение может быть отозвано НЦЗПД в любой момент до окончания трансграничной передачи в случае:

– нарушения заявителем или получателем персональных данных условий, в соответствии с которыми осуществлялась выдача разрешения;

– получения информации, подтверждающей, что на территории иностранного государства не обеспечивается уровень защиты персональных данных не ниже, чем это предусмотрено законодательством Республики Беларусь.

Трансграничная передача персональных данных после отзыва разрешения запрещается.

В некоторых областях, например, медицина или образование НЦЗПД разработаны рекомендации с учетом специфики деятельности.

Рекомендации по обработке персональных данных в сфере здравоохранения подготовлены НЦЗПД совместно с ГУ «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения» с использованием правовых актов по состоянию на 18 октября 2024 г. Для формирования представления об обработке персональных данных в области здравоохранения сформируем несколько ключевых пунктов.

– Обработка персональных данных осуществляется с учетом законодательства о здравоохранении и законодательства о защите персональных данных.

– Персональные данные, касающиеся здоровья человека, относятся к специальным персональным данным, для которых установлен особый режим обработки.

– Сведения о состоянии здоровья пациента, содержащиеся в биологических образцах (кровь, слюна, соскоб слизистой рта, выделения из половых органов, околоплодной жидкости, волосы, ногти и т.д.), медико-генетических заключениях, медицинских справках о состоянии здоровья

содержат информацию о физиологии и здоровье человека, однако не обладают уникальностью и не относятся к генетическим персональным данным.

– В качестве правовых оснований обработки персональных данных может выступать, например, оказание медицинской помощи гражданам, выдача справок и иных документов в рамках осуществления административных процедур, осуществление действий в рамках гражданско-правовых договоров.

– Учреждение здравоохранения с одним пациентом может выступать как в качестве уполномоченного лица, так и в качестве оператора. (*Например, при оказании медицинских услуг медицинское учреждение по конкретному договору добровольного страхования медицинских расходов осуществляют обработку персональных данных в интересах страховщика (оператора) и выступает в качестве уполномоченного лица. Это опосредовано тем фактом, что медицинское учреждение не определяет ключевые параметры обработки персональных данных (они определены в договоре) и действует в интересах страховой организации в соответствии с ее поручениями за вознаграждение. При оказании непосредственно медицинской помощи застрахованному лицу и ведении медицинской документации медицинское учреждение является самостоятельным оператором.).*

– В качестве субъекта персональных данных могут выступать пациенты, их близкие родственники и законные представители, доноры, посетители.

– Основание обработки персональных данных «в целях оказания медицинской помощи» распространяется на обработку персональных данных не только медицинским, фармацевтическим или иным работником здравоохранения, но и дезинфекторами, медицинскими регистраторами, сестрами-хозяйками, бухгалтерами, юрисконсультами.

– При заведении электронной медицинской карты необходимо получать согласие пациента (то есть для внесения сведений в информационные ресурсы (информационные системы)), при ведении медицинской карты только на бумажном носителе получать его не нужно. В качестве примера внесения сведений в информационный ресурс может быть компьютерный томограф, магнитно-резонансный томограф.

– Пациент вправе отозвать свое согласие на внесение персональных данных в информационную систему, однако в такой ситуации учреждение здравоохранения вправе осуществлять обработку обезличенных данных (информации) пациента в целях обеспечения полноты и достоверности статистического учета данных о случаях оказания медицинской помощи пациентам.

– Обработка персональных данных пациента, в том числе с помощью средств автоматизации, при оказании ему экстренной медицинской помощи осуществляется без согласия пациента, если она обусловлена этой целью и получение согласия невозможно. Вместе с тем, как только пациент физически может дать согласие, оно должно быть получено, если обработка осуществляется с использованием средств автоматизации.

– Согласие на обработку персональных данных не приравнивается к согласию на медицинское вмешательство.

– Отказ в оказании медицинской помощи в связи с отказом пациента в даче согласия на обработку персональных данных или отзыве ранее данного согласия не допускается.

– Передача сведений о пациентах из одной организации здравоохранения в другую (например, выписки из медицинских документов) является составным элементом организации оказания медицинской помощи и может быть осуществлена без их согласия.

– Учреждение здравоохранения может предоставлять персональные данные пациентом третьим лицам при наличии в запросе цели обработки персональных данных, объема и содержания запрашиваемых персональных данных, правовое основание на обработку персональных данных пациентов со ссылкой на конкретную норму законодательного акта, которая наделяет ее обязанностью (полномочием), требующей обработки персональных данных или специальных персональных данных. Если правовым основанием для обработки персональных данных является согласие субъекта персональных данных, то запрос направляется с приложением копии согласия. Не подпускается в качестве основания использовать следующие формулировки: служебная необходимость, укрепление межведомственного взаимодействия, проведение воспитательной работы.

– Учреждение здравоохранения может осуществлять трансграничную передачу персональных данных, например, направление организацией здравоохранения персональных данных пациентов, работников в организации, расположенные в другой стране; хранение файлов, содержащих персональные данные, на Google Диск, Яндекс Диск; использование Viber и иных мессенджеров для передачи персональных данных. Трансграничная передача осуществляется в общем порядке в соответствии с законодательством о защите персональных данных.

– При использовании в учреждении здравоохранения информационных систем должна соблюдаться Инструкция о порядке разработки, формирования, ведения, эксплуатации информационных систем, информационных ресурсов, баз (банков) данных и (или) реестров (регистров) в здравоохранении, входящих в состав централизованной информационной системы здравоохранения, требования к ним, порядке их взаимодействия с централизованной информационной системой здравоохранения, утвержденная Постановлением Министерства здравоохранения Республики Беларусь от 31 июля 2021 г. № 91. В п. 6 данной Инструкции указаны критерии, которые применяются в отношении таких систем: (1) она должна располагается на серверах на территории Беларуси, и быть зарегистрирована в соответствии с законодательством об информации, информатизации и защите информации; (2) должны использоваться средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам

государственной экспертизы, проводимой Оперативно-аналитическим центром при Президенте Республики Беларусь.

Рекомендации по обработке персональных данных в сфере образования подготовлены в виде нескольких документов: Информация о применении Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» в сфере образования (24.08.2022), О применении Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (17.03.2023 №5-13/93), Разъяснения о применении законодательства о персональных данных в деятельности учреждений среднего специального и высшего образования. Для формирования представления об обработке персональных данных в области образования сформируем несколько ключевых пунктов.

– Часто обработка персональных данных обусловлена наличием законодательного правомочия. Например, не нужно брать согласие в целях осуществления обучения и воспитания, в целях физического воспитания, ведения классных журналов и дневников учащегося, участие в олимпиадах, конкурсах, турнирах, фестивалях, конференциях, спортивно-массовой, общественной, научной деятельности.

– Обработка персональных данных учреждениями образования для целей ведения электронного дневника и журнала осуществляется без согласия субъекта персональных данных (его законных представителей) на основании абз. 20 ст. 6 Закона в целях реализации обязанностей (полномочий), предусмотренных законодательными актами.

– Истребование для целей заключения договора с субъектом персональных данных ксерокопий отдельных страниц паспорта, иных документов, подаваемых в приемную комиссию в оригинале, не допускается, за исключением случаев, прямо предусмотренных Правилами приема в учреждения среднего специального и Правилами приема в учреждения высшего образования.

– Согласие субъекта персональных данных не требуется при размещении в общедоступных списках персональных данных (фамилии, собственного имени, отчества (если таковое имеется) обучающихся, принятых (зачисленных) для получения образования. В качестве правового основания выступает абз. 20 ст. 6 Закона.

– На территории учреждения образования устанавливаются видеокамеры для целей обеспечения общественной безопасности и общественного порядка. Для установки камер видеонаблюдения в учреждении образования, в том числе в учебных аудиториях, для других целей также необходимо правовое основание.

– Трансграничная передача персональных данных обучающихся в рамках соглашения о сотрудничестве и академической мобильности между учреждением образования Республики Беларусь и учреждением образования такого иностранного государства при наличии международного договора о сотрудничестве в сфере образования, наделяющего учреждения образования сторон договора правом определять конкретные формы сотрудничества, осуществляется на основании абз. 6 п. 1 ст. 9 Закона, а при отсутствии названного договора – с согласия субъекта персональных данных на основании абз. 2 п. 1 ст.

9 Закона. Правовым основанием трансграничной передачи персональных данных преподавателей и других работников учреждения образования для целей академической мобильности в случае, если участие этих лиц в мероприятии обусловлено выполнением поручения нанимателя в рамках трудовых функций работников, в том числе при направлении их в командировку, выступает абз. 8 п. 1 ст. 9 Закона.

– Размещение фото и видеоизображения, в том числе несовершеннолетних лиц, государственными учреждениями образования осуществляется в соответствии с п. 7 Положения о порядке функционирования интернет-сайтов государственных органов и организаций, утвержденным постановлением Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645. Частные учреждения образования также могут применять указанное положение в своей деятельности. Если съемка производится учреждением образования на публичном мероприятии или в месте, открытом для свободного посещения, изображение ребенка не должно быть основным объектом на снимке, фотография должна отражать именно проводимое мероприятие. В случае, если акцент делается на изображении ребенка, то для размещения таких фотографий или видеоизображения необходимо получать согласие участника мероприятия (в отношении несовершеннолетнего в возрасте до 16 лет – согласие одного из его законных представителей).

– Размещение информации, содержащей персональные данные, в создаваемых обучающимися, их родителями группах в мессенджерах, то данные отношения, несмотря на наличие обработки с использованием средств автоматизации, не являются предметом регулирования Закона. Такая обработка персональных данных осуществляется указанными лицами в процессе исключительно личного использования и не связана с их профессиональной или предпринимательской деятельностью.

Еще одной немаловажной сферой, где обрабатывается большое количество персональных данных – трудовые отношения. Для правильного применения Закона НЦЗПД разработаны Рекомендации об обработке персональных данных в связи с трудовой (служебной) деятельностью. Отметим несколько ключевых моментов, которые необходимо учитывать:

(1) Согласие, как правило, не может выступать правовым основанием для обработки нанимателем персональных данных работников (работник находится в подчиненном положении, и согласие не носит свободного характера). Также следует помнить про абз. 8 ст. 6 и абз. 3 п. 2 ст. 8 Закона, в которых указано, что не требуется согласие при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством.

(2) В некоторых случаях согласие субъекта персональных данных может выступать в качестве правого основания обработки персональных данных, например, при рассмотрении резюме соискателей на трудоустройство. Среди иных оснований может быть обработка персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом

персональных данных, в соответствии с содержанием такого документа; обработка персональных данных, когда такая обработка является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами.

(3) В соответствии с абзацем восьмым статьи 6 и абзацем третьим пункта 2 статьи 8 Закона согласие субъекта персональных данных на обработку персональных данных, в том числе специальных персональных данных, не требуется при оформлении трудовых (служебных) отношений в случаях, предусмотренных законодательством.

Так, статьей 26 Трудового кодекса Республики Беларусь (далее – Трудовой кодекс) установлен перечень документов, которые наниматель обязан потребовать, а гражданин должен предъявить нанимателю при заключении трудового договора.

Кроме указанных в данной статье документов к ним относятся и другие документы о подтверждении иных обстоятельств, имеющих отношение к работе, если их предъявление предусмотрено законодательными актами.

Так, для отдельных категорий работников при приеме на работу законодательными актами установлено обязательное прохождение предварительного медицинского осмотра. Соответственно, при оформлении с ними трудовых (служебных) отношений требуется представление медицинской справки о состоянии здоровья.

Например, такое требование установлено законодательными актами для лиц моложе восемнадцати лет, педагогических работников, лиц, занятых на работах с вредными и (или) опасными условиями труда или на работах, где в соответствии с законодательством есть необходимость оценки состояния здоровья работающего на предмет его годности (негодности) к выполнению отдельных видов работ, лиц, принимаемых на работу по профессиям рабочих (должностям служащих) работников организаций железнодорожного транспорта общего пользования, непосредственно обеспечивающих перевозочный процесс, и т.п.).

При назначении на отдельные должности законодательными актами предусмотрена процедура согласования.

(4) В одних случаях обработка персональных данных прямо предусматривается в актах законодательства, равно как и перечень обрабатываемых персональных данных. Например, постановлением Министерства труда и социальной защиты Республики Беларусь от 16 июня 2014 г. № 40 «О трудовых книжках» установлены образец трудовой книжки и форма книги учета движения трудовых книжек и вкладышей к ним.

Инструкцией о порядке формирования, ведения и хранения личных дел работников, утвержденной постановлением Комитета по архивам и делопроизводству при Совете Министров Республики Беларусь от 26 марта 2004 г. № 2, установлены формы личного листка по учету кадров, дополнения к личному листку по учету кадров, журнала (книги) учета личных дел, контрольной карточки.

В иных случаях у нанимателя остается определенная степень усмотрения в части круга обрабатываемых сведений.

(5) Не требуется получение согласия на обработку персональных данных и в тех случаях, когда обработка персональных данных и их перечень прямо не называются в акте законодательстве, но на нанимателя возлагаются определенные обязанности, требующие использования персональных данных.

Например, Трудовой кодекс возлагает на нанимателя обязанности:

выдавать заработную плату в сроки и размерах, установленных законодательством, коллективным договором, соглашением или трудовым договором;

предоставлять работникам гарантии и компенсации (в связи с беременностью, наличием детей, инвалидностью, при служебных командировках, в связи с переездом на работу в другую местность и т.п.);

расторгнуть срочный трудовой договор досрочно по требованию работника в случае наличия уважительных причин, препятствующих выполнению работы по трудовому договору;

предоставлять работникам трудовые и социальные отпуска, в том числе планировать трудовой отпуск в определенное время отдельным категориям работников;

затребовать письменное объяснение работника до применения дисциплинарного взыскания, до издания распоряжения нанимателя об удержании из заработной платы для возмещения ущерба, причиненного работником, и т.п.

(6) Обработка персональных данных работников при реализации мер, направленных на исполнение нанимателями обязанностей (например, ведение телефонных справочников с указанием фамилии, собственного имени, отчества, должности, рабочего телефона, сайтов общего доступа работников, иных инструментов делового сотрудничества и обмена информацией между работниками, указание фамилии, собственного имени, отчества и должности на дверях кабинетов и т.п.), также может осуществляться без получения согласия работников на основании абзаца восьмого статьи 6 Закона.

Если трудовая функция работника предусматривает необходимость его внешнего взаимодействия (с клиентами, контрагентами в рамках подписанных между организациями договоров и т.п.) с указанием его персональных данных, то предоставление (нанимателем) и обработка (организацией, с которой наниматель взаимодействует) персональных данных такого работника могут осуществляться без согласия работника на основании абзаца восьмого статьи 6 Закона.

(7) Что касается размещения информации о работниках на интернет-сайтах организаций, то такая необходимость (возможность) может быть обусловлена законодательством.

Например, требования о размещении сведений об отдельных категориях работников на интернет-сайтах организаций установлены статьей 22-1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации,

информатизации и защите информации», Указом Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» и принятым в его развитие постановлением Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645, которым утверждено Положение о порядке функционирования интернет-сайтов государственных органов и организаций.

(8) Как обработку на основании абзаца восьмого статьи 6 Закона следует рассматривать в том числе случаи награждения работников грамотами, благодарностями, занесения работника на Доску Почета.

(9) Обработка личной информации работника, не связанной с исполнением трудовых обязанностей (ей могут являться личные адреса электронной почты, аккаунты в социальных сетях, религиозные взгляды, участие в общественной деятельности, сведения о родственниках, если их предоставление не предусмотрено законодательством, и т.п.) не может рассматриваться как обработка в процессе трудовой (служебной) деятельности в соответствии с абзацем восьмым статьи 6 и абзацем третьим пункта 2 статьи 8 Закона.

При этом в отношении обработки информации о дате рождения работника необходимо учитывать следующее.

При приеме на работу работник представляет нанимателю сведения о дате рождения (заполняется в личном листке по учету кадров) для целей трудовых отношений и в предусмотренных законодательством случаях могут использоваться без согласия работника (предоставление предусмотренных законодательством (коллективным договором) гарантий, решение вопросов, связанных с пенсионным обеспечением, и т.п.).

Если информация о дате рождения работника используется в рамках организации в целях исключительно личного и иного подобного использования, не связанного с профессиональной деятельностью работника (например, для поздравления работника коллегами), то на такие отношения в соответствии со статьей 2 Закона его действие не распространяется. При этом обращаем внимание, что основания для получения сведений о днях рождения работников для таких целей в кадровой службе организации без согласия работника отсутствуют. Данные сведения могут быть получены у самого работника.

(10) В отношении необходимости получения от работников обязательства о неразглашении персональных данных. Подписание обязательства, как необходимого документа, влекущего определенные правовые последствия, осуществляется в случаях, прямо предусмотренных законодательством. В частности, такие требования установлены в статье 16 Закона Республики Беларусь от 15 июля 2015 г. № 305-З ”О борьбе с коррупцией“ и в статье 17 Закона Республики Беларусь от5 января 2013 г. № 16-З ”О коммерческой тайне“.

Законом подписание работниками обязательства о неразглашении персональных данных не предусматривается.

(11) В случае если на основании договора обработка персональных данных работников от имени нанимателя и в его интересах поручена уполномоченному лицу (например, при ведении кадровой работы, бухгалтерского учета),

наниматель и уполномоченное лицо обязаны соблюдать требования статьи 7 Закона. При этом, исходя из положений статей 5 и 7 Закона, если получение оператором согласия на обработку персональных данных работников не требуется, поскольку обработка осуществляется на ином правовом основании, предусмотренном Законом, то, соответственно, не требуется получение согласия на привлечение к обработке персональных данных уполномоченного лица.

Если же обработка персональных данных работников осуществляется на основании их согласия, то, исходя из статьи 5 Закона, до получения согласия на обработку персональных данных оператор должен предоставить информацию об уполномоченных лицах, которым поручается обработка.

(12) Наниматели могут предоставить соискателям возможность подачи резюме на своих интернет-ресурсах, в том числе заполнить разработанную ими анкету. В данном случае наниматель, выступающий оператором, должен получить согласие субъекта персональных данных на обработку его персональных данных, например, посредством проставления соответствующей отметки на интернет-ресурсе.

Кроме того, для обеспечения действительности полученного согласия согласно пункту 5 статьи 5 Закона до получения согласия субъекта персональных данных оператор обязан предоставить субъекту персональных данных необходимую информацию, содержащую в том числе перечень действий с персональными данными, на совершение которых дается согласие субъекта персональных данных, общее описание используемых оператором способов обработки персональных данных, срок, на который дается согласие субъекта персональных данных.

