

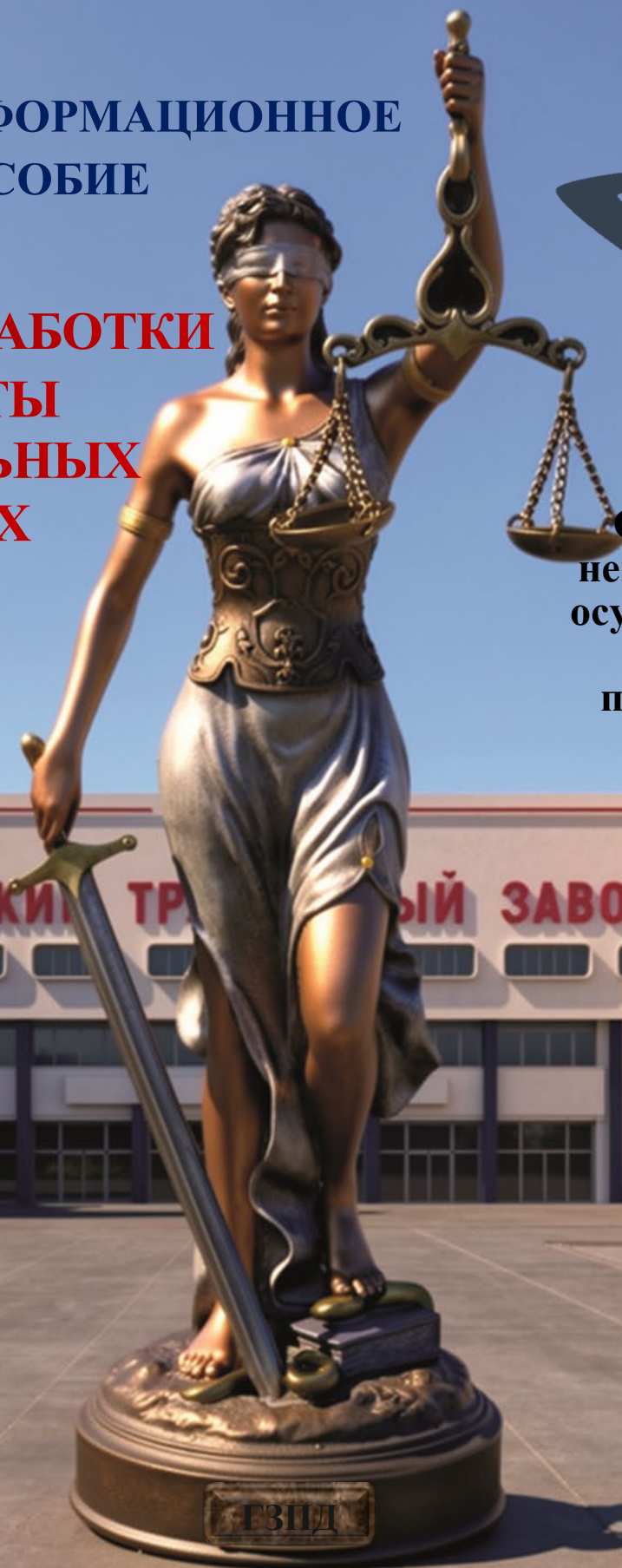
ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «МИНСКИЙ ТРАКТОРНЫЙ ЗАВОД»
ГРУППА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

УЧЕБНО-ИНФОРМАЦИОННОЕ ПОСОБИЕ

ОСНОВЫ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ



Для
работников
ОАО «МТЗ»,
непосредственно
осуществляющих
обработку
персональных
данных



ЗАКОННОСТЬ

БЕСПРИСТРАСТНОСТЬ

СПРАВЕДЛИВОСТЬ

Настоящее учебно-информационное пособие подготовлено группой защиты персональных данных в рамках реализации тематики обучения работников, непосредственно осуществляющих обработку персональных данных в ОАО «МТЗ».

При подготовке настоящего пособия использовались:

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Постатейный комментарий к Закону «О защите персональных данных», подготовленный Национальным центром защиты персональных данных Республики Беларусь в 2023 году;

учебно-методические материалы Национального центра защиты персональных данных Республики Беларусь;

иные акты законодательства Республики Беларусь и локальные правовые акты ОАО «МТЗ», в части касающейся сферы персональных данных.

Авторский коллектив:

Кудревич Денис Николаевич – главный специалист по внутреннему контролю за обработкой персональных данных ГЗПД;

Лукьянович Екатерина Алексеевна – ведущий специалист по внутреннему контролю за обработкой персональных ГЗПД.