Получение согласия не освобождает от необходимости соблюдения иных положений Закона, в частности, о необходимости обеспечения соответствия содержания и объема обрабатываемых персональных данных заявленным целям их обработки, исключения избыточности обрабатываемых персональных данных по отношению к заявленным целям их обработки.

Распространенными нарушениями в этом контексте являются случаи, когда форма резюме, составленная нанимателем, предусматривает сбор данных о кандидате, которые не имеют отношения к выполнению планируемой работы, например, сбор информации о его родственниках, размере заработной платы на предыдущем месте работы, указание идентификационного номера, если это не предусмотрено законодательством.

(13) При направлении резюме потенциальному нанимателю в письменной форме, подписанной субъектом персональных данных, либо представлении такого документа в ходе личного приема порядок работы с резюме зависит от используемого алгоритма его обработки.

Если потенциальный наниматель знакомится с полученным таким образом резюме без внесения соответствующей информации в картотеки, списки, базы данных, журналы и т.п., то такая обработка персональных данных согласно пункту 1 статьи 2 Закона не является предметом регулирования Закона,

поскольку в данном случае отсутствует систематизация персональных данных по определенным критериям.

(14) При направлении резюме на электронную почту потенциального нанимателя правовым основанием для его обработки выступает согласие субъекта персональных данных. В этой связи наниматель, получивший резюме таким способом, для его рассмотрения должен принять меры для получения от соискателя согласия на обработку его резюме, например, путем направления соответствующей информации на адрес электронной почты, с которой получено резюме. В противном случае резюме подлежит удалению.

(15) Срок хранения документов лиц, не принятых на работу (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и т.п.), составляет 1 год.

(16) В случаях, предусмотренных законодательством, обработка персональных данных близких родственников (членов семьи) работника осуществляется без их согласия на основании абзаца восьмого статьи 6 Закона. Например, предоставление сведений о близких родственниках и (или) членах семьи работника предусмотрено законодательством о труде (например, при предоставлении социального отпуска при рождении ребенка, компенсаций в связи с переездом на работу в другую местность и т.п.).

(17) В отношении уволенных работников правовыми основаниями для предоставления персональных данных без их согласия третьим лицам в зависимости от ситуации могут, в частности выступать абзацы одиннадцатый и двадцатый статьи 6 Закона.

Например, Налоговым кодексом Республики Беларусь установлена обязанность налоговых агентов представлять по требованию налоговых органов документы и (или) информацию, необходимые для осуществления контроля за правильностью исчисления, удержания и перечисления в бюджет соответствующих налогов, сборов (пошлин) (подпункт 3.3 пункта 3 статьи 23 Налогового кодекса).

В случае направления запроса о предоставлении персональных данных работников запрашивающий орган (организация) должен указать правовые основания для запроса, цель обработки, содержание и объем запрашиваемых персональных данных. При этом если правовым основанием для обработки персональных данных является согласие субъекта персональных данных, то запрос направляется с приложением копии согласия.

Если правовые основания в запросе не указаны, то персональные данные работника могут быть представлены третьему лицу только при условии получения нанимателем от работника согласия на обработку его персональных данных для этой цели.

(18) Как правило, дополнительные трудовые и иные гарантии для работников устанавливаются в коллективном договоре организации, сторонами которого являются работники организации в лице их представительного органа (профсоюзной организации) и наниматель или уполномоченный им представитель (статья 363 Трудового кодекса).

Примерами таких гарантий могут быть оказание материальной помощи, в том числе бывшим работникам, выплаты к праздничным и юбилейным датам, организация оздоровления, добровольное медицинское страхование и т.п.

Статьей 365 Трудового кодекса установлено, что коллективный договор распространяется на нанимателя и работников, от имени которых он заключен. Положения коллективного договора о рабочем времени и времени отдыха, регулировании внутреннего трудового распорядка, нормах труда, формах, системах, размерах оплаты труда, сроках выплаты и порядке индексации заработной платы, охране труда, гарантиях и компенсациях, предоставляемых в соответствии с законодательством, применяются в отношении всех работников организации. Действие иных положений коллективного договора распространяется на работников, от имени которых он не заключался, при условии, что они выразят согласие на это в письменной форме, если иные порядок и условия распространения действия таких положений коллективного договора на указанных работников не определены коллективным договором.

Следует также отметить, что в соответствии со статьей 373 Трудового кодекса все работники, в том числе впервые принятые, должны быть ознакомлены нанимателем с действующими у него коллективными договорами, что соответствует принципу прозрачности обработки персональных данных.

С учетом изложенного обработка персональных данных, которая необходима для выполнения нанимателем и профсоюзной организацией, созданной у нанимателя, обязанностей, предусмотренных коллективным договором, осуществляется без согласия субъектов персональных данных на основании:

абзаца восьмого статьи 6 Закона и абзаца третьего пункта 2 статьи 8 Закона (по специальным персональным данным) – в отношении работников и членов их семей;

абзаца двадцатого статьи 6 Закона и абзаца семнадцатого статьи 8 Закона (по специальным персональным данным) – в отношении бывших работников и членов их семей.

(19) При использовании системы видеонаблюдения осуществляется сбор и фиксация широкого спектра информации (видеонаблюдение независимо от цели затрагивает всех лиц, попадающих в объектив видеокамеры, осуществляется в постоянном режиме, позволяющем выявлять поведенческие признаки субъектов персональных данных, их психологическое состояние и т.п.). В отдельных случаях видеонаблюдение используется в силу прямого требования законодательных актов. Такая обработка персональных данных осуществляется без согласия субъектов персональных данных, в том числе работников.

Например, использование системы видеонаблюдения предусмотрено в случае отнесения объектов к числу подлежащих обязательному оборудованию средствами системы видеонаблюдения за состоянием общественной безопасности. Порядок ее использования и виды соответствующих объектов определены Указом Президента Республики Беларусь от 28 ноября 2013 г. № 527

«О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка».

Если необходимость использования видеонаблюдения напрямую не предусмотрена законодательными актами, оно может использоваться без получения согласия субъектов персональных данных в случае необходимости выполнения обязанностей (полномочий), предусмотренных законодательными актами. Например, обеспечение реализации нанимателем возложенных на него Трудовым кодексом обязанностей, в том числе вытекающих из пункта 2 части первой статьи 55 Трудового кодекса в части обеспечения производственно-технологической, исполнительской и трудовой дисциплины.

Вместе с тем указанные положения не предоставляют нанимателю неограниченных возможностей по использованию видеонаблюдения. В любом случае наниматель должен соблюдать требования статьи 4 Закона, в том числе в части соразмерности обработки персональных данных заявленным целям их обработки, обеспечения справедливого соотношения интересов всех заинтересованных лиц и исключения избыточной обработки, а также учитывать особенности обработки персональных данных, входящих в состав охраняемой законом тайны.

Видеонаблюдение может иметь место при наличии высокой степени рисков, связанных с опасными условиями труда (на строительных площадках, иных травмоопасных производствах и т.п.), работе с материальными ценностями (кассиры на торговых объектах, в банках и т.п.) или связанной с непрерывным обслуживанием клиентов.В то же время видеонаблюдение за офисными работниками, работа которых не обременена подобными факторами (рабочие места считаются безопасными) или выборочно на рабочих местах отдельных (конкретных) работников, выполняющих аналогичные функции, не соответствует требованиям статьи 4 Закона.

Например, использование видеонаблюдения с видеораспознаванием лиц (уникальной идентификацией) в системах управления и контроля доступом в здание при организации пропускного режима и учета явки работников на работу и ухода с нее возможно, как правило, с согласия работников. При этом согласие может быть признано свободным лишь при условии наличия у работников альтернативного варианта входа в здание (по пропускам, карточкам и т. п.). Использование таких систем видеонаблюдения как единственного механизма учета явки работников на работу и ухода с нее может осуществляться только в случаях, когда такой цели нельзя достичь иным способом (например, с использованием карточки) либо когда такое требование прямо предусмотрено в законодательных актах. Подобная обработка биометрических персональных данных может быть оправдана, например, в связи с работой на особо опасных, режимных объектах, объектах военного и специального назначения, в банковской сфере в целях защиты помещений, в которых хранятся денежные средства и иные ценности либо установлены серверы, и т.п. В иных случаях такая модель не отвечает требованию соразмерности (пункт 2 статьи 4 Закона) и влечет риски для прав субъектов персональных данных.

Предоставленная работникам информация должна включать цель видеонаблюдения, места размещения камер и пространство, которое они охватывают, срок хранения видеозаписи и иную информацию, необходимую для обеспечения прозрачности процесса обработки персональных данных, в том числе информацию о праве работника на получение информации об обработке персональных данных (в данном случае в форме видеозаписи) при реализации им права, предусмотренного статьей 11 Закона.

Информация отражается в политику в отношении обработки персональных данных (политику видеонаблюдения), к которой должен быть обеспечен неограниченный доступ, в том числе с использованием глобальной компьютерной сети Интернет. Работники и посетители также должны быть проинформированы о видеонаблюдении с помощью специальных информационных знаков (табличек), размещенных на территории, где оно ведется.

Не допускается использование видеонаблюдения для наблюдения за местами, которые являются частью наиболее личной сферы жизни работников, в том числе предназначенных для их личных нужд, включая отдых и общение работников. Наличие видеонаблюдения в таких объектах может препятствовать их эффективному использованию, оказывать влияние на поведение работников и их взаимодействие друг с другом.

Хранение видеозаписей должно быть ограничено во времени. Целесообразно, чтобы его срок не превышал, как правило, 30 дней, если отсутствуют иные основания для такого хранения (например, необходимость проведения расследования произошедших несчастных случаев на производстве, противоправных действий). Однако в любом случае он не должен быть больше срока достижения заявленной цели обработки персональных данных.

Необходимо также учитывать, что само по себе видеонаблюдение не включает в себя аудиомониторинг (запись голоса). Во время видеонаблюдения отсутствует право прослушивать разговоры работников, кроме исключительных ситуаций (таких как необходимость принятия мер безопасности и т.п.), о которых работники должны быть проинформированы.

Видеозаписи не могут быть использованы в личных и иных целях, не связанных с профессиональной деятельностью, и не подлежат изменению, использованию, распространению и предоставлению, кроме случаев, предусмотренных законодательными актами.

ЛЕКЦИЯ 8. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И МЕХАНИЗМ ИХ РЕАЛИЗАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Права субъектов персональных данных предусмотрены в гл. 3 Закона. Среди основных прав можно выделить следующее: (1) право на отзыв согласия, (2) право на получение информации, касающейся обработки персональных данных, и изменение персональных данных, (3) право на получение информации о предоставлении персональных данных третьим лицам, (4) право требовать прекращения обработки персональных данных и (или) их удаления, (5) право на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных. Данные права коррелируются с закрепленными в GDPR.

Для реализации прав субъект персональных данных подает оператору заявление в письменной форме либо в виде электронного документа. В случае направления заявления субъекта персональных данных для реализации своих прав уполномоченному лицу, последний не обязан отвечать по существу на данный запрос. Вместе с тем ответ уполномоченным лицом на заявление субъекта персональных данных не будет противоречить законодательству о персональных данных.

Законодательными актами может быть предусмотрена обязательность личного присутствия субъекта персональных данных и предъявления документа, удостоверяющего личность, при подаче им заявления оператору в письменной форме.

Заявление субъекта персональных данных должно содержать:

фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания);

дату рождения субъекта персональных данных;

идентификационный номер субъекта персональных данных, при отсутствии такого номера - номер документа, удостоверяющего личность субъекта персональных данных, в случаях, если эта информация указывалась субъектом персональных данных при даче своего согласия оператору или обработка персональных данных осуществляется без согласия субъекта персональных данных;

изложение сути требований субъекта персональных данных;

личную подпись либо электронную цифровую подпись субъекта персональных данных.

Ответ на заявление направляется субъекту персональных данных в форме, соответствующей форме подачи заявления, если в самом заявлении не указано иное.

(1) Право на отзыв согласия субъекта персональных данных (ст. 10 Закона).

Данное право влечет прекращение обработки персональных данных, полученных на основании согласия. Оно может быть реализовано в любое время без объяснения причин путем подачи оператору заявления в порядке, установленном ст. 14 Закона, либо в форме, посредством которой получено его

согласие (например, согласие было получено посредством проставления «галочки» на сайте, то на сайте должна быть реализована форма его отзыва). При реализации субъектом такого права оператору необходимо проверить наличие иных оснований для обработки персональных данных. При обработке одних и тех же персональных данных по разным правовым основаниям, обработка этих же персональных данных может продолжаться при сохранении иных оснований.

Отзыв согласия субъекта персональных данных не имеет обратной силы, то есть обработка персональных данных до ее прекращения в соответствии с реализацией права на отзыв не является незаконной. Печатные издания, аудио- либо видеозаписи программ, радио-, телепрограммы, кинохроникальные программы, иная информационная продукция, содержащие персональные данные, выпущенные до момента отзыва согласия субъекта персональных данных, не подлежат изъятию из гражданского оборота.

Оператор обязан в течение 15 дней после получения заявления субъекта персональных данных в соответствии с его содержанием прекратить обработку персональных данных, осуществить их удаление и уведомить об этом субъекта персональных данных, если отсутствуют иные основания для таких действий с персональными данными, предусмотренные Законом и иными законодательными актами. При отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование, и уведомить об этом субъекта персональных данных в тот же срок.

Окончание срока действия договора, в соответствии с которым осуществлялась обработка персональных данных, или его расторжение влекут такие же последствия, как при отзыве согласия, если иное не предусмотрено этим договором или актами законодательства. Например, обработка персональных данных продолжается при необходимости обеспечения гарантийного и послегарантийного обслуживания, защиты прав одной из сторон при неисполнении другой стороной условий договора, а также соблюдение законодательства об архивном деле и делопроизводстве в части сроков хранения документов.

(2) Право на получение информации, касающейся обработки персональных данных, и изменение персональных данных (ст. 11 Закона).

Субъект персональных данных не должен обосновывать свой интерес к запрашиваемой информации. При реализации данного права субъект персональных данных может получить следующую информацию:

– наименование (фамилию, собственное имя, отчество (если таковое имеется)) и место нахождения (адрес места жительства (места пребывания)) оператора;

– подтверждение факта обработки персональных данных оператором (уполномоченным лицом);

– персональные данные данного субъекта персональных данных и источник их получения (*необходимо указывать все персональные данные,*

которые есть у оператора, с их конкретизацией, а не общим описанием, например, данные о передвижениях);

– правовые основания и цели обработки персональных данных;

– срок, на который дано его согласие;

– наименование и место нахождения уполномоченного лица, которое является государственным органом, юридическим лицом Республики Беларусь, иной организацией, если обработка персональных данных поручена такому лицу (*необходимо указывать конкретного субъекта с его УНП, адресом местонахождения*);

– иная информация, предусмотренная законодательством.

Срок для ответа или отказа в предоставлении информации – 5 рабочих дней после получения заявления субъекта персональных данных, если иной срок не установлен законодательными актами. Форма представления – доступная для восприятия. Информация представляется бесплатно, за исключением случаев, предусмотренных законодательными актами. Вместе с тем, например, в соответствии с п. 7 ст. 26 Закона Республики Беларусь от 21.07.2008 № 418-З «О регистре населения» справки (выписки) из регистра, запрашиваемые физическим лицом один раз в пределах календарного года, предоставляются бесплатно. Предоставление таких справок (выписок) более одного раза в пределах календарного года осуществляется на платной основе. За предоставление таких справок (выписок) взимается государственная пошлина в порядке и размерах, установленных законодательными актами. Периодичность запросов физическим лицом справок (выписок) в отношении своих персональных данных определяется отдельно от периодичности запросов им справок (выписок) в отношении персональных данных физических лиц, законным представителем которых оно является, а также других физических лиц.

Важно, что персональные данные не предоставляются в следующих случаях:

– если персональные данные могут быть получены любым лицом посредством направления запроса в порядке, установленном законодательством, либо доступа к информационному ресурсу (системе) в глобальной компьютерной сети Интернет (*например, интернет-ресурсы, предлагающие услуги продажи тех или иных предметов частными лицами с указанием данных продавцов (имя, телефон)*);

– если обработка персональных данных осуществляется:

в соответствии с законодательством о государственной статистике;

в соответствии с законодательством в области национальной безопасности, об обороне, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, о Государственной границе Республики Беларусь;

в соответствии с законодательством об оперативно-розыскной деятельности, процессуально-исполнительным законодательством об

административных правонарушениях, уголовно-процессуальным, уголовно-исполнительным законодательством;

по вопросам ведения криминалистических учетов;

– в иных случаях, предусмотренных законодательными актами.

Субъект персональных данных вправе требовать от оператора внесения изменений в свои персональные данные в случае, если персональные данные являются неполными, устаревшими или неточными. В этих целях субъект персональных данных подает оператору заявление в порядке, установленном ст. 14 Закона, с приложением соответствующих документов и (или) их заверенных в установленном порядке копий, подтверждающих необходимость внесения изменений в персональные данные. Оператор обязан в течение 15 дней после получения заявления субъекта персональных данных внести соответствующие изменения в его персональные данные и уведомить об этом субъекта персональных данных либо уведомить субъекта персональных данных о причинах отказа во внесении таких изменений, если иной порядок внесения изменений в персональные данные не установлен законодательными актами.

(3) право на получение информации о предоставлении персональных данных третьим лицам (ст. 12 Закона).

В отношении данного права НЦЗПД принято Письмо Национального центра защиты персональных данных Республики Беларусь от 02.03.2023 № 5-5/228 «О разъяснении законодательства о персональных данных (о праве субъекта персональных данных получать от оператора информацию о предоставлении своих персональных данных третьим лицам)».

Субъект персональных данных вправе получать от оператора информацию о предоставлении своих персональных данных третьим лицам один раз в календарный год бесплатно, если иное не предусмотрено Законом и иными законодательными актами.

Для этого необходимо подать заявление оператору в порядке, установленном ст. 14 Закона. Срок для подготовки ответа – 15 дней после получения заявления субъекта персональных данных предоставить ему информацию о том, какие персональные данные этого субъекта и кому предоставлялись в течение года, предшествовавшего дате подачи заявления, либо уведомить субъекта персональных данных о причинах отказа в ее предоставлении. Информация может не предоставляться в случаях, предусмотренных п. 3 ст. 11 Закона (*например, если обработка персональных данных осуществляется в соответствии с законодательством об исполнительном производстве при осуществлении правосудия и организации деятельности судов общей юрисдикции, если персональные данные могут быть получены любым лицом посредством направления запроса в порядке, установленном законодательством, либо доступа к информационному ресурсу (системе) в глобальной компьютерной сети Интернет*), а также если обработка персональных данных осуществляется в соответствии с законодательством об исполнительном производстве, при осуществлении правосудия и организации деятельности судов общей юрисдикции.

В случае получения бесплатно информации в течение календарного года субъект персональных данных не может требовать от оператора предоставления ему в течение того же календарного года обновленной информации на платной основе. Законом не предусмотрено предоставление субъекту персональных данных при реализации им права в соответствии с п. 1 ст. 12 Закона копий документов, содержащих его персональные данные.

(4) право требовать прекращения обработки персональных данных и (или) их удаления (ст. 13 Закона).

Данное право в GDPR называется «право на забвение». Субъект персональных данных вправе требовать от оператора бесплатного прекращения обработки своих персональных данных, включая их удаление, при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами. В качестве примера отсутствия оснований для обработки персональных данных может быть несоответствия согласия требованиям законодательства о защите персональных данных, его отзыв или истечение срока его действия, избыточность обработки персональных данных.

Для реализации указанного права субъект персональных данных подает оператору заявление в порядке, установленном ст. 14 Закона.

Срок для удаления самим оператором (обеспечение прекращения обработки персональных данных), удаление уполномоченным лицом и уведомление об этом субъекта персональных данных – 15 дней после получения заявления. При отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование, и уведомить об этом субъекта персональных данных в тот же срок. Оператор вправе отказать субъекту персональных данных в удовлетворении требований о прекращении обработки его персональных данных и (или) их удалении при наличии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами, в том числе если они являются необходимыми для заявленных целей их обработки, с уведомлением об этом субъекта персональных данных в течение 15 дней. Например, когда обработка персональных данных будет осуществляться в соответствии с законодательством об архивном деле и делопроизводстве.

Законом предусмотрено, что при отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование. В контексте Закона данная мера является альтернативой удалению, когда удаление по техническим причинам невозможно (например, может нарушить работу всей системы). По своим последствиям блокирование является равнозначным удалению и должно исключать использование, предоставление, распространение персональных данных и др.

Механизм удаления во многом зависит от того, в каком виде и в каких документах содержатся персональные данные.

Например, при удалении персональных данных, содержащихся в документах на бумажных носителях, необходимо руководствоваться абз. 3 п. 16 Инструкции по делопроизводству удаление персональных данных из документов, по общему правилу. Персональные данные удаляются одновременно с уничтожением таких документов. По результатам уничтожения составляется акт о выделении к уничтожению. После составления акта отобранные к уничтожению документы и дела передаются организациям, ведающим заготовкой вторичного сырья. Вместе с тем в целях обеспечения защиты персональных данных документы на бумажных носителях, содержащие специальные персональные данные, иные персональные данные, распространение которых создает высокий риск для прав и свобод физических лиц (круг таких данных определяется самим оператором), целесообразно передавать организациям, ведающим заготовкой вторичного сырья после предварительного измельчения.

Удаление персональных данных, содержащихся в документах в электронном виде (за исключением удаления из систем хранения данных, иного серверного оборудования) осуществляется в соответствии с главой 9 Правил работы с документами в электронном виде в архивах государственных органов, иных организаций, утвержденных постановлением Министерства юстиции Республики Беларусь от 6 февраля 2019 г. № 20. Также составляется акт о выделении к уничтожению. Съемные носители, пригодные к повторной эксплуатации, после стирания записанной на них информации могут быть использованы для повторной записи информации. Съемные носители, непригодные к использованию, списываются и уничтожаются в установленном порядке.

При наличии в документах в электронном виде информации, распространение и (или) предоставление которой ограничено (к чему и относятся персональные данные), применяются следующие способы ее уничтожения:

– использование специального программного обеспечения путем перезаписи или стирания;

– воздействие на поверхность съемного носителя магнитным полем (размагничивание);

– механическое уничтожение съемного носителя вместе с информацией (измельчение, расплавление, использование химикатов). Для обеспечения полной информационной безопасности данный способ является предпочтительным.

Если документы или информация хранится на рабочих столах работников и не относится к номенклатуре дел с установленными сроками хранения, то порядок удаления определяет оператор.

Если персональные данные содержаться в информационных системах (ресурсах), то в соответствии с Законом оператор обязан удалить персональные данные при отсутствии правовых оснований для их обработки. Данное требование распространяется в том числе и на ситуации, когда персональные

данные содержатся в информационных ресурсах (системах) соответствующего оператора (например, локальной вычислительной сети, интернет-сайте, бухгалтерской информационной системе, системе электронного документооборота, системе видеонаблюдения и др.). Порядок удаления определяется оператором, например, в отдельном локальном правовом акте, локальном акте, определяющем порядок функционирования такой информационной системы (ресурса), в политике информационной безопасности.

Законодательством не предусматривается в этих случаях обязательное составление акта об удалении на бумажном носителе. В иных случаях целесообразно создавать лог-файлы и настраивать их ведение таким образом, чтобы в эти файлы вносились записи об удалении персональных данных, но без информации, позволяющей идентифицировать физических лиц (например, запись сведений о дате удаления и объеме удаленных сведений).

Из информационных систем (ресурсов) персональные данные следует удалять таким образом, чтобы их невозможно было восстановить обычному пользователю. Например, простое «перемещение в корзину» не является надлежащим выполнением обязанности по удалению персональных данных. При этом сама по себе возможность применения специальных технических средств по восстановлению информации не может рассматриваться как свидетельство невыполнения оператором обязанности по удалению персональных данных.

(5) право на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных (ст. 15 Закона).

Субъект персональных данных как самостоятельно, так и через представителей вправе обжаловать действия (бездействие) и решения оператора, нарушающие его права при обработке персональных данных, в уполномоченный орган по защите прав субъектов персональных данных (НЦЗПД) в порядке, установленном законодательством об обращениях граждан и юридических лиц. В законодательстве не установлен обязательный досудебный порядок, то есть предварительное обращение к оператору не нужно.

Предметом жалобы могут быть действия (бездействие) оператора. Она может быть подана в течение 3 месяцев со дня, когда о нарушении стало известно лицу, направившему жалобу. Действия оператора могут быть оформлены соответствующим актом (решением), а могут такой формы не иметь и носить характер фактических действий. Бездействие, в свою очередь, может выражаться в несовершении оператором действий, направленных на защиту персональных данных субъекта (например, неудалении данных).

Порядок рассмотрения жалоб установлен в Положении о НЦЗПД, утвержденном в Указе Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных». Субъекты персональных данных, полагающие, что их права, свободы и законные интересы нарушены при обработке персональных данных, вправе направить в Национальный центр защиты персональных данных жалобу по вопросам обработки персональных данных (далее - жалоба).

Жалоба подается в письменной форме или в виде электронного документа и должна содержать:

фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания);

изложение сути жалобы с указанием действий (бездействия), которыми нарушаются права, свободы и законные интересы субъекта персональных данных;

информацию о принятых мерах по восстановлению нарушенных прав, свобод и законных интересов субъекта персональных данных (в том числе обращение к оператору (уполномоченному лицу), в суд, органы прокуратуры или иные государственные органы) или об отсутствии таких мер;

личную подпись субъекта персональных данных в случае направления жалобы в письменной форме.

К жалобе прилагаются документы и иные материалы (в том числе фотографии, графические изображения экрана (скриншоты), подтверждающие нарушение прав, свобод и законных интересов субъекта персональных данных, подающего жалобу (при их наличии).

Жалобы в письменной форме подаются нарочным (курьером) или по почте. Жалобы в виде электронного документа должны быть удостоверены электронной цифровой подписью, выработанной с использованием личного ключа, сертификат открытого ключа которого издан в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Жалоба оставляется без рассмотрения по существу, если она:

не соответствует требованиям, предусмотренным в п. 27 - 29 Положения;

рассмотрена, рассматривается или подлежит рассмотрению в соответствии с законодательством о конституционном судопроизводстве, гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса, либо если в соответствии с законодательными актами установлен иной порядок подачи и рассмотрения такой жалобы.

Решение об оставлении жалобы без рассмотрения по существу принимается Национальным центром защиты персональных данных в течение 10 рабочих дней со дня, следующего за днем ее регистрации, с уведомлением об этом субъекта персональных данных, подавшего жалобу, и указанием причин принятого решения.

Жалобы рассматриваются не позднее одного месяца со дня, следующего за днем их регистрации в НЦЗПД. В случае, если жалоба требует дополнительного изучения и проверки, указанный срок может быть продлен НЦЗПД не более чем на один месяц с уведомлением об этом субъекта персональных данных, подавшего жалобу.

В случае, если содержащиеся в жалобе сведения о нарушениях при обработке персональных данных подтверждаются, НЦЗПД принимает необходимые меры по защите нарушенных прав, свобод и законных интересов

субъекта персональных данных, подавшего жалобу, и уведомляет его об этом. В случае, если содержащиеся в жалобе сведения о нарушениях при обработке персональных данных не подтверждаются, НЦЗПД оставляет такую жалобу без удовлетворения и информирует об этом субъекта персональных данных, подавшего жалобу, с разъяснением порядка обжалования такого решения. Принятые по результатам рассмотрения жалоб решения могут быть обжалованы в судебном порядке.

В случае поступления повторных жалоб, не содержащих новых обстоятельств, имеющих значение для их рассмотрения по существу, по таким жалобам с соответствующим субъектом персональных данных прекращается переписка с уведомлением его об этом. При поступлении повторных жалоб по вопросам, по которым с субъектом персональных данных прекращена переписка, такие жалобы рассмотрению не подлежат (без уведомления субъекта персональных данных).

В качестве еще одного права, которое предусмотрено ст. 152 Гражданского кодекса Республики Беларусь от 07.12.1998 № 218-З, является компенсация морального вреда. Если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, гражданин вправе требовать от нарушителя денежную компенсацию указанного вреда.

При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинен вред.

Правам субъекта персональных данных корреспондируют обязанности оператора, закрепленные в ст. 16 Закона. К таким обязанностям относят следующее:

разъяснять субъекту персональных данных его права, связанные с обработкой персональных данных (*например, это предусмотрено при получении согласия для обеспечения признания его информированным*);

получать согласие субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами (*В данной ситуации необходимо обратиться к ст. 6 и 8 Закона, где указаны исключения, когда согласие получать не нужно. Часто на практике используется множественность правовых оснований для обработки персональных данных, например, согласие и заключение договора*);

обеспечивать защиту персональных данных в процессе их обработки (*это универсальная обязанность оператора, для обеспечения ее реализации с уполномоченным лицом необходимо включать соответствующие положения в договор*);

предоставлять субъекту персональных данных информацию о его персональных данных, а также о предоставлении его персональных данных

третьим лицам, за исключением случаев, предусмотренных Законом и иными законодательными актами (*данной обязанности корреспондирует право субъекта персональных данных, закрепленные в ст. 11-12 Закона*);

вносить изменения в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных (*Данной обязанности корреспондирует право субъекта персональных данных, закрепленные в ст. 11 Закона. Вместе с тем, у оператора нет обязанности отслеживать актуальность полученных персональных данных. Оператор обязан изменить персональные данные при получении заявления об этом от субъекта персональных данных или при получении информации о неактуальности у него персональных данных*);

прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами (*данной обязанности корреспондирует право субъекта персональных данных, закрепленные в ст. 13 Закона*);

уведомлять уполномоченный орган по защите прав субъектов персональных данных (НЦЗПД) о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, за исключением случаев, предусмотренных НЦЗПД (*Порядок уведомления установлен Приказом НЦЗПД от 15.11.2021 № 13 «Об уведомлении о нарушениях системы защиты персональных данных». Уведомление на одном из государственных языков направляется оператором незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, в письменной форме или в виде электронного документа в НЦЗПД, по общему правилу, при нарушении систем защиты персональных данных. Уведомление не направляется, если нарушение систем защиты не привело к:*

– незаконному распространению, предоставлению персональных данных;

– изменению, блокированию либо удалению персональных данных без возможности восстановления доступа к ним.

В уведомлении необходимо отразить следующее:

– фамилию, собственное имя, отчество (если таковое имеется), адрес места жительства (места пребывания) оператора (физического лица) или полное наименование и место нахождения оператора (государственного органа, юридического лица Республики Беларусь, иной организации), а также номер телефона, адрес электронной почты (при наличии) оператора;

– фамилию, собственное имя, отчество (если таковое имеется), должность лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных оператора либо наименование

соответствующего структурного подразделения (в отношении государственного органа, юридического лица Республики Беларусь, иной организации), его номер телефона и адрес электронной почты (при наличии);

– дату и время нарушения системы защиты персональных данных;

– дату и время, когда стало известно о произошедшем нарушении системы защиты персональных данных;

– описание нарушения системы защиты персональных данных;

- примерное количество субъектов персональных данных, затронутых нарушением;

– вероятные неблагоприятные последствия нарушения системы защиты персональных данных (потеря контроля над персональными данными, их хищение, нарушение прав и свобод субъектов персональных данных, чести, достоинства или деловой репутации, наступление убытков, разглашение охраняемой законом тайны, наступление иного существенного имущественного или иного вреда у субъектов персональных данных);

– меры, принятые или предлагаемые оператором для устранения нарушения системы защиты персональных данных.);

осуществлять изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных субъекта персональных данных по требованию уполномоченного органа по защите прав субъектов персональных данных, если иной порядок внесения изменений в персональные данные, их блокирования или удаления не установлен законодательными актами (*Оператор обязан по требованию уполномоченного органа осуществлять изменение, блокирование или удаление персональных данных в случае выявления недостоверных персональных данных; персональных данных, полученных незаконным путем. Подобные требования могут являться результатом проведенных проверок, рассмотрения жалоб субъектов персональных данных, обращений граждан и юридических лиц, изучения информации, размещенной в глобальной компьютерной сети Интернет либо полученной от других государственных органов и организаций (абз 8 п. 8 Положения, утвержденного Указом Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных».)*;

исполнять иные требования уполномоченного органа по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных (*На практике к числу таких требований относятся разработка (корректировка) необходимых документов (локальных правовых актов), доработка сайта (например, рубрик, посредством которых осуществляется сбор персональных данных), удаление персональных данных (например, обрабатываемых без надлежащих правовых оснований), повторное рассмотрение заявления субъекта персональных данных о реализации права, направление субъектам персональных данных писем в случае утечки персональных данных и т.п.;*);

выполнять иные обязанности, предусмотренные настоящим Законом и иными законодательными актами (*Например, внесение в государственный*

информационный ресурс «Реестр операторов персональных данных» сведений об информационных ресурсах (системах), содержащих персональные данные).

Оператор, являющийся республиканским органом государственного управления, размещает на своем официальном сайте в глобальной компьютерной сети Интернет информацию об информационных ресурсах (системах), содержащих персональные данные, владельцем которых он является, за исключением информации об информационных ресурсах (системах), содержащих:

персональные данные, обработка которых осуществляется в случаях, предусмотренных абз. 4 – 7 п. 3 ст. 11 Закона;

персональные данные его работников в процессе осуществления трудовой (служебной) деятельности;

служебную информацию ограниченного распространения.

В ст. 19 Закона установлена обязанность оператора (уполномоченного лица) принимать организационные, правовые и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных, содержание которых в Законе не расшифровывается. Оператор (уполномоченное лицо) обязан принимать правовые, организационные и технические меры. Как видно из ст. 17 Закона, для оператора установлено три вида мер: правовые, организационные и технические. При этом содержание каждого вида мер не раскрывается. Например, реализация многих организационных мер невозможна без издания локальных правовых актов. Принятие технических мер требует совершения организационных действий. Тем не менее, указанное деление имеет своей целью определить основные направления (векторы), по которым требуется принятие мер.

Обратимся к ст. 29 Закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», в которой раскрывается значение каждой меры в отношении защиты информации. На данном основании попробуем сформулировать понятия правовых, организационных и технических мер защиты персональных данных.

Правовые меры по защите персональных данных – это документальное оформление организационных и технических мер по порядку обработки персональных данных, закреплённое в локальных правовых актах оператора (уполномоченного лица), устанавливающих порядок обработки персональных данных у оператора (уполномоченного лица), а также в договорах, заключаемых оператором с субъектом персональных данных, уполномоченным лицом, третьим лицом, сооператором, содержащих, среди прочего цели обработки персональных данных, перечень действий с ними.

Организационные меры по защите персональных данных – это средства и способы построения внутренней структуры оператора по разграничению доступа к персональным данным между работниками оператора, а также

организации взаимодействия оператора с субъектом персональных данных, уполномоченным лицом, третьим лицом, сооператором по выстраиванию бизнес-процессов и определению правового основания обработки персональных данных.

Технические меры по защите персональных данных – это меры по использованию средств технической и криптографической защиты персональных данных, применяемые в зависимости от вида обрабатываемых персональных данных, включающие аттестацию информационных ресурсов, в которых обрабатываются персональные данные.

Оператор (уполномоченное лицо) определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты персональных данных, с учетом требований настоящего Закона и иных актов законодательства.

Обязательными мерами по обеспечению защиты персональных данных являются:

назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных;

издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных;

ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством;

установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);

осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Оператору не следует ограничиваться принятием необходимого минимума (что является достаточно типичным нарушением законодательства), а необходимо принять и иные меры, прямо не указанные в законодательстве о персональных данных, но требующиеся с учетом его специфики.

Техническая и криптографическая защита осуществляется на основании Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Приказ №66), Приказа

Оперативно-аналитического центра при Президенте Республики Беларусь от 12.11.2021 № 195 «О технической и криптографической защите персональных данных» (далее – Приказ №195).

Приказом №66 утверждено Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (далее – Положение).

Положение не применяется собственниками (владельцами) в отношении информационных систем, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания.

Справочно: информационная система - совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств (ст. 1 Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации).

Работы по технической и криптографической защите информации включают:

(1) проектирование системы защиты информации;

(2) создание системы защиты информации;

(3) аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом №66;

(4) обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

(5) обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

До первого этапа собственник (владелец) информационной системы определяет вид информации, которая будет обрабатываться в информационной системе, и осуществляет отнесение предполагаемой информационной системы к одному или нескольким классам типовых информационных систем, установленных в Приложении №1 к Положению. Принятое решение оформляется актом отнесения информационной системы к классу (классам) типовых информационных систем.

В Приложении №1 установлено 10 классов типовых информационных систем. 6 классов из 10 связаны с обработкой персональных данных: 4-ин, 4-спец, 4-бг, 3-ин, 3-спец, 3-бг.

Класс	Описание
1. Класс 4-ин	информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к сетям электросвязи общего пользования (открытым каналам передачи данных)
2. Класс 4-спец	информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных
3. Класс 4-бг	информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных
4. Класс 3-ин	информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных
5. Класс 3-спец	информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных
6. Класс 3-бг	информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.

Первые три этапа могут выполняться как работниками собственника (владельца) информационной системы, так и привлеченной организацией, имеющей лицензию на осуществление деятельности по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и (или) услуг. У собственника (владельца) для этих целей может быть создано отдельное подразделение защиты информации или эти должностные обязанности могут быть возложены на иное подразделение (должностных лиц), ответственных за обеспечение защиты информации.

Важно, что работники собственника (владельца) должны иметь высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством. Если собственником информационных систем, в которых обрабатываются персональные данные, является физическое лицо, то оно вправе

самостоятельно выполнять работы по проектированию и (или) созданию систем защиты информации этих информационных систем

Допускается применение единой системы защиты информации для нескольких информационных систем, принадлежащих одному собственнику (владельцу). Перечень работ по технической и криптографической защите информации может предусматриваться в техническом задании на создание информационной системы. При выполнении специализированными организациями работ по проектированию и (или) созданию систем защиты информации информационное взаимодействие между информационными системами должно осуществляться с использованием защищенных каналов передачи данных.

(1) При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационной системы другого собственника (владельца), имеющей аттестованную систему защиты информации, может быть предусмотрено применение требований, реализованных в системе защиты информации информационной системы этого собственника (владельца). Такие требования применяются согласно договору на оказание соответствующих услуг.

На этапе проектирования системы защиты информации осуществляются:

(i) Разработка (корректировка) политики информационной безопасности.

Если собственником информационной системы является физическое лицо, то политику информационной безопасности разрабатывать не нужно. При этом если физическое лицо имеет статус индивидуального предпринимателя или осуществляет деятельность по оказанию услуг в сфере агроэкотуризма, то политику разрабатывать нужно.

Требования к Политике информационной безопасности установлены в п. 10 Положения. Она должна содержать цели и принципы защиты информации, обязательства собственника (владельца) информационной системы соответствовать требованиям по защите информации, постоянно совершенствовать систему защиты информации. В ней может быть отражена и иная информация, отражающая общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в информационной системе. Политика должна быть доведена до сведения работников собственника (владельца) информационной системы в части, их касающейся, быть доступной всем заинтересованным субъектам информационных отношений для ознакомления. При наличии у одного собственника (владельца) нескольких информационных систем разрабатывается и утверждается единая политика информационной безопасности.

(ii) Разработка структурной и логической схем информационной системы.

Структурная и логическая схемы информационной системы разрабатываются на основе анализа структуры информационной системы и информационных потоков (внутренних и внешних), состава, количества и мест

размещения активов информационной системы, ее физических и логических границ. Она должна содержать следующее:

– наименование информационной системы;

– места размещения физических устройств, относящихся к активам информационной системы, средств защиты информации с указанием названия устройства согласно его системному имени (серийный номер - для неуправляемого устройства), названий физических интерфейсов устройства;

– физические линии связи с указанием их типа (витая пара, волоконно-оптический кабель и др.), идентификаторы виртуальных локальных вычислительных сетей (VLAN ID);

– физические границы информационной системы.

К структурной схеме информационной системы должны прилагаться:

– сведения о назначении линий связи (передача данных или управление активами информационной системы, средствами защиты информации);

– перечень виртуальных локальных вычислительных сетей (VLAN) с указанием их идентификаторов (VLAN ID), названий виртуальных локальных вычислительных сетей (VLAN Name), IP-адресации, используемой в виртуальных локальных вычислительных сетях (VLAN);

– перечень телекоммуникационного оборудования с указанием производителя оборудования, его модели, системного имени (серийного номера для неуправляемого устройства), IP-адреса управления устройством, места размещения (помещение, номер стойки, место в стойке и др.).

Логическая схема информационной системы отражает особенности функционирования информационной системы на сетевом и последующих уровнях и должна содержать:

– наименование информационной системы;

– направления информационных потоков (внутренних и внешних). Для информационных систем классов «3-ин», «3-спец», «3-бг» допускается взаимодействие с любыми информационными системами;

– логические границы информационной системы.

К логической схеме информационной системы должны прилагаться сведения:

– об информационных ресурсах, входящих в состав информационной системы, с указанием IP-адресов и названий физических серверов, виртуальных машин, контейнеров, обеспечивающих их функционирование;

– о средствах защиты информации с указанием IP-адресов их администрирования;

– об открытых портах транспортного уровня с указанием соответствующих им IP-адресов технологий и (или) протоколов.

В структурной и логической схемах информационной системы допускается объединение однотипных физических устройств, виртуальных машин, относящихся к активам информационной системы, средствам защиты информации, в единый элемент при условии наличия соответствующих обозначений, отражающих наполнение данного элемента. Структурная и

логическая схемы информационной системы и прилагаемые к ним документы составляются в произвольной форме с учетом особенностей функционирования информационной системы и должны обеспечивать читаемость содержащихся в них сведений.

(iii) Разработка технического задания на создание системы защиты информации.

Техническое задание разрабатывается собственником (владельцем) информационной системы либо специализированной организацией и утверждается собственником (владельцем) информационной системы. Оно должно содержать следующее:

– наименование информационной системы с указанием присвоенного (присвоенных) ей класса (классов) типовых информационных систем;

– требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3 к Положению;

– порядок обезличивания персональных данных, если предполагается обезличивание персональных данных;

– требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого собственника (владельца), если функционирование информационной системы, для которой осуществляется проектирование системы защиты информации, предполагается на базе информационной системы другого собственника (владельца;

– требования к средствам криптографической защиты информации на основе перечня государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденным постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. №375.

Требования к системе защиты, подлежащих включению в техническое задание, разделены на 8 групп:

(a) аудит безопасности (например, обеспечение сбора и хранения сведений о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года),

(b) требования по обеспечению защиты информации (например, регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием),

(c) требования по обеспечению идентификации и аутентификации (например, обеспечение идентификации и аутентификации пользователей активов информационной системы, средств защиты информации обеспечение централизованного управления учетными записями пользователей информационной системы),

(d) требования по защите системы защиты информации информационной системы (синхронизация системного времени активов информационной системы, средств защиты информации от единого (общего) источника),

(e) обеспечение криптографической защиты информации (обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографический токен и (или) средства выработки электронной цифровой подписи; обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и (или) средства выработки электронной цифровой подписи)),

(f) дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре (обеспечение безопасного перемещения виртуальных машин и обрабатываемой на них информации; обеспечение резервного копирования виртуальных машин),

(g) иные требования (обеспечение контроля за внешними подключениями к информационной системе; ежегодное проведение оценки эффективности защищенности информационной системы (тестирование на проникновение); обеспечение обнаружения и реагирования на угрозы безопасности конечных узлов (уровня узла) в информационной системе).

Собственник (владелец) информационной системы вправе не включать в техническое задание отдельные обязательные требования к системе защиты информации по перечню согласно приложению 3 при отсутствии в информационной системе соответствующего актива (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.

(iv) Разработка проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации.

В документах должны быть регламентированы права и обязанности пользователей информационной системы, а также порядок применения системы защиты информации, в том числе порядок реализации мероприятий по:

– выявлению угроз, которые могут привести к сбоям, нарушению функционирования информационной системы, реагированию на соответствующие события и ликвидации их последствий;

– применению технологии электронной цифровой подписи (особенности выработки и проверки электронной цифровой подписи, обращения с личными ключами электронной цифровой подписи).

(2) На этапе создания системы защиты информации осуществляется реализация мер по технической и криптографической защите информации, в том числе:

– внедрение средств защиты информации, проверка их работоспособности и совместимости с активами информационной системы;

– корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации структурной и логической схем информационной системы;

– корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации и их утверждение.

В ходе внедрения средств технической и криптографической защиты информации осуществляются:

– их монтаж и наладка в соответствии с проектами локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации, рекомендациями изготовителей, ограничениями, установленными в сертификатах соответствия, требованиями по совместимости средств криптографической защиты информации;

– проверка корректности выполнения такими средствами требований по защите информации в реальных условиях эксплуатации и во взаимодействии с активами информационной системы. В рамках такой проверки допускается обработка только общедоступной информации;

– маркировка всех физических линий связи согласно структурной схеме информационной системы.

В процессе эксплуатации информационной системы с применением аттестованной в установленном порядке системы защиты информации подразделение защиты информации или иное подразделение (должностное лицо), ответственное за обеспечение защиты информации:

– реализует регламентированные в локальных правовых актах и других организационно-распорядительных документах по вопросам применения системы защиты информации меры по защите информации;

– реализует мероприятия по выявлению угроз, которые могут привести к сбоям, нарушению функционирования информационной системы, реагированию на соответствующие события и ликвидации их последствий;

– при выявлении событий, которые фактически угрожают конфиденциальности, целостности, подлинности, доступности и сохранности информации или представляют собой нарушение политики информационной безопасности, проводит на внеплановой основе мероприятия, предусмотренные в абзаце десятом настоящей части;

– осуществляет контроль за соблюдением у собственника (владельца) информационной системы требований, установленных законодательством, локальными правовыми актами и другими организационно-распорядительными документами по вопросам применения системы защиты информации;

– принимает меры, направленные на совершенствование системы защиты информации;

– при заключении и исполнении собственником (владельцем) информационной системы договоров с юридическими и физическими лицами по вопросам обеспечения функционирования, модернизации информационной

системы участвует в проведении наладочных работ и сервисного (технического) обслуживания активов информационной системы, средств защиты информации;

– на регулярной основе, но не реже одного раза в год со дня аттестации системы защиты информации проводит:

инструктажи, иные мероприятия, направленные на повышение уровня знаний и навыков работников собственника (владельца) информационной системы по вопросам применения системы защиты информации в части, их касающейся;

анализ эффективности применения системы защиты информации, включая пересмотр применяемых мер по защите информации на предмет их актуальности и необходимости внесения изменений в систему защиты информации.

(3) Аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам осуществляется на основании Положения, утвержденного Приказом №66. Положение об аттестации не применяется в отношении информационных систем, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания. Аттестация проводится организациями, имеющими лицензии на осуществление деятельности по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ. В такой ситуации привлекаются работники собственника (владельца). Собственники (владельцы) информационных систем вправе самостоятельно проводить аттестацию.

При проведении аттестации собственником (владельцем) информационной системы самостоятельно работы по аттестации выполняются комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) информационной системы. Физические лица, являющиеся собственниками информационных систем, в которых обрабатываются персональные данные, вправе выполнять работы по аттестации единолично.

Аттестация проводится:

– при создании или модернизации системы защиты информации;

– в случае истечения срока действия аттестата соответствия;

– в случае изменения технологии обработки защищаемой информации и (или) технических мер, реализованных при создании или модернизации системы защиты информации.

Аттестация создаваемой системы защиты информации осуществляется до ввода информационной системы в эксплуатацию.

Программа и методика аттестации разрабатываются должны содержать перечень выполняемых работ с указанием ответственных лиц, сроков выполнения этих работ, описанием используемых методов проверки требований, реализованных в системе защиты информации, перечень используемых контрольных средств.

Программа и методика аттестации разрабатываются тем, кто проводит аттестацию.

Протокол испытаний должен содержать подробное описание проведенных мероприятий, в том числе с применением графических изображений, позволяющее сформировать вывод о полноте выполнения мероприятий.

Срок проведения аттестации:

– определяется руководителем собственника (владельца) информационной системы, физическим лицом, являющимся собственником информационной системы, в которой обрабатываются персональные данные, - при проведении аттестации собственником (владельцем) информационной системы самостоятельно;

– не может превышать 180 календарных дней - при проведении аттестации специализированной организацией.

Аттестат соответствия оформляется сроком на пять лет.

В случае невозможности устранения выявленных в процессе эксплуатации информационной системы нарушений ее функционирования в течение 5 рабочих дней с момента выявления таких нарушений собственник (владелец) информационной системы обязан прекратить обработку информации, распространение и (или) предоставление которой ограничено, о чем письменно проинформировать ОАЦ.

При получении собственником (владельцем) информационной системы от физического лица его персональных данных, предоставленных этим физическим лицом без использования средств криптографической защиты информации, предоставление в последующем этих персональных данных тем же собственником (владельцем) информационной системы названному физическому лицу может осуществляться без использования средств криптографической защиты информации.

В случае прекращения эксплуатации информационной системы собственник (владелец) информационной системы в соответствии с локальными правовыми актами и другими организационно-распорядительными документами по вопросам применения системы защиты информации принимает меры по:

защите информации, которая обрабатывалась в информационной системе;

резервному копированию информации и криптографических ключей (при необходимости), обеспечению их конфиденциальности и целостности;

уничтожению (удалению) информации и криптографических ключей с машинных носителей информации и (или) уничтожению таких носителей информации.

С требованиями по технической и криптографической защите связаны методы обезличивания персональных данных. В приложении №4 к Положению установлены следующие методы обезличивания:

– введение идентификаторов;

Он реализуется путем замены персональных данных или части персональных данных, позволяющих идентифицировать субъекта персональных

данных, их идентификаторами и создания таблицы соответствия с последующим раздельным хранением идентификаторов и таблиц.

– изменение состава;

Он реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта персональных данных, с последующим раздельным хранением полученных персональных данных и правил изменения.

– декомпозиция;

Он реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создания таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением подмножеств и таблиц. Для его реализации необходимо предварительно разработать правила разбиения множества записей на подмножества, правила установления соответствия между записями в различных таблицах и правила внесения изменений в подмножества и таблицы.

–- перестановка.

Он реализуется путем взаимного перемещения отдельных записей и (или) групп записей с последующим раздельным хранением полученных персональных данных и правил изменения.

ЛЕКЦИЯ 9. ДОКУМЕНТАЛЬНОЕ ОФОРМЛЕНИЕ ПОРЯДКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ У ОПЕРАТОРА В РЕСПУБЛИКЕ БЕЛАРУСЬ

Как указано в ст. 19 Закона оператором (уполномоченным лицом) установлены требования по соблюдению правовых мер, к которым относится подготовка документов. Некоторые из правовых мер указаны в п. 3 ст. 17 Закона.

Первое – это назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных. Так как требования в Законе не установлены, то ввиду того, что это отдельная должность, то мы можем обратиться к Постановлению Министерства труда Республики Беларусь от 30.12.1999 № 159 «Об утверждении выпуска 1 Единого квалификационного справочника должностей служащих «Должности служащих для всех видов деятельности», выпуска 6 ЕКСД «Должности служащих, занятых в машиностроении и металлообработке», выпуска 33 ЕКСД «Должности служащих, занятых финансами, кредитом и страхованием» и выпуска 21 ЕКСД «Должности служащих, занятых геодезией и картографией».

В выпуске №1 содержится характеристика специалиста по внутреннему контролю за обработкой персональных данных (далее – DPO). Как указывает НЦЗПД в своем комментарии, должностные обязанности DPO можно разделить на следующие блоки:

организационные (изучение и анализ процессов обработки персональных данных, определение рисков, связанных с процессами обработки персональных данных, выработка предложений по их минимизации, разработка и поддержание в актуальном состоянии документов, определяющих политику оператора в отношении обработки персональных данных, порядка доступа к персональным данным, иных документов (форм) по вопросам обработки персональных данных, разработка формы реестра персональных данных и координация его ведения, участие в определении и осуществлении мер технической и криптографической защиты персональных данных и т.п.);

консультативные (консультирование работников и уполномоченных лиц по вопросам обработки и защиты персональных данных, согласование локальных правовых актов, договоров на предмет их соответствия законодательству о персональных данных, ознакомление работников с законодательством о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных и т.п.);

контрольные (осуществление контроля за своевременным внесением работниками изменений в персональные данные, которые являются неполными, устаревшими или неточными, прекращением обработки персональных данных, а также осуществлением их удаления или блокирования при отсутствии оснований для обработки персональных данных, предусмотренных законодательными актами; проведение проверки по соблюдению требований законодательства о персональных данных в структурных подразделениях организации для выявления нарушений и предупреждения их возникновения, проведение расследования по нарушениям работниками требований обработки персональных данных, внесение предложений по привлечению виновных к ответственности и т.п.);

информационно-образовательные (организация прохождения обучения работников, осуществляющих обработку персональных данных, по вопросам обработки и защиты персональных данных в порядке, установленном законодательством, поиск оптимальных форм обучения работников, исходя из их трудовых функций и т.п.);

иные функции, связанные с обеспечением комплексной работы по соблюдению законодательства о персональных данных (рассмотрение (участие в рассмотрении) заявлений и жалоб субъектов персональных данных по вопросам обработки персональных данных, принятие необходимых мер по восстановлению их нарушенных прав, обеспечение взаимодействия с Национальным центром защиты персональных данных, в том числе по вопросам уведомления о нарушениях систем защиты персональных данных, исполнения требований по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных и т.п.).

Оператор (уполномоченное лицо) из числа физических лиц, включая индивидуальных предпринимателей, адвокатов, нотариусов, ремесленников, репетиторов, медиаторов и др., такое лицо не назначает.

В организациях назначение DPO может происходить несколькими способами: (1) создание специального подразделения (как правило, это характерно для крупных корпораций, банков, холдингов, в отдел могут включаться юрисконсульты, которые обеспечат соблюдение правовых и организационных мер, и специалисты по информационной безопасности, которые обеспечат соблюдение технических мер); (2) назначение отдельного работника (он назначается приказом, специальных требований к образованию нет, за исключением высшего образования), (3) возложение дополнительных должностных обязанностей на нескольких работников (такой вариант подразумевает разделение должностных обязанностей, как правило, между юрисконсультом и специалистом по информационной безопасности).

Для обеспечения соблюдения должностных обязанностей необходимо обеспечить независимость DPO и необходимые условия для осуществления его функций посредством:

(1) предоставления доступа к документам и информации, в том числе обрабатываемой в информационных системах (ресурсах) в объеме, необходимом для выполнения возложенных на него обязанностей;

(2) организации непосредственной подчиненности руководителю организации или его заместителю.

Формальное назначение DPO без реальной деятельности (проведения фактического контроля, ведения реестра обработок, консультирования и др.) не рассматривается как надлежащее выполнение обязанности, предусмотренной абз. 2 п. 3 ст. 17 Закона, и является основанием для привлечения юридического лица к административной ответственности согласно ч. 4 ст. 23.7 КоАП.

Нередко на практике возникает вопрос о допустимости привлечения DPO по гражданско-правовому договору. Такая модель не соответствует требования Закона. Вместе с тем это не исключает возможности привлечения иных лиц на основании гражданско-правового договора для оказания содействия в выполнении отдельных функций ответственного за контроль (например, для разработки документов, определяющих политику в отношении обработки персональных данных, и иных документов, проведения обучения работников и иных лиц, непосредственно осуществляющих обработку персональных данных по вопросам защиты персональных данных).

Одной из обязательных правовых мер является издание оператором (уполномоченным лицом), являющимся юридическим лицом Беларуси, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных (далее – Политика). НЦЗПД разработаны Разъяснения по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных. Определим несколько пунктов, которые обязательно должны быть отражены в Политике:

(1) Политика может быть в виде одного документа или нескольких документов по направлениям (например, отдельно вывести регулирование

трудовых отношений, обработка файлов cookie, политика видеонаблюдения, обработка в рамках программы лояльности).

(2) Политика должна быть написана простым, ясным, доступным языком и отражать особенности обработки персональных данных у конкретного оператора (уполномоченного лица). Следует избегать абстрактных или неоднозначных формулировок, не позволяющих субъекту персональных данных понять суть и параметры обработки персональных данных («может», «вероятно», «некоторый», «часто», «возможно», «в зависимости от ситуации»), излишнего цитирования законодательства, использования большого числа специальных терминов, подробного описания технических аспектов обработки персональных данных.

(3) Политика должна быть структурированной, то есть с возможностью ее последовательного изучения. Например, использование таблиц, инфографики, возможность поиска ключевых слов,

(4) Оператор (уполномоченное лицо) обязан (обязано) обеспечить неограниченный доступ к Политике. При наличии у оператора (уполномоченного лица) официального сайта (далее – сайт) Политика должна размещаться на сайте, как правило, на странице не ниже второго уровня или в элементе структуры сайта со сквозным отображением (футере сайта), что позволит обеспечить доступ к Политике с любой страницы сайта.

При наличии у оператора (уполномоченного лица) нескольких сайтов для разных направлений деятельности Политика размещается на каждом сайте, при этом допускается размещение на каждом сайте Политики по соответствующему отдельному направлению деятельности (например, на одном сайте предлагаются товары оптом для бизнеса, а на другом – в розницу для физических лиц). Если наряду с сайтом у оператора (уполномоченного лица) имеется мобильное приложение, неограниченный доступ к Политике должен быть предоставлен посредством такого приложения, например, из его главного меню.

При отсутствии у оператора (уполномоченного лица) сайта обеспечение неограниченного доступа к Политике осуществляется посредством ее размещения на информационных стендах или иными способами.

Так, при наличии страницы в социальной сети, посредством которой осуществляется коммуникация с субъектами персональных данных для оказания им услуг либо реализации товаров, Политика может быть размещена с использованием предоставляемых этой социальной сетью инструментов (например, в случае использования Instagram – в Reels либо закрепленных постах).

(5) Если у оператора осуществляется видеонаблюдение, то Политика видеонаблюдения может быть также размещена в общедоступных местах (например, при входе в здание, в фойе и т.п.) на бумажном носителе или в виде ссылки (QR-кода) на её текст на сайте.

(6) Ознакомление с Политикой является правом, а не обязанностью субъекта персональных данных. В этой связи не допускается требовать ознакомления с Политикой, согласия с ней или ее принятия для получения

доступа к сервису, оказания услуги, реализации товара. Такие действия субъекта персональных данных не могут рассматриваться в качестве его согласия на обработку персональных данных, в том числе на условиях, изложенных в Политике.

(7) Политика должна поддерживаться в актуальном состоянии. Если в содержание Политики вносятся существенные изменения, включая изменение целей обработки, сроков хранения, порядка реализации прав субъектов персональных данных, условий трансграничной передачи, их следует доводить до сведения субъектов персональных данных заблаговременно до вступления в силу таких изменений.

В Политику необходимо включать следующую информацию:

– Общие положения (наименование оператора (уполномоченного лица), контактные данные, сферы (бизнес-процессы), на которые распространяется действие Политики (например, обработка персональных данных пользователей сайта, приложения, лиц, претендующих на трудоустройство), сокращения).

– Порядок и условия обработки персональных данных (перечень осуществляемых оператором (уполномоченным лицом) действий с персональными данными, источник получения персональных данных; цели обработки персональных данных (категории субъектов персональных данных, чьи данные подвергаются обработке; перечень обрабатываемых персональных данных; правовые основания обработки персональных данных; срок хранения персональных данных).

– Об уполномоченных лицах;

– О трансграничной передаче персональных данных;

– Права субъектов персональных данных и механизмы их реализации.

При осуществлении оператором (уполномоченным лицом) распространения персональных данных необходимо указать цель такой обработки, а также источник, посредством которого такое распространение осуществляется.

В Политике могут указываться принимаемые правовые, организационные и технические меры по обеспечению защиты персональных данных, например, как персональные данные защищены от неправомерных действий третьих лиц, механизм контроля за уполномоченным (субуполномоченным) лицом.

Цели обработки персональных данных должны быть конкретными и законными, то есть они должны основываться на требованиях законодательства, положениях договоров, вытекать из осуществляемой оператором (уполномоченным лицом) деятельности. Не допускается использование в качестве целей «для совершенствования деятельности организации», «для разработки новых услуг», «в исследовательских целях» (за исключением случаев, когда речь идет об обработке обезличенных персональных данных), «для обеспечения реализации Устава», «для обеспечения соблюдения законодательства».

В качестве категорий субъектов персональных данных в Политике могут быть, в частности, указаны посетители; покупатели (заказчики); пациенты, граждане, подавшие (подающие) обращения.

Если обработка персональных данных необходима для выполнения обязанностей (полномочий), предусмотренных законодательными актами, наряду со ссылкой на соответствующий абзац статьи 6 или пункта 2 статьи 8 Закона в качестве правового основания также указывается законодательство, которое содержит соответствующую обязанность (полномочие). Допускается указание на законодательство без ссылки на конкретные структурные элементы (например, законодательство о труде, о защите прав потребителей, об архивном деле и делопроизводстве, об обращениях граждан и юридических лиц, об административных процедурах, о государственных закупках и т.п.).

Срок хранения персональных данных отражается с указанием на дату или период времени либо критерии, используемые для определения такого срока.

В случае если оператор поручает обработку персональных данных уполномоченному лицу (уполномоченным лицам), в Политике отражается:

наименование и местонахождение уполномоченного лица (уполномоченных лиц), а при невозможности указания данной информации из-за большого количества уполномоченных лиц, динамичности или краткосрочности договорных отношений – категории уполномоченных лиц. При этом следует избегать общих формулировок, таких как «подрядчики», «партнеры», «контрагенты» без указания конкретных сфер их деятельности. Допускается указание в Политике ссылки (QR-кода) на информацию, размещенную в открытом доступе, например, на сайте, и содержащую перечень уполномоченных лиц;

цели обработки персональных данных, для реализации которых привлекается уполномоченное лицо (уполномоченные лица).

При осуществлении трансграничной передачи персональных данных в Политике применительно к каждой цели передачи персональных данных отражаются:

субъекты (категории субъектов) в иностранных государствах, которым персональные данные передаются;

иностранные государства, на территории которых находятся такие субъекты (категории субъектов);

правовые основания трансграничной передачи;

передаваемые персональные данные.

В качестве правовых оснований трансграничной передачи персональных данных могут быть указаны:

основания, предусмотренные статьями 5, 6 и пунктом 2 статьи 8 Закона (в случае передачи персональных данных в иностранные государства, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных);

основания, предусмотренные пунктом 1 статьи 9 Закона (в случае передачи персональных данных в иностранные государства, на территории которых не

обеспечивается надлежащий уровень защиты прав субъектов персональных данных).

Если трансграничная передача персональных данных не осуществляется, информация об этом также отражается в Политике.

Оператор вправе предусмотреть в Политике возможность подачи субъектом персональных данных заявления о реализации его прав посредством информационного ресурса (системы) без соблюдения требований статьи 14 Закона. При этом предоставление такой возможности не является для оператора обязательным.

Таким образом, Политика – это основной документ оператора (уполномоченного лица), который может быть в виде единого документа или нескольких, разделенных по бизнес-процессам, размещается в открытом доступе для субъектов персональных данных, является обязательным для применения и отражает порядок обработки персональных данных.

Согласно ч. 4 ст. 19 Закона оператор (уполномоченное лицо), являющийся юридическим лицом Беларуси, иной организацией, индивидуальным предпринимателем, обязан обеспечить неограниченный доступ, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику оператора (уполномоченного лица) в отношении обработки персональных данных, до начала такой обработки.

В качестве иных локальных правовых актов можно назвать следующее:

(1) Реестр обработки персональных данных. Он может как частью Политики, так и в виде самостоятельного документа. Как правило, составляется в виде таблицы. В ней может быть отражено следующее: цель обработки, подразделение, занимающее обработкой, категории лиц, вид данных), вид обработки (автоматизированная или нет), правовое основание обработки, точка входа (например, как получаем резюме), название информационной системы, в которой происходит обработка персональных данных, наименование уполномоченных лиц, срок хранения, категории получателей.

Дополнительно может быть разработано Положение о реестре обработки персональных данных. Оно определяет порядок ведения Реестра, состав включаемых в него сведений, порядок их внесения в Реестр, изменения и исключения из него.

(2) Перечень уполномоченных лиц, обрабатывающих персональные данные. Это может дополнительный список, сформированный на основании Политики и Реестра.

(3) Согласие на обработку персональных данных. Форма разработана НЦЗПД. Если цели обработки персональных данных не требуют обработки всей совокупности информации, она не подлежит обработке оператором при получении согласия субъекта персональных данных. Например, если для регистрации личного кабинета на сайте и получения рекламной рассылки достаточно указать ФИО и адрес электронной почты, то указание даты рождения и идентификационного номера при получении согласия на рекламную рассылку не требуется. В согласии необходимо указывать цели (с каждой из которых

соглашается субъект персональных данных), информация об уполномоченных лицах (при наличии такой возможности, данные каждой организации), срок получения согласия для каждой цели, если он различается (не допускается использование при определении сроков согласия таких формулировок, как «до отзыва согласия субъектом персональных данных», «сроки устанавливаются законодательством», не рекомендуется использовать срок свыше 3 лет), дата и подпись. Важно, что лицо может дать согласие только на одну из целей, указанных в согласии.

(4) Положение о порядке осуществления внутреннего контроля за обработкой персональных данных. Данный документ является «настольной книгой» DPO. В нем указывается на проведение мониторинга и частоты его проведения, внеплановых проверок и срока его проведения, порядок проведения проверки и оформление ее результатов. Дополнительно, в Положении отражается необходимость подготовки сводного отчета о проведении проверок.

(5) Положение о порядке доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе). Данный документ определяет перечень лиц, кому предоставляется доступ к персональным данным, их категория (или перечень) и цели обработки, порядок предоставления, изменения и прекращения доступа к персональным данным, возможность получения временного доступа,

Еще один документ, на который необходимо обратить внимание – договор между оператором и уполномоченным лицом о поручении обработки персональных данных. В ст. 7 Закона закреплен перечень пунктов, которые должны быть в нем отражены:

– цели обработки персональных данных.

Они должны соответствовать целям, заявленным в документе, определяющем политику оператора в отношении обработки персональных данных, и не должны быть абстрактными или общими.

– перечень действий, которые будут совершаться с персональными данными уполномоченным лицом.

В частности, это может быть сбор персональных данных для заключения договора с определением перечня необходимых персональных данных; внесение сведений в информационный ресурс; хранение персональных данных с указанием сроков и условий хранения; их актуализация путем сопоставления с дополнительной информацией и т.п. Если планируется обезличивание, это необходимо указать. Условия, при которых возможно предоставление персональных данных третьим лицам или их распространение (если предполагается их предоставление или распространение).

– обязанность уполномоченного лица по соблюдению конфиденциальности персональных данных.

В соответствии с Законом об информации, информатизации и защите информации конфиденциальность информации – это требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами.

Соответственно, в договоре следует предусмотреть требование о том, что уполномоченное лицо не вправе распространять и (или) предоставлять персональные данные, которые стали ему (им) известны в связи с исполнением договора о поручении обработки, в том числе после прекращения обработки без наличия правового основания, предусмотренного законодательными актами.

– меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона.

В качестве механизма контроля оператором может быть закреплена обязанность уполномоченного лица предоставлять оператору информацию, необходимую для подтверждения реализации мер. Если договор является длительным, то предоставление такой информации может быть периодическим (например, отчет раз в квартал или раз в полгода).

В качестве мер может быть прописано наличие аттестата соответствия системы защиты информации информационной системы требованиям по защите информации; наличие структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных; наличие документов, определяющих политику уполномоченного лица в отношении обработки персональных данных.

Если планируется привлечение субуполномчоенных лиц, это так же необходимо указать, как и уведомление об этом и возможности необходимости получения нового согласия субъекта персональных данных.

В случае допустимости привлечения субуполномоченных лиц необходимо предусмотреть:

условие об обеспечении субуполномоченным лицом защиты персональных данных на уровне не ниже, чем обеспечено уполномоченным лицом;

обязанность уполномоченного лица обеспечить соблюдение субуполномоченным лицом обязательств, возложенных на уполномоченное лицо.

В договоре целесообразно определить порядок действий уполномоченного лица в случае поступления к нему или к оператору заявлений субъектов персональных данных. Например, может быть предусмотрено, что в случае поступления заявления уполномоченному лицу оно может предоставлять субъекту персональных данных информацию об обработке персональных данных. Дополнительно, можно предусмотреть срок для ответов на запросы оператора о текущей обработке персональных данных; уведомлении оператора о любом заявлении (запросе), полученном от субъекта персональных данных; информировании оператора в случае, если стало известно, что персональные данные, обработку которых осуществляет уполномоченное лицо, являются неполными, устаревшими или неточными; уведомлении оператора в случае, если имеются основания полагать, что поручения оператора по обработке персональных данных не соответствуют требованиям законодательства.

Обязанность уполномоченного лица по окончании договора прекратить обработку персональных данных, передать все персональные данные оператору

либо удалить (блокировать) персональные данные, за исключением случаев, когда законодательными актами предусмотрена обязанность их хранения, а также удалить (блокировать) все имеющиеся копии персональных данных и подтвердить оператору, что это сделано. Подтверждение передачи, удаления или блокирования персональных данных может быть, например, оформлено отдельным актом, либо соответствующая информация может быть указана в акте сдачи-приемки выполненных работ, либо представлен письменный отчет о выполненном поручении.

ЛЕКЦИЯ 10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Понятие «нарушение» за законодательство в сфере персональных данных в законодательстве не закреплено. Под ним можно понимать нарушение или попытка нарушения юридическим лицом, должностным лицом, индивидуальным предпринимателем или физическим лицом законодательства о защите персональных данных. В ст. 19 Закона установлено, что лица, виновные в нарушении Закона, несут ответственность, предусмотренную законодательными актами.

За нарушение законодательства о персональных данных в Республике Беларусь предусмотрена дисциплинарная (п. 10 ч. 1 ст. 47 ТК), административная (ст. 23.7 КоАП), уголовная (ст.ст. 203-1, 203-2 УК) и гражданско-правовая ответственность. В п. 2 ст. 19 Закона установлено, что моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, установленных Законом, подлежит возмещению. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Нарушение порядка обработки персональных данных является дисциплинарным проступком. Под ним понимается противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей. В ст. 198 Трудового кодекса Республики Беларусь от 26.07.1999 № 296-З (далее – ТК) установлены меры дисциплинарного взыскания, такие как замечание; выговор; лишение полностью или частично стимулирующих выплат на срок до двенадцати месяцев; увольнение (подп. 10 ч. 1 ст. 47 ТК). За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

В качестве дополнительных оснований прекращения трудового договора с некоторыми категориями работников может быть нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных.

До применения дисциплинарного взыскания наниматель обязан затребовать письменное объяснение работника. Отказ его дачи или невозможность получения – это не препятствие для применения

дисциплинарного взыскания. В качестве документального подтверждения нанимателем составляется акт с указанием присутствовавших при этом свидетелей.

Дисциплинарное взыскание оформляется приказом (распоряжением, постановлением, решением, протоколом), с которым работник ознакамливается под роспись в течение 5 дней с даты его издания, не считая времени болезни работника или ухода за больным членом семьи, подтвержденных листком нетрудоспособности или справкой о временной нетрудоспособности, пребывания работника в отпуске, нахождения на военных или специальных сборах. Если работник не ознакомлен, он считается не имеющим дисциплинарного взыскания. Отказ работника от ознакомления с приказом (распоряжением, постановлением, решением, протоколом) о дисциплинарном взыскании оформляется актом с указанием присутствовавших при этом свидетелей.

Дисциплинарное взыскание применяется не позднее 1 месяца со дня обнаружения дисциплинарного проступка, не считая времени болезни работника или ухода за больным членом семьи, подтвержденных листком нетрудоспособности или справкой о временной нетрудоспособности, пребывания работника в отпуске, нахождения на военных или специальных сборах. Днем обнаружения дисциплинарного проступка считается день, когда о проступке стало известно лицу, которому работник непосредственно подчинен.

Дисциплинарное взыскание не может быть применено позднее 6 месяцев, а по результатам ревизии, проверки, проведенной компетентными государственными органами или организациями, - позднее 2 лет со дня совершения дисциплинарного проступка. В указанные сроки не включается время производства по уголовному делу.

Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, он считается не подвергавшимся дисциплинарному взысканию. При этом дисциплинарное взыскание погашается автоматически без издания приказа (распоряжения, постановления, решения, протокола).

Досрочное снятие дисциплинарного взыскания оформляется приказом (распоряжением, постановлением, решением, протоколом).

Таким образом, привлечение к дисциплинарной ответственности за нарушение законодательства о персональных данных возможно только в отношении тех категорий работников, на которых возложена обязанность по обработке персональных данных, в связи с нарушением ими порядка обработки персональных данных.

Привлечение работника к дисциплинарной ответственности за нарушение законодательства о персональных данных не влияет на возможность привлечения его к гражданско-правовой, административной или уголовной ответственности за те же нарушения в порядке и на основаниях, установленных законодательством.

Административная ответственность установлена в ст. 23.7 КоАП. Она состоит из 4 частей, в каждой из которых установлен самостоятельный состав административного правонарушения, являющихся формальным, то есть для привлечения к административной ответственности не нужно наступление последствий.

В ч. 1 ст. 23.7 КоАП установлена административная ответственность за умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных. В качестве меры ответственности предусмотрен штраф в размере до 50 базовых величин. Термины, упомянутые в ст. 23.7 КоАП, используется в значении, указанном в Законе.

Нарушение прав субъекта, связанных с обработкой персональных данных, может иметь различные формы:

отсутствие ответа на заявления, поданные в соответствии со ст. 14 Закона;

несоблюдение сроков ответов на данные заявления;

неправомерный отказ в удовлетворении соответствующих требований субъектов персональных данных (например, отказ в прекращении обработки данных и их удалении при отсутствии правовых оснований для обработки);

предоставление неполной информации в ответ на поступившее заявление (например, при подаче заявления в соответствии со ст. 11 Закона субъекту вместо конкретных персональных данных указывается общая характеристика таких данных; при подаче заявления в соответствии со ст. 12 Закона указывается лишь, что данные передавались субъектам, имеющим право на их получение).

Субъектом является любое вменяемое физическое лицо, достигшее возраста 16 лет. В силу требований п. 2 ч. 1 ст. 4.6 КоАП индивидуальный предприниматель также может являться субъектом рассматриваемого правонарушения.

В качестве примера дела может быть следующее. «*Б. умышленно незаконно с личной электронной почты предоставил Департаменту финансовых расследований персональные данные Ш. Суд оштрафовал Б. на 10 базовых величин по ч. 1 ст. 23.7 КоАП за незаконное предоставление персональных данных физического лица (дело от 13.10.2022 № 17АП221974/Н)*».

В ч. 2 ст. 23.7 КоАП предусмотрен квалифицированный состав правонарушения: деяния, предусмотренные ч. 1 ст. 23.7 КоАП, совершенные лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью. В качестве меры ответственности предусмотрен штраф в размере штрафа в размере от 4 до 100 базовых величин.

При привлечении лица к административной ответственности в данном случае следует установить, что соответствующие действия по обработке персональных данных охватывались трудовой функцией работника, отражены в его должностной инструкции.

Субъектом является любое вменяемое физическое лицо, достигшее возраста 16 лет. В силу требований п. 2 ч. 1 ст. 4.6 КоАП индивидуальный

предприниматель также может являться субъектом рассматриваемого правонарушения.

В качестве примера дела может быть следующее. «*Н. работал следователем по особо важным делам. Умышленно из личной заинтересованности, не имея письменного согласия Ш. на обработку его персональных данных, а также при отсутствии служебной необходимости использовал предоставленный ему логин и пароль и вошел в АИС "ГАИ-Центр", незаконно извлек (собрал) и обработал информацию о персональных данных Ш. Суд оштрафовал Н. на 10 базовых величин по ч. 2 ст. 23.7 КоАП (дело от 20.01.2022 №17АП212391/Н)*».

В ч. 3 ст. 23.7 КоАП установлена административная ответственность за умышленное незаконное распространение персональных данных физических лиц. Под «распространением» понимаются действия, направленные на ознакомление с персональными данными неопределенного круга лиц. В качестве меры ответственности предусмотрен штраф в размере до 200 базовых величин.

Распространение может осуществляться в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет).

В качестве примера дела может быть следующее. «*11.11.2023 в 21 час 23 минуты обнаружено, что К. в мессенджере Viber сети Интернет в сообществе С. умышленно незаконно разместил информацию, являющуюся персональными данными, а именно: номер и серию паспорта, идентификационный номер, адрес места жительства К., которые позволяют идентифицировать ее как физическое лицо. Суд оштрафовал на 2 базовых величин по ч. 2 ст. 23.7 КоАП (Постановление суда Центрального района города Гомеля от 11.01.2024)*».

В ч. 4 ст. 23.7 КоАП установлена административная ответственность за несоблюдение мер обеспечения защиты персональных данных физических лиц. Они установлены в ст. 17 Закона, к ним относятся правовые, организационные и технические меры по обеспечению защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных. В ч. 3 ст. 17 Закона установлен перечень обязательных мер, к которым относится следующее:

назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных;

издание оператором (уполномоченным лицом), являющимся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных;

ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством;

установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);

осуществление технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

В качестве меры ответственности установлен дифференцированный штраф в зависимости от субъекта правонарушения: наложение штрафа на физическое лицо в размере от 2 до 10 базовых величин, на индивидуального предпринимателя - от 10 до 25 базовых величин, а на юридическое лицо - от 20 до 50 базовых величин.

Исходя из положений ст. 4.4 КоАП, ответственность за данное правонарушение применяется независимо от требования потерпевшего, его законного представителя. Однако это не лишает их права обратиться в уполномоченные органы с заявлением о начале административного процесса по ст. 23.7 КоАП по факту нарушения законодательства о защите персональных данных.

В соответствии со ст. 3.30 ПИКоАП протоколы об административных правонарушениях по ст. 23.7 КоАП имеют право составлять уполномоченные на то должностные лица органов внутренних дел, а также прокурор (при осуществлении им надзорных функций), дела рассматриваются единолично судьей районного (городского) суда.

В качестве примера дела может быть следующее. «*Суд рассмотрел дело об ответственности директора организации по ч. 4 ст. 23.7 КоАП. Согласно результатам внеплановой проверки директор не принял мер:*

– по ознакомлению работников, непосредственно обрабатывающих персональные данные, с законодательством о таких данных и с внутренними документами;

– обучению работников и иных лиц в порядке, установленном законодательством;

– определению порядка доступа к персональным данным, в том числе к обрабатываемым в информационном ресурсе;

– технической и криптографической защите персональных данных.

Организация выполнила требование НЦЗПД об устранении нарушений, а директор признал свою вину. Суд освободил его от административной ответственности с вынесением предупреждения (дело от 06.02.2023 № 26АП231/Н».

В качестве примера дела может быть следующее. «*Директор организации не принял мер по ознакомлению работников, непосредственно осуществляющих обработку персональных данных, с требованиями по защите таких данных; с документами, определяющими политику организации в отношении их обработки; а также мер по обучению сотрудников и иных лиц работе с персональными данными; по установлению порядка доступа к персональным данным, в том числе к обрабатываемым в информационном ресурсе; мер по их технической и криптографической защите. Директор признал вину и указал на частичное устранение выявленных нарушений. Суд оштрафовал его по ч. 4 ст. 23.7 КоАП на 4 БВ (дело от 30.09.2022 № 101АП222657/Н)*».

Уголовная ответственность установлена в ст. 203-1 и 203-2 Уголовного кодекса Республики Беларусь от 09.07.1999 № 275-З (далее – УК).

В ст. 203-1 УК установлена уголовная ответственность за незаконные действия в отношении информации о частной жизни и персональных данных, а в ст. 203-2 УК – за несоблюдение мер обеспечения защиты персональных данных.

Ст. 203-1 УК состоит из трех составов:

(1) Умышленные незаконные сбор, предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина.

(2) Умышленное незаконное распространение информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшее причинение существенного вреда правам, свободам и законным интересам гражданина.

(3) Действия, предусмотренные ч. 1 или 2 ст. 203-1 УК, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга.

Она применяется независимо от распространения на обработку персональных данных действия Закона. Общественно опасное деяние представлено в виде двух альтернативных действий: незаконный сбор или незаконное предоставление. Способ не имеет значения. Обязательным элементом объективной стороны является отсутствие согласия субъекта персональных данных или иных правовых оснований для обработки персональных данных.

В качестве обязательного признака объективной стороны предусмотрены общественно опасные последствия – причинение существенного вреда правам, свободам и законным интересам гражданина. Наличие общественно опасных последствий выступает основным критерием разграничения административного правонарушения и уголовно наказуемого деяния.

С субъективной стороны рассматриваемое преступление характеризуется умышленной формой вины. При этом мотив и цель для квалификации деяния как преступления значения не имеют.

Субъектом преступного посягательства является физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летного возраста.

Уголовная ответственность наступает по требованию потерпевшего. Дела частного обвинения возбуждаются лицом, пострадавшим от преступления, его законным представителем или представителем юридического лица, и производство по ним подлежит прекращению в случае примирения его с обвиняемым (ч. 2 ст. 26 УПК). Вместе с тем согласно ч. 5 ст. 26 УПК прокурор вправе возбудить уголовное дело о преступлениях частного и частно-публичного обвинения и при отсутствии заявления лица, пострадавшего от преступления, если они затрагивают существенные интересы государства и общества или совершены в отношении лица, находящегося в служебной или иной зависимости от обвиняемого либо по иным причинам не способного самостоятельно защищать свои права и законные интересы.

В ч. 2 ст. 203-1 УК установлен квалифицированный состав преступления, касающийся распространения информации о частной жизни и (или) персональных данных при аналогичных последствиях. Формы распространения не имеет значения: в сети Интернет или в социальных сетях, средствах массовой информации, размещения информации на стендах, дверях подъездов и др.

Ч. 3 ст. 203-1 УК предусматривает повышенную уголовную ответственность за рассмотренные действия, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга. В соответствии с п. 3 ч. 2 ст. 4 УК под близкими признаются близкие родственники и члены семьи потерпевшего либо иные лица, которых он обоснованно признает своими близкими.

Понятия «осуществление служебной деятельности» или «выполнение общественного долга» раскрываются в п. 14 постановления Пленума Верховного Суда Республики Беларусь от 17 декабря 2002 г. № 9 «О судебной практике по делам об убийстве (ст. 139 Уголовного кодекса Республики Беларусь)».

Под осуществлением служебной деятельности следует понимать законные действия любого лица, входящие в круг его служебных обязанностей, вытекающих из трудового договора (контракта) с государственными, частными и иными, зарегистрированными в установленном порядке предприятиями и организациями независимо от формы собственности, а также с предпринимателями.

Под выполнением общественного долга понимается осуществление гражданином как специально возложенных на него обязанностей в интересах общества или законных интересах отдельных лиц, так и других общественно полезных действий (пресечение правонарушений, сообщение органам власти о совершенном или готовящемся преступлении либо о местонахождении лица, разыскиваемого в связи с совершением им правонарушений, дача свидетелем или потерпевшим показаний, изобличающих лицо в совершении преступления, и др.).

В качестве наказания по ст. 203-1 УК предусмотрены общественные работы, штраф (в виде основного или дополнительного наказания), арест, ограничения свободы, лишение свободы.

В ст. 203-2 УК установлена ответственность за несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий.

Перечень обязательных мер по обеспечению защиты персональных данных (правовых, организационных и технических) определен в п. 3 ст. 17 Закона.

Рассматриваемый состав является материальным и будет окончен с момента наступления последствий. В качестве общественно опасных последствий, предусмотренных ст. 203-2 УК, является одновременное распространение персональных данных (ознакомление с ними неопределенного круга лиц) и причинение тяжких последствий.

Субъект преступного посягательства специальный – лицо, осуществляющее обработку персональных данных.

Лицо может осуществлять обработку персональных данных в связи с должностным положением, трудовыми или служебными обязанностями, выполнением обязательств по гражданско-правовому договору и на иных законных основаниях.

Как самостоятельная правовая форма гражданско-правовой ответственности за нарушение законодательства о персональных данных может быть использован гражданско-правовой институт обязательств вследствие причинения вреда, предусмотренный главой 58 ГК.

Юридическое лицо либо гражданин возмещает вред, причиненный его работником при исполнении своих трудовых (служебных, должностных) обязанностей (п. 1 ст. 937 ГК). При этом наниматель не несет ответственности в случае, если работник причинил вред третьему лицу не при исполнении трудовых обязанностей.

Работник, причинивший вред, может добровольно возместить его полностью или частично. В случае отказа работника от возмещения причиненного его противоправными действиями (бездействием) при исполнении им служебных, должностных или иных трудовых обязанностей вреда, он может быть взыскан в судебном порядке.

Лицо, возместившее вред, причиненный другим лицом (работником при исполнении им служебных, должностных или иных трудовых обязанностей, лицом, управляющим транспортным средством и т.п.), имеет право обратного требования (регресса) к этому лицу в размере выплаченного возмещения, если иной размер не определен законодательством, или в порядке, им устанавливаемом (п. 1 ст. 950 ГК).

При этом следует руководствоваться положениями п. 50 постановления Пленума Верховного Суда Республики Беларусь от 29 марта 2001 г. № 2 «О некоторых вопросах применения судами законодательства о труде». Споры, связанные с регрессными требованиями, относят к трудовым спорам.

Удержание причиненного ущерба из заработной платы работника допускается в соответствии с требованиями ст. 107 ТК.

Возмещение морального вреда осуществляется по правилам ст. 152 ГК и § 4 главы 58 ГК и детализировано в постановлении Пленума Верховного Суда Республики Беларусь от 28 сентября 2000 г. № 7 «О практике применения судами законодательства, регулирующего компенсацию морального вреда» (далее - постановление Пленума №7). При этом в п. 12 постановления Пленума N 7 особо отмечается, что правило, изложенное в ст. 937 ГК об ответственности юридических лиц или граждан по возмещению вреда, причиненного их работниками при исполнении ими своих трудовых (служебных, должностных) обязанностей, распространяется и на случаи причинения морального вреда.

Под моральным вредом следует понимать испытываемые гражданином физические и (или) нравственные страдания (ч. 1 ст. 152 ГК).

Если гражданину причинен моральный вред действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законодательством, гражданин вправе требовать от нарушителя денежную компенсацию указанного вреда. При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинен вред.

Понятие физических и нравственных страданий раскрывается в п. 8 постановления Пленума № 7.

К числу наиболее распространенных физических страданий относятся повышение артериального давления, сердечная аритмия, постоянные головные боли, обострение хронических заболеваний (астма, язва, гипертония), проблемы со сном, а также общее ухудшение состояния здоровья. Нравственные страдания выражаются в ощущениях страха, стыда, унижения, тревоги, беспокойстве за здоровье, состоянии постоянного стресса, раздражительности, эмоциональном потрясении, а равно в иных неблагоприятных для человека в психологическом аспекте переживаниях.

2. ПРАКТИЧЕСКИЙ РАЗДЕЛ

СЕМИНАРСКИЕ ЗАНЯТИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
для очной (дневной) формы получения общего высшего образования по специальности 6-05-0421-02 «Международное право»

Семинарское занятие 1

Тема 2. Приватность и идентификация личности: международные подходы (2 часа)

Вопросы для обсуждения:

1. Основополагающие международные правовые акты в области защиты персональных данных.

2. Правовое регулирование защиты персональных данных в странах ЕАЭС и СНГ.

3. Правовые основы защиты персональных данных в Европейском союзе.

Темы рефератов:

1. Биометрические методы идентификации (ДНК, отпечатки пальцев).

2. Цифровая идентификация личности.

3. Защита персональных данных в контексте цифровых технологий с учетом современных вызовов и угроз.

Практические задания:

1. Сопоставьте термины, закрепленные в ст. 4 GDPR и ст. 1 Закона о персональных данных.

2. Изучите положения ст. 5 GDPR.

Как соотносятся принципы, касающиеся обработки персональных данных, закрепленные в GDPR, с общими требованиями к обработке персональных данных, определенными в ст. 4 Закона о персональных данных?

3. Составьте глоссарий из следующих терминов: уровни надежности, интерфейс прикладного программирования (API), биомеханическая биометрия, учетные данные, провайдер учетных данных (CSP), атака с подстановкой учетных данных (credential stuffing), провайдер идентификационных услуг (IDSP), прогрессивное удостоверение, полагающаяся сторона (ПС).

Семинарское занятие 2

Тема 5. Правовое регулирование защиты персональных данных в Республике Беларусь (2 часа)

Практические задания:

1. Изучите положения ст. 17 и 18 Закона об информации, информатизации и защите информации и ст. 1 Закона о персональных данных. Дайте определение понятию «персональные данные».

Как соотносятся понятия «информация о частной жизни» и «персональные данные»? Ответ аргументируйте.

2. Гражданин Ю. разместил в своем аккаунте в социальной сети видео с участием своего родственника с поздравлениями по случаю его свадьбы.

Родственник гражданина Ю., посчитав видео неудачным, обратился к последнему с требованием об удалении поста, указав на нарушение Закона о персональных данных.

Распространяются ли положения Закона о персональных данных на указанные отношения? Можно ли признать гражданина А. оператором по смыслу Закона о персональных данных?

3. При трудоустройстве кадровая служба организации запросила у гражданина М. фотографию для оформления пропуска. Гражданин М., сославшись на то, что фотографическое изображение является биометрическими персональными данными, указал на необходимость получения у него на такую обработку согласия.

Можно ли согласиться с доводами, представленными гражданином М.? Что представляют собой биометрические персональные данные? Какие сведения могут быть отнесены к биометрическим персональным данным? В чем заключаются особенности обработки биометрических персональных данных?

4. Перечислите общие требования к обработке персональных данных, закрепленные в ст. 4 Закона о персональных данных, охарактеризуйте содержание каждого из них.

Семинарское занятие 3

Тема 7. Правовые основания для обработки персональных данных в Республике Беларусь (2 часа)

Практические задания:

1. Сопоставьте правовые основания обработки персональных данных, закрепленные в ст. 6 и 8 Закона о персональных данных.

Перечислите частные случаи обработки персональных данных, необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами. В чем заключается специфика обработки специальных персональных данных?

2. В каком(их) из приведенных ниже случаев правовым основанием обработки персональных данных субъектов может выступать согласие?

а) при обращении в медицинский центр запрашивается согласие на обработку персональных данных в целях оказания медицинской помощи, без которого ее отказываются предоставлять;

б) при оформлении ребенка в первый класс школы родителям предложили подписать согласие на обработку персональных данных, а в случае отказа от подписания ребенка отказываются принимать в учреждение образования;

в) на интернет-сайте появляется сообщение с просьбой предоставить согласие на обработку куки-файлов с вариантами возможного ответа: «согласен», «не согласен», «выбрать настройки».

Оцените необходимость получения согласия. Дайте аргументированный ответ.

3. В форму заявления на зачисление несовершеннолетнего в группу для занятий по вокалу включена графа «Согласен на обработку персональных данных моего ребенка в соответствии с требованиями Закона о персональных данных».

Проанализируйте сложившуюся ситуацию на предмет соответствия требованиям Закона о персональных данных. С достижением какого возраста Закон о персональных данных связывает способность лица давать согласие на обработку его персональных данных самостоятельно?

4. Определите статус согласия, указав при этом, в каких случаях оно выступает в качестве правового основания обработки персональных данных по смыслу Закона о персональных данных:

а) согласие на неотложное медицинское вмешательство;

б) согласие на оказание психологической помощи гражданину;

в) согласие на осуществление рекламной рассылки при регистрации личного кабинета на сайте интернет-магазина;

г) согласие родителей на выезд ребенка за границу;

д) согласие законного представителя на осуществление вакцинации в отношении его ребенка;

е) согласие преподавателя учреждения высшего образования на размещение фотоизображения на сайте университета.

5. В каких из ситуаций осуществляется обработка общедоступных персональных данных:

а) при использовании резюме соискателей, направленных на электронную почту организации;

б) при подготовке библиографического описания для каталога библиотеки;

в) при использовании размещенной в открытом доступе информации о сборе средств на лечение;

г) при направлении поздравительного адреса по случаю Дня учителя директорам школ на их домашний адрес.

Что представляют собой общедоступные персональные данные? Какие особенности устанавливает Закон о персональных данных для их обработки?

Семинарское занятие 4

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь (2 часа)

Практические задания:

1. Какие меры необходимо принять нанимателю для обеспечения принципа прозрачности обработки персональных данных работников при осуществлении видеонаблюдения?

2. Опишите алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона о персональных данных.

Какие документы должны быть разработаны у оператора (уполномоченного лица) в связи с реализацией мер, предусмотренных названным алгоритмом?

3. Специалистом по осуществлению внутреннего контроля за обработкой персональных данных торговой сети в рамках приведения деятельности организации в соответствие с требованиями Закона о персональных данных была разработана форма согласия на обработку персональных данных. Работникам предлагалось предоставить согласие на изготовление визиток с указанием их фамилии, имени, отчества, номера телефона, адреса электронной почты, а также бейджей с размещением на них фамилии, имени, отчества и должности работника.

Оцените представленную ситуацию на предмет соответствия требованиям Закона о персональных данных.

4. Имеется ли необходимость в составлении Политики обработки персональных данных в организации?

5. Подготовьте отчет о проведении внутреннего контроля за деятельностью кадровой службы организации с отражением нарушений, которые могут быть выявлены в ее деятельности и предложениями по их устранению.

Семинарское занятие 5

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных (2 часа)

Практические задания:

1. Изучите содержание п. 10 ч. 1 ст. 47 ТК.

В каких случаях возможно применение увольнения в качестве дисциплинарного взыскания по указанному основанию?

2. Изучите содержание ст. 2031 и 2032 УК.

Какая ответственность установлена за незаконные действия (умышленные незаконные сбор, предоставление, распространение) в отношении информации о частной жизни и персональных данных? Несоблюдение каких мер по защите персональных данных может повлечь уголовную ответственность?

3. Сравните санкции, предусмотренные за нарушение законодательства о персональных данных в Беларуси и зарубежных странах.

В каких странах предусмотрена более строгая ответственность за совершение преступлений и правонарушений в сфере защиты персональных данных?

4. Оцените предложенные ситуации на предмет наличия нарушений законодательства о персональных данных, дайте им юридическую оценку:

а) воспитатель старшей группы дошкольного учреждения образования направила в группу, созданную в мессенджере ВКонтакте, список должников по питанию за месяц с просьбой оплатить до указанной в сообщении даты;

б) отдел образования направил информацию о результатах проведения социального расследования по месту работы родителей для рассмотрения

нанимателями и проведения ими в отношении своих работников воспитательной работы;

в) кадровой службой организации составлен Excel-документ, включающий сведения о соискателях на трудоустройство, представлявших свои резюме в течение последних пяти лет, но не принятых на работу к этому нанимателю.

СЕМИНАРСКИЕ ЗАНЯТИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
для очной (дневной) формы получения общего высшего образования по специальности 6-05-0421-03 «Экономическое право»

Семинарское занятие 1

Тема 2. Приватность и идентификация личности: международные подходы (2 часа)

Вопросы для обсуждения:

1. Основополагающие международные правовые акты в области защиты персональных данных.
2. Правовое регулирование защиты персональных данных в странах ЕАЭС и СНГ.
3. Правовые основы защиты персональных данных в Европейском союзе.

Темы рефератов:

1. Биометрические методы идентификации (ДНК, отпечатки пальцев).
2. Цифровая идентификация личности.
3. Защита персональных данных в контексте цифровых технологий с учетом современных вызовов и угроз.

Практические задания:

1. Сопоставьте термины, закрепленные в ст. 4 GDPR и ст. 1 Закона о персональных данных.
2. Изучите положения ст. 5 GDPR.

Как соотносятся принципы, касающиеся обработки персональных данных, закрепленные в GDPR, с общими требованиями к обработке персональных данных, определенными в ст. 4 Закона о персональных данных?

3. Составьте глоссарий из следующих терминов: уровни надежности, интерфейс прикладного программирования (API), биомеханическая биометрия, учетные данные, провайдер учетных данных (CSP), атака с подстановкой учетных данных (credential stuffing), провайдер идентификационных услуг (IDSP), прогрессивное удостоверение, полагающаяся сторона (ПС).

Семинарское занятие 2

Тема 5. Правовое регулирование защиты персональных данных в Республике Беларусь (2 часа)

Практические задания:

1. Изучите положения ст. 17 и 18 Закона об информации, информатизации и защите информации и ст. 1 Закона о персональных данных. Дайте определение понятию «персональные данные».

Как соотносятся понятия «информация о частной жизни» и «персональные данные»? Ответ аргументируйте.

2. Гражданин Ю. разместил в своем аккаунте в социальной сети видео с участием своего родственника с поздравлениями по случаю его свадьбы. Родственник гражданина Ю., посчитав видео неудачным, обратился к последнему с требованием об удалении поста, указав на нарушение Закона о персональных данных.

Распространяются ли положения Закона о персональных данных на указанные отношения? Можно ли признать гражданина А. оператором по смыслу Закона о персональных данных?

3. При трудоустройстве кадровая служба организации запросила у гражданина М. фотографию для оформления пропуска. Гражданин М., сославшись на то, что фотографическое изображение является биометрическими персональными данными, указал на необходимость получения у него на такую обработку согласия.

Можно ли согласиться с доводами, представленными гражданином М.? Что представляют собой биометрические персональные данные? Какие сведения могут быть отнесены к биометрическим персональным данным? В чем заключаются особенности обработки биометрических персональных данных?

4. Перечислите общие требования к обработке персональных данных, закрепленные в ст. 4 Закона о персональных данных, охарактеризуйте содержание каждого из них.

Семинарское занятие 3

Тема 7. Правовые основания для обработки персональных данных в Республике Беларусь (2 часа)

Практические задания:

1. Сопоставьте правовые основания обработки персональных данных, закрепленные в ст. 6 и 8 Закона о персональных данных.

Перечислите частные случаи обработки персональных данных, необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами. В чем заключается специфика обработки специальных персональных данных?

2. В каком(их) из приведенных ниже случаев правовым основанием обработки персональных данных субъектов может выступать согласие?

а) при обращении в медицинский центр запрашивается согласие на обработку персональных данных в целях оказания медицинской помощи, без которого ее отказываются предоставлять;

б) при оформлении ребенка в первый класс школы родителям предложили подписать согласие на обработку персональных данных, а в случае отказа от подписания ребенка отказываются принимать в учреждение образования;

в) на интернет-сайте появляется сообщение с просьбой предоставить согласие на обработку куки-файлов с вариантами возможного ответа: «согласен», «не согласен», «выбрать настройки».

Оцените необходимость получения согласия. Дайте аргументированный ответ.

3. В форму заявления на зачисление несовершеннолетнего в группу для занятий по вокалу включена графа «Согласен на обработку персональных данных моего ребенка в соответствии с требованиями Закона о персональных данных».

Проанализируйте сложившуюся ситуацию на предмет соответствия требованиям Закона о персональных данных. С достижением какого возраста Закон о персональных данных связывает способность лица давать согласие на обработку его персональных данных самостоятельно?

4. Определите статус согласия, указав при этом, в каких случаях оно выступает в качестве правового основания обработки персональных данных по смыслу Закона о персональных данных:

а) согласие на неотложное медицинское вмешательство;

б) согласие на оказание психологической помощи гражданину;

в) согласие на осуществление рекламной рассылки при регистрации личного кабинета на сайте интернет-магазина;

г) согласие родителей на выезд ребенка за границу;

д) согласие законного представителя на осуществление вакцинации в отношении его ребенка;

е) согласие преподавателя учреждения высшего образования на размещение фотоизображения на сайте университета.

5. В каких из ситуаций осуществляется обработка общедоступных персональных данных:

а) при использовании резюме соискателей, направленных на электронную почту организации;

б) при подготовке библиографического описания для каталога библиотеки;

в) при использовании размещенной в открытом доступе информации о сборе средств на лечение;

г) при направлении поздравительного адреса по случаю Дня учителя директорам школ на их домашний адрес.

Что представляют собой общедоступные персональные данные? Какие особенности устанавливает Закон о персональных данных для их обработки?

Семинарское занятие 4

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь (2 часа)

Практические задания:

1. Какие меры необходимо принять нанимателю для обеспечения принципа прозрачности обработки персональных данных работников при осуществлении видеонаблюдения?

2. Опишите алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона о персональных данных.

Какие документы должны быть разработаны у оператора (уполномоченного лица) в связи с реализацией мер, предусмотренных названным алгоритмом?

3. Специалистом по осуществлению внутреннего контроля за обработкой персональных данных торговой сети в рамках приведения деятельности организации в соответствие с требованиями Закона о персональных данных была разработана форма согласия на обработку персональных данных. Работникам предлагалось предоставить согласие на изготовление визиток с указанием их фамилии, имени, отчества, номера телефона, адреса электронной почты, а также бейджей с размещением на них фамилии, имени, отчества и должности работника.

Оцените представленную ситуацию на предмет соответствия требованиям Закона о персональных данных.

4. Имеется ли необходимость в составлении Политики обработки персональных данных в организации?

5. Подготовьте отчет о проведении внутреннего контроля за деятельностью кадровой службы организации с отражением нарушений, которые могут быть выявлены в ее деятельности и предложениями по их устранению.

Семинарское занятие 5

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных (2 часа)

Практические задания:

1. Изучите содержание п. 10 ч. 1 ст. 47 ТК.

В каких случаях возможно применение увольнения в качестве дисциплинарного взыскания по указанному основанию?

2. Изучите содержание ст. 2031 и 2032 УК.

Какая ответственность установлена за незаконные действия (умышленные незаконные сбор, предоставление, распространение) в отношении информации о частной жизни и персональных данных? Несоблюдение каких мер по защите персональных данных может повлечь уголовную ответственность?

3. Сравните санкции, предусмотренные за нарушение законодательства о персональных данных в Беларуси и зарубежных странах.

В каких странах предусмотрена более строгая ответственность за совершение преступлений и правонарушений в сфере защиты персональных данных?

4. Оцените предложенные ситуации на предмет наличия нарушений законодательства о персональных данных, дайте им юридическую оценку:

а) воспитатель старшей группы дошкольного учреждения образования направила в группу, созданную в мессенджере ВКонтакте, список должников по питанию за месяц с просьбой оплатить до указанной в сообщении даты;

б) отдел образования направил информацию о результатах проведения социального расследования по месту работы родителей для рассмотрения нанимателями и проведения ими в отношении своих работников воспитательной работы;

в) кадровой службой организации составлен Excel-документ, включающий сведения о соискателях на трудоустройство, представлявших свои резюме в течение последних пяти лет, но не принятых на работу к этому нанимателю.

СЕМИНАРСКИЕ ЗАНЯТИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
для заочной формы получения общего высшего образования по специальности 6-05-0421-03 «Экономическое право»

Семинарское занятие 1

Тема 9. Документальное оформление порядка обработки персональных данных у оператора в Республике Беларусь (1 час).

Тема 10. Ответственность за нарушения законодательства в сфере персональных данных (1 часа)

Практические задания:

1. Какие меры необходимо принять нанимателю для обеспечения принципа прозрачности обработки персональных данных работников при осуществлении видеонаблюдения?

2. Опишите алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона о персональных данных.

Какие документы должны быть разработаны у оператора (уполномоченного лица) в связи с реализацией мер, предусмотренных названным алгоритмом?

3. Специалистом по осуществлению внутреннего контроля за обработкой персональных данных торговой сети в рамках приведения деятельности организации в соответствие с требованиями Закона о персональных данных была разработана форма согласия на обработку персональных данных. Работникам предлагалось предоставить согласие на изготовление визиток с указанием их фамилии, имени, отчества, номера телефона, адреса электронной почты, а также бейджей с размещением на них фамилии, имени, отчества и должности работника.

Оцените представленную ситуацию на предмет соответствия требованиям Закона о персональных данных.

4. Имеется ли необходимость в составлении Политики обработки персональных данных в организации?

5. Подготовьте отчет о проведении внутреннего контроля за деятельностью кадровой службы организации с отражением нарушений, которые могут быть выявлены в ее деятельности и предложениями по их устранению.

6. Изучите содержание п. 10 ч. 1 ст. 47 ТК.

В каких случаях возможно применение увольнения в качестве дисциплинарного взыскания по указанному основанию?

7. Изучите содержание ст. 2031 и 2032 УК.

Какая ответственность установлена за незаконные действия (умышленные незаконные сбор, предоставление, распространение) в отношении информации о частной жизни и персональных данных? Несоблюдение каких мер по защите персональных данных может повлечь уголовную ответственность?

8. Сравните санкции, предусмотренные за нарушение законодательства о персональных данных в Беларуси и зарубежных странах.

В каких странах предусмотрена более строгая ответственность за совершение преступлений и правонарушений в сфере защиты персональных данных?

9. Оцените предложенные ситуации на предмет наличия нарушений законодательства о персональных данных, дайте им юридическую оценку:

а) воспитатель старшей группы дошкольного учреждения образования направила в группу, созданную в мессенджере ВКонтакте, список должников по питанию за месяц с просьбой оплатить до указанной в сообщении даты;

б) отдел образования направил информацию о результатах проведения социального расследования по месту работы родителей для рассмотрения нанимателями и проведения ими в отношении своих работников воспитательной работы;

в) кадровой службой организации составлен Excel-документ, включающий сведения о соискателях на трудоустройство, представлявших свои резюме в течение последних пяти лет, но не принятых на работу к этому нанимателю.

3. РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. История развития правового регулирования защиты персональных данных в Европейском союзе. Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера 1981 г.
2. Общая характеристика законодательства о защите персональных данных государств – членов ЕАЭС.
3. Понятие приватности и защиты персональных данных. История информационной приватности. Виды приватности.
4. История создания и общая характеристика Генерального регламента о защите персональных данных 2016г.
5. Ключевые термины и определения в Генеральном регламенте о защите персональных данных 2016 г. Основные принципы обработки персональных данных в Европейском Союзе.
6. Субъекты правоотношения в сфере защиты персональных данных в Европейском Союзе: «Data controller», «Data processor», «Data subject».
7. Основания обработки персональных данных и их характеристика по Генеральному регламенту о защите персональных данных 2016 г.
8. Основания и условия привлечения к ответственности по Генеральному регламенту о защите персональных данных 2016 г.
9. Правовое регулирование защиты персональных данных в Республике Беларусь.
10. Общая характеристика Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
11. Национальный центр защиты персональных данных Республики Беларусь: правовой статус, основные задачи и функции.
12. Юридическая сила и общая характеристика приказов директора Национального центра защиты персональных данных Республики Беларусь.
13. Понятие и категории персональных данных по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».
14. Общая характеристика специальных персональных данных.
15. Особенности защиты биометрических и генетических персональных данных.
16. Субъекты правоотношения в сфере защиты персональных данных в Республике Беларусь: субъект персональных данных, оператор и уполномоченное лицо.
17. Права и обязанности оператора при обработке персональных данных.
18. Права и обязанности уполномоченного лица при обработке персональных данных.
19. Понятие, виды и формы обработки персональных данных в Республике Беларусь.

20. Правовые основания обработки персональных данных по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

21. Общая характеристика согласия субъекта персональных данных на обработку персональных данных в Республике Беларусь.

22. Условия получения согласия субъекта персональных данных на обработку персональных данных.

23. Основания обработки персональных данных без согласия субъекта персональных данных (специальных персональных данных) в Республике Беларусь.

24. Общая характеристика обработки персональных данных по поручению оператора в Республике Беларусь. Обязательные договорные пункты.

25. Особенности обработки персональных данных в рамках трудовых отношений в Республике Беларусь.

26. Общая характеристика трансграничной передачи персональных данных. Порядок документального оформления.

27. Права субъектов персональных данных в Республике Беларусь. Характеристика права на отзыв согласия субъекта персональных данных, права на получение информации, касающейся обработки персональных данных, и изменение персональных данных, а также права на получение информации о предоставлении персональных данных третьим лицам.

28. Права субъектов персональных данных в Республике Беларусь. Характеристика права на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных, а также права на возмещение морального вреда, причиненного незаконной обработкой персональных данных. Порядок реализации прав субъекта персональных данных.

29. Правовые, организационные и технические меры по обеспечению защиты персональных данных в Республике Беларусь.

30. Документационное оформление обработки персональных данных оператором по Закону Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных».

31. Функции, права и обязанности лица, ответственного за осуществление внутреннего контроля за защитой персональных данных в организации, в Республике Беларусь.

32. Порядок и условия привлечения к административной ответственности за незаконную обработку персональных данных в Республике Беларусь.

33. Порядок и условия привлечения к уголовной ответственности за незаконную обработку персональных данных в Республике Беларусь.

34. Основания и условия привлечения к гражданско-правовой ответственности за нарушение законодательства о персональных данных в Республике Беларусь.

35. Порядок и условия наложения дисциплинарного взыскания за нарушение порядка обработки персональных данных, установленного законодательством и локальными правовыми актами.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ УПРАВЛЯЕМОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Управляемая самостоятельная работа студентов служит закреплению знаний, а также способствует овладению практическими материалами с учетом их индивидуальных способностей и наклонностей. Управляемая самостоятельная работа студентов включает: изучение международных договоров, нормативных правовых актов по темам дисциплины с последующим обсуждением на семинарских занятиях и решением ситуационных задач; решение тестовых заданий; проверка контрольной работы.

Управляемая самостоятельная работа по изучению учебной дисциплины является объективно необходимым компонентом комплексного метода подготовки и обучения в образовательном процессе, в равной степени важным и логически связанным с иными элементами и формами. Управляемая самостоятельная работа предполагает автономное, дистанционное освоение поставленных целей и задач в пределах учебного материала. Данная форма подготовки должна носить логически последовательный, системный, комплексный характер и предполагает использование всех доступных рекомендуемых форм и методов подготовки.

Важным этапом формирования первичных навыков управляемой самостоятельной работы является ознакомление с содержанием учебной программы, темами и информационно-методической частью. Непременным условием усвоения содержания учебной дисциплины является углубленное изучение рекомендуемой учебной и специальной литературы.

Управляемая самостоятельная работа предусмотрена учебным планом для развития способностей обучающихся к самостоятельной научной исследовательской деятельности. Такая форма приобретения обучающимися знаний, навыков, умений служит: углубленному изучению определенной темы, ее отдельных вопросов, теоретико-правовых проблем и, тем самым, росту знаний студента; формированию умений использования литературных источников; поиска, отбора и изучения информации; критического обзора литературы, осуществлению полного и последовательного анализа источников; овладению отдельными методами и методологией научного исследования, анализом нормативных правовых актов, относящихся к используемым источникам; выработке навыков изложения изученного материала; формированию собственной позиции студента по правовым вопросам и возможности ее выражения, в том числе изложения собственных теоретических и экспериментальных результатов, оценка достоверности полученных данных.

При подготовке управляемой самостоятельной работы студентами рекомендуется проводить самостоятельный подбор соответствующих нормативных правовых актов, учебной и специальной литературы по темам дисциплины.

ПЕРЕЧЕНЬ ЗАДАНИЙ И КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ УСР

№ темы	Тема УСР	Кол-во часов	Метод. обеспечение	Форма контроля
4 семестр (4 часа)				
4.	Средства правовой защиты персональных данных и практика исполнения генерального регламента	2	Интернет-ресурсы, библиотека университета	РПЗ, ЗТТ
6.	Основные понятия в области защиты персональных данных в Республике Беларусь	2	Интернет-ресурсы, библиотека университета	РПЗ, ЗТТ, Э

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ УСР

Тема 4. Средства правовой защиты персональных данных и практика исполнения генерального регламента (2 часа)

1. Подготовить презентацию по вопросу: Стандартные договорные оговорки. Бизнес-процессы юридических лиц. «Best practices». Представители на территории Европейского Союза.

2. Подготовить сравнительную таблицу по вопросу: Виды нарушений Генерального регламента о защите персональных данных. Действия субъектов правоотношений в случаях нарушений в сфере защиты персональных данных.

3. Охарактеризовать: Меры ответственности за несанкционированную обработку персональных данных.

4. Подготовить письменный доклад по вопросам: Порядок и условия наложения административного штрафа. Возмещение ущерба контролером в пользу субъекта персональных данных. Уголовная ответственность за нарушение правил обработки персональных данных в государствах-членах Европейского Союза.

Тема 6. Основные понятия в области защиты персональных данных в Республике Беларусь (2 часа)

Вопросы, подлежащие изучению:

1. Научные подходы к понятию «персональные данные». Нормативное понятие и признаки персональных данных в Республики Беларусь. Соотношение понятий «персональные данные» и «банковская тайна», «врачебная тайна», «нотариальная тайна».

2. Категории персональных данных. Общедоступные персональные данные. Специальные персональные данные. Биометрические и генетические персональные данные.

3. Субъекты правоотношения в сфере защиты персональных данных: субъект персональных данных, оператор и уполномоченное лицо. Их функции, права и обязанности в рассматриваемом правоотношении.

4. Понятие обработки персональных данных, их виды и формы. Общие требования к обработке персональных данных: законность, соразмерность и справедливость, наличие правового основания, ограничение цели, запрет избыточности, прозрачность, ограничение хранения, достоверность.

5. Особенности обработки персональных данных при их обезличивании, блокировании и удалении. Предоставление и распространение персональных данных.

Задание: составить тестовое задание, состоящее из 35 вопросов (5 вариантов ответа).

4. ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Василевич, Г. А. Информационное право : учебн. пособие / М. С. Абламейко [и др.] ; под общ. ред. Г. А. Василевича, М. С. Абламейко. – Минск : Адукацыя і выхаванне, 2021. – 424 с.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

2. Абламейко, М. С. Защита визуальных персональных данных: правовые аспекты / М. С. Абламейко // Веб-программирование и интернет-технологии WebConf2021 : материалы 5-й Междунар. науч.-практ. конференции, Минск, 18–21 мая 2021 г. / БГУ, Механико-математический фак. ; редкол.: И. М. Галкин (отв. ред.) [и др.]. – Минск : БГУ, 2021. – С. 318–321.

3. Абламейко, М. С. Правовое регулирование персональных данных с учетом введения ID-карт и биометрических паспортов / М. С. Абламейко // Журн. Белорус. гос. ун-та. Серия «Право». – 2018. – № 1. – С. 14–20.

4. Абламейко, М. С. Биометрические персональные данные и дипфейки: правовой аспект / М. С. Абламейко, Н. В. Шакель // Право.by : научно-практический журнал / учредитель Национальный центр правовой информации Республики Беларусь, Кафедра ЮНЕСКО по информационным технологиям и праву. – 2024. – № 3. – URL: https://journal.pravo.by/articles/informatsionnoe-pravo-pravovaya-informatizatsiya/biometricheskie-personalnye-dannye-i-dipfeyki-pravovoy-aspekt/ (дата обращения 19.10.2024).

5. Абламейко, М. С. Трансграничная передача персональных данных в рамках ЕАЭС / М. С. Абламейко, Н. В. Шакель // Право.by : научно-практический журнал / учредитель Национальный центр правовой информации Республики Беларусь, Кафедра ЮНЕСКО по информационным технологиям и праву. – 2023. – № 1. – С. 113–120.

6. Архипов, В. В. Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория / В. В. Архипов // ЮрФак : изучение права онлайн. – URL: https://urfac.ru/?p=144 (дата обращения 19.10.2024).

7. Вабищевич, В. В. Персональные данные: пределы и объем их уголовно-правовой охраны / В. В. Вабищевич // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы : навукова-тэарэтычны часопіс. – 2020. – Т. 10, № 2. – С. 83–90.

8. Вабищевич, В. В. Социально-правовые и исторические предпосылки криминализации вмешательства в персональные данные / В. В. Вабищевич // Журн. Белорус. гос. ун-та. Право. – 2020. – № 1. – С. 61–71.

9. Вабищевич, В. В. Уголовно-правовая охрана персональных данных: отдельные направления совершенствования / В. В. Вабищевич // Актуальные

проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Международный университет "МИТСО". – 2023. – № 2 (22). – С. 81–94.

10. Валюшко-Орса, Н. В. Сущностно-содержательные аспекты персональных данных в Республике Беларусь / Н. В. Валюшко-Орса // Журн. Белорус. гос. ун-та. Право. – 2017. – № 2. – С. 17-23.

11. Гавриленко, А. И. К вопросу о возрасте согласия на обработку персональных данных / А. И. Гавриленко // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Междунар. университет "МИТСО". – 2023. – № 2 (22). – С. 95–106.

12. Дудко, М. О. Правовой механизм защиты персональных данных в сети Интернет / М. О. Дудко // Международное гуманитарное право глазами белорусской общественности : материалы междунар. науч. форума, Минск, 30 окт. 2020 г. / Белорус. гос. ун-т ; редкол.: Е. Ф. Довгань (гл. ред.) [и др.]. – Минск : БГУ, 2020. – С. 87–98.

13. Дудко, О. М. Особенности правового регулирования общедоступных персональных данных / М. О. Дудко // Современные проблемы юридической науки и практики в условиях глобализации общественных отношений : сборник научных статей / Учреждение образования "Гродненский государственный университет им. Я. Купалы". – Гродно, 2022. – С. 67–71.

14. Захилько, К. С. Существенный вред как признак уголовной противоправности незаконных действий в отношении информации о частной жизни и персональных данных / К. С. Захилько // Журн. Белорус. гос. ун-та. Право. – 2022. – № 2. – С. 58–68.

15. Ипатов, В. Д. Проблемы применения законодательства о персональных данных в свете развития информационных технологий / В. Д. Ипатов, Н. А. Саванович // Право.by. – 2021. – № 5. – С. 60–65.

16. Ипатов, В. Д. Проблемы применения законодательства о персональных данных в свете развития информационных технологий / В. Д. Ипатов, Н. А. Саванович // Информационные технологии и право: правовая информатизация-2021 : сб. материалы VII Междунар. науч.-практ. конф. (г. Минск, 28 октября 2021 г.) / под общ. ред. А. Ф. Мательского. – Минск, 2021. – С. 156–159.

17. Исаев, А.С. Правовые основы организации защиты персональных данных / А.С. Исаев, Е.А. Хлюпина // СПб. : НИУ ИТМО, 2014. – 106 с. – URL: https://books.ifmo.ru/file/pdf/1570.pdf (дата обращения 19.10.2024).

18. Кирильчик, А. А. Аудиториум ilex. Персональные данные в банках. Биометрические данные и цифровые технологии / А. А. Кирильчик // КонсультантПлюс / ООО «ЮрСпектр». – Минск, 2024.

19. Кунец, А. Г. Научные подходы к пониманию конституционного права на личную жизнь / А. Г. Кунец // Труд. Профсоюзы. Общество = Labour. Trade Unions. Society : ежеквартальный научно-практический журнал / Федерация профсоюзов Беларуси, Междунар. ун-т "МИТСО". – 2018. – № 2. – С. 74–78.

20. Лосев, В. В. Нарушение законодательства о защите персональных данных: административная и уголовная ответственность / В. В. Лосев //

Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Международный университет "МИТСО". – 2023. – № 2 (22). – С. 65–80.

21. Методологические документы, рекомендации // Национальный центр защиты персональных данных Республики Беларусь. – URL: https://cpd.by/ (дата обращения 19.10.2024).

22. Михалевич, Е. В. Обработка персональных данных: анализ законодательства и судебной практики – М., 2019. – Вып. 18. – 143 с.

23. Официальные руководства и разъяснения, заключения и рекомендации общеевропейского надзорного органа в области защиты персональных данных // GDPR TEXT. – URL: https://gdpr-text.com/ru/guidelines/ (дата обращения 19.10.2024).

24. Полещук, Д. Г. Видеонаблюдение и видеосъемка как обработка персональных данных / Д. Г. Полещук // Актуальные проблемы гражданского права: научный журнал / Учреждение образования Федерации профсоюзов Беларуси "Междунар. университет "МИТСО". – 2023. – № 2 (22). – С. 32–48.

25. Полещук, Д. Г. Ответственность за незаконные действия с персональными данными: текущее состояние и перспективы / Д. Г. Полещук // Законность и правопорядок. – 2020. – № 4. – С. 44-49.

26. Полещук, Д. Г. Уголовная ответственность за незаконные действия с персональными данными: новеллы правового регулирования и направления их возможного практического применения / Д. Г. Полещук // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2021. – Вып. 16. – С. 756-768.

27. Полещук, Д. Г. Право на защиту персональных данных: конституционные основы и их реализация в законодательстве и правоприменении / Д. Г. Полещук // Конституционное право как фактор динамичного развития белорусского государства: история и современность : материалы респ. науч.-практ. конф., Минск, 15 окт. 2021 г. / Белорус. гос. ун-т ; редкол.: Г. А. Василевич (гл. ред.), А. В. Шавцова; В. Е. Петухова. – Минск : БГУ, 2021. – С. 225–229.

28. Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» : по состоянию на 19.10.2024 г. / А. А. Гаев [и др.] // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

29. Рыбак, С. В. Направления развития защиты персональных данных в Республике Беларусь / С. В. Рыбак // Право. Экономика. Социальное партнерство : сб. докладов Междунар. науч.-практ. конф., посвященной 90-летию Учреждения образования Федерации профсоюзов Беларуси "Международный университет "МИТСО" (г. Минск, 26 марта 2020 г.) : в 2 ч. / редкол.: В. В. Лосев (гл. ред.) [и др.]. – Минск : МИТСО, 2020. Ч. 1. – С. 491–496.

30. Саванович, Н. А. К вопросу о соотношении информации о частной жизни и персональных данных / Н. А. Саванович // КонсультантПлюс / ООО

«ЮрСпектр». – Минск, 2024.

31. Саванович, Н. А. Персональные данные в условиях технологии Big Data (больших данных): по состоянию на 12.02.2019 г. / Н. А. Саванович // ЭТАЛОН. Правоприменительная практика / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

32. Саванович, Н. А. Эволюция понимания персональных данных на современном этапе: по состоянию на 11.02.2019 г. / Н. А. Саванович // ЭТАЛОН. Правоприменительная практика / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

33. Саванович, Н. А. Дефиниция персональных данных в Законе Республики Беларусь «О защите персональных данных» и проблемы ее применения / Н. А. Саванович // Юридический научно-практический журнал «Юстиция Беларуси». – 2022. – № 6. – С. 41–44. – URL: https://cpd.by/storage/2024/03/Str_41-44-Savanovich_2.pdf (дата обращения 19.10.2024).

34. Саванович, Н. А. Обработка персональных данных в сфере государственного управления на примере Республики Беларусь и Российской Федерации / Н. А. Саванович, Е. В. Кудряшова // Право в современном белорусском обществе. – 2020. – Вып. 15. – С. 144–158.

35. Сачава, П. Д. Защита персональных данных в компании. Локальные документы / П. Д. Сачава // Бюллетень «Меркурый». – Минск, 2024. – № 1. – URL: https://www.cci.by/byulleten-merkuryy/publikatsii/v-interesakh-biznesa/zashchita-personalnykh-dannykh-v-kompanii-lokalnye-dokumenty/ (дата обращения 23.09.2024).

36. Синкевич, К. В. Дискуссия о месте персональных данных в системе объектов гражданских прав / К. В. Синкевич // Государство и право в XXI веке : материалы междунар. науч.-практ. конф., посвященной 95-летию юридического факультета Белорусского государственного университета, 26–27 ноября 2020 года, г. Минск / БГУ, Юридический фак. ; редкол.: Т. Н. Михалёва (гл. ред.) [и др.]. – Минск : БГУ, 2021. – С. 597–602.

37. Тенюта, Е. С. Юридическая ответственность за нарушение законодательства в сфере персональных данных (на примере законодательства Республики Беларусь) / Е. С. Тенюта // Приоритетные направления развития правовой системы общества : материалы IX Междунар. науч.-практ. конференции (Гомель, 12–13 мая 2022 года) : в 2 ч. Ч. 2 / редкол. : И. И. Эсмантович (гл. ред.) [и др.] ; Гомельский гос. ун-т им. Ф. Скорины. – Гомель : ГГУ им. Ф. Скорины, 2022. – С. 104–108.

38. Томашевский, К. Л. Все об обработке и защите персональных данных в трудовых и связанных с ними отношениях / К. Л. Томашевский // Отдел кадров: профессиональный ежемесячный журнал / учредитель ОДО «Профигруп». – 2023. – № 5. – С. 72–79.

39. Шакель, Н. В. Права субъектов персональных данных и юридические возможности их защиты в Республике Беларусь / Н. В. Шакель // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы : навукова-тэарэтычны

часопіс. – 2022. – Т. 12, № 3. – С. 14–19.

40. Шакель, Н. В. Проблемы определения статуса сооператоров в праве Республики Беларусь / Н. В. Шакель // Юстиция Беларуси : юридический научно-практический журнал / учредитель Министерство юстиции Республики Беларусь. – 2024. – № 3. – С. 23–26.

41. Шебанова, Н. А. Охрана персональных данных: опыт Европейского сообщества / Н. А. Шебанова // Журнал Суда по интеллектуальным правам – Москва, 2019. – № 25. – С. 5–14. – URL: https://ipcmagazine.ru/articles/1729209/ (дата обращения 19.10.2024).

42. The European Union data Privacy Directive / Julia M Fromholz - Berkeley Technology Law Journal, 2000. – Volume 15, issue 1. – P. 468–484.

43. Korff, D. The DPO Handbook Guidance for data protection officers in the public and quasi- public sectors on how to ensure compliance with the European Union General Data Protection Regulation (Regulation (EU) 2016/679) // D. Korff, M. Georges. – URL: https://ssrn.com/abstract=3428957 (Date of access: 19.10.2024).

44. Laputko, K. European Data Protection Law: Analysis of European (GDPR), Canadian, and US regulations / K. Laputko // Success Publication. – 2023. – 411 pages.

45. Laputko, K. CIPP/e 2024 prep: European Data Protection Law / K. Laputko. – 2024. – 398 pages.

46. McCarty-Snead, Steven S. Research Guide to European Data Protection Law / Steven S. McCarty-Snead, Anne Titus Hilby. – URL: https://doi.org/10.2139/ssrn.2355833 (Date of access: 19.10.2024).

47. Mondschein, C. F. The EU's General Data Protection Regulation (GDPR) in a Research Context / C. F. Mondschein, C. Monda. // Springer. Fundamentals of Clinical Data Science. – URL: https://doi.org/10.1007/978-3-319-99713-1_5. (Date of access: 19.10.2024).

48. Streinz, T. The Evolution of European Data Law / T. Streinz // Paul Craig and Gráinne de Búrca (eds). Oxford University Press. – Mode of access: http://dx.doi.org/10.2139/ssrn.3762971. (Date of access: 19.10.2024).

49. Handbook on European data protection law // European Union Agency for Fundamental Rights. – Luxembourg: Publications Office of the European Union, 2018. – 402 pages. – URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. (Date of access: 19.10.2024).

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

50. Конституция Республики Беларусь : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 февр. 2022 г. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2024. – 109 с.

51. Конвенция о защите физических лиц при автоматизированной обработке персональных данных : заключена в г. Страсбурге 28.01.1981 г.. – URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?doc umentId=0900001680078c46. (дата обращения: 20.10.2024).

52. О соответствии Конституции Республики Беларусь Закона Республики Беларусь «О защите персональных данных» : Решение Конституционного Суда

Респ. Беларусь, 29 апреля 2021 г., № Р-1261/2021 // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

53. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : в ред. от 1 июня 2022 г. № 175-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

54. Об архивном деле и делопроизводстве в Республике Беларусь: Закон Респ. Беларусь, 25 нояб. 2011 г., № 323-З : в ред. от 18 апр. 2022 г. № 163-З // ЭТАЛОН. Законодательство Респ. Беларусь / ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

55. Об информации, информатизации и защите информации : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред. от 10 окт. 2022 г. № 209-З// ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

56. О мерах по совершенствованию защиты персональных данных : Указ Президента Респ. Беларусь от 28 окт. 2021 г. № 422 // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

57. Кодекс Республики Беларусь об административных правонарушениях : 6 янв. 2021 г. № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г : в ред. Закона Респ. Беларусь от 17 февр. 2025 г. № 61-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

58. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях : 6 янв. 2021 г. № 92-З : принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г.: в ред. от 17 февр. 2025 г. № 61-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

59. Трудовой кодекс Республики Беларусь : 26 июля 1999 г. № 296-З : принят Палатой представителей 8 июня 1999 г. : одобрен Советом Респ. 30 июня 1999 г. : в ред. от 8 июля 2024 г. № 25-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

60. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. №: 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. от 8 апр. 2024 г. // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

61. Об обучении по вопросам защиты персональных данных : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 ноября 2021 г. № 194 // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

62. О технической и криптографической защите персональных данных : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 12 ноября 2021 г., № 195 // ЭТАЛОН : информ.-поисковая система (дата обращения: 17.05.2025).

63. General Data Protection Regulation : Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016 // EURLex. – Mode of access: https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Date of access: 20.10.2024).