СОДЕРЖАНИЕ

Тема 1.1. Законодательство и локальные правовые акты о персональных данных	2-6
Тема 1.2. Обязанности работника, осуществляющего обработку персональных данных	7-10
Тема 1.3. Общие требования к обработке персональных данных	11-15
Тема 1.4. Основания обработки персональных данных	15-27
Тема 1.5. Права субъектов персональных данных	27-30
Тема 1.6. Обработка персональных данных уполномоченными лицами, условия предоставления персональных данных третьим лицам, трансграничная передача персональных данных	30-33
Тема 1.7. Порядок работы с обращениями, заявлениями и жалобами субъектов персональных данных	34-35
Тема 1.8. Меры по обеспечению защиты персональных данных..	35-38
Тема 1.9. Виды ответственности за неправомерную обработку персональных данных	38-43

ТЕМА 1.1.

ЗАКОНОДАТЕЛЬСТВО И ЛОКАЛЬНЫЕ ПРАВОВЫЕ АКТЫ О ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Законодательство о персональных данных.

Конституция Республики Беларусь.

Статья 28. Каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

Государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании.

Законодательные акты общего характера, регулирующие персональные данные:

Закон Республики Беларусь от 7 мая 2021 г. № 99-3 «О защите персональных данных» (далее, если не определено иное, – Закон 99-3);

Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных».

Основные локальные правовые акты ОАО «МТЗ» в сфере персональных данных:

Политика обработки персональных данных ОАО «МТЗ»;

Политика ОАО «МТЗ» в отношении обработки персональных данных в процессе трудовой деятельности, утверждена приказом ОАО «МТЗ» от 8 января 2026 г. № 6;

Политика видеонаблюдения ОАО «МТЗ», утверждена приказом ОАО «МТЗ» от 30 марта 2026 г. № 229.

§ Основные термины, используемые в законодательстве и их определения.

Персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

**Любая информация,
относящаяся к
физическому лицу**



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.



Идентифицированное
физическое лицо



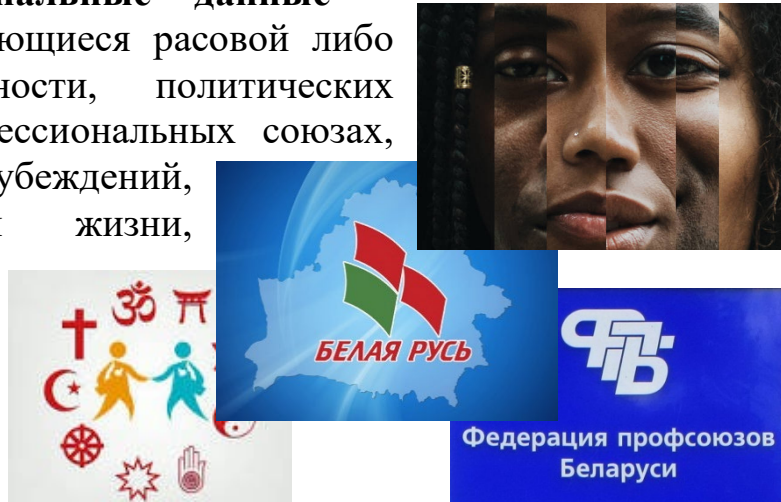
Физическое лицо, которое может
быть идентифицировано

Биометрические персональные данные – 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*).



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 (*анализы ДНК (дезоксирибонуклеиновой кислоты) или РНК (рибонуклеиновая кислота), сведения о группе крови, резус-факторе, а также другие данные, полученные из анализа биологических образцов, такие как уникальные паттерны в хромосомах или нуклеотидные последовательности, раскрывающие предрасположенности к заболеваниям*).

Специальные персональные данные – персональные данные, 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.



Общедоступные персональные данные – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов.

Персональные данные **распространенные самим субъектом персональных данных**, то есть персональные данные публикуемые самим человеком, в том числе Ф.И.О., фото, контакты, биография в интернете через мессенджеры.

Персональные данные **распространенные в соответствии с требованиями законодательных актов**, например при реализации норм законодательства о выборах, когда сведения о кандидатах публикуются избирательными комиссиями (Ф.И.О., фото, биография), в рамках реализации норм законодательства о борьбе с коррупцией, в области национальной безопасности и т.п.

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



Оператор



**BELARUS
TRACTORS**

Закон 99-3 выделяет двух субъектов, которые обрабатывают персональные данные, – оператор и уполномоченное лицо.

Субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Закон 99-3 не устанавливает требований к возрасту, гражданству, занимаемой должности физического лица и др. для признания его субъектом персональных данных. Как следствие, защите подлежат в равной степени персональные данные новорожденного и взрослого, граждан Беларуси, иностранных граждан, лиц без гражданства. При этом в отношении несовершеннолетних и недееспособных лиц устанавливается традиционный механизм реализации их прав через законных представителей.



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.



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

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

В отличие от оператора уполномоченное лицо не определяет ключевые параметры обработки персональных данных (цели и сроки обработки, объем обрабатываемых данных, круг лиц, которым предоставляются персональные данные), а действует от имени или в интересах оператора в соответствии с его поручениями, как правило, за вознаграждение.

Например.

ОАО «МТЗ» передало системное администрирование локальной сети на аутсорсинг ООО «Крамио-сервис».

Для ООО «Крамио-сервис» обработка персональных данных, содержащихся в локальной сети ОАО «МТЗ», не является целью, однако возложение обязанностей по администрированию локальной сети не может осуществляться без доступа к ним.

В данной ситуации ОАО «МТЗ» является оператором, а ООО «Крамио-сервис» – уполномоченным лицом, осуществляющим обработку персональных данных в интересах оператора.

Важной особенностью взаимоотношений между оператором и уполномоченным лицом является то, что после окончания обработки уполномоченное лицо должно 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. Как правило, эти процессы оформляются соответствующим актом или отчетом.

Обработка персональных данных – любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.



Следует отметить, что приведенные действия не носят исчерпывающий характер и является ориентиром для правоприменителя, о чем свидетельствует использованный законодателем оборот «включая».

Это очень важное обстоятельство, поскольку в законодательстве используются различные термины для описания действий с информацией: поиск, получение, запись, извлечение, накопление, пользование, доступ и др. Все эти действия являются разновидностями обработки. Даже простое хранение информации на жестком диске компьютера является обработкой таких данных. Учитывая незакрытый перечень действий с персональными данными, трансграничную обработку также следует рассматривать в качестве частного случая обработки.



ТЕМА 1.2.**ОБЯЗАННОСТИ РАБОТНИКА, ОСУЩЕСТВЛЯЮЩЕГО
ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ****§ Статус работника ОАО «МТЗ», осуществляющего обработку персональных данных.**

Приобретение работником статуса «Работник, осуществляющий обработку персональных данных» реализуется посредством издания организационно-распорядительного документа руководителя структурного подразделения – распоряжения.

Основанием для издания распоряжения является деятельность работника (в ходе которой обрабатываются персональные данные), внесенная в реестр обработки персональных данных структурного подразделения.

С приобретением работником статуса – «Работник, осуществляющий обработку персональных данных» (далее, если не определено иное, – РООПД) осуществляется:

уведомление работника об ответственности за нарушение установленного порядка обработки персональных данных;

ознакомление работника с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику ОАО «МТЗ» в отношении обработки персональных данных;

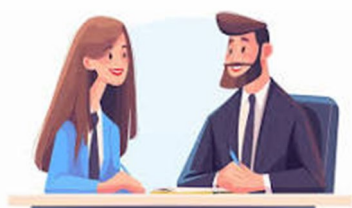
внесение в должностную (рабочую) инструкцию работника обязанностей и полномочий, касающихся обработки персональных данных;

предоставление доступа работнику к информационным системам (ресурсам) ОАО «МТЗ» (при необходимости);

планирование обучения работника по вопросам обработки и защиты персональных данных.

§ Обязанности работника, осуществляющего обработку персональных данных.**Основные обязанности РООПД, следующие из Закона 99-З:**

– разъяснять субъекту персональных данных его права, связанные с обработкой персональных данных.



Данная обязанность направлена на реализацию требования о прозрачном характере обработки персональных данных и предполагает доведение до сведения субъекта персональных данных его прав, связанных с обработкой

персональных данных. Из Закона «О защите персональных данных» следуют два случая, когда субъекту персональных данных необходимо разъяснить его права:

при получении согласия на обработку персональных данных;
в документах, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных;

– получать согласие субъекта персональных данных, за исключением случаев, предусмотренных Законом 99-З и иными законодательными актами.



Указанное положение также означает, что согласие не может выступать надлежащим правовым основанием в случае, когда имеются правовые основания обработки персональных данных без согласия;

– обеспечивать защиту персональных данных в процессе их обработки.



Обязанность обеспечивать защиту персональных данных – универсальное требование к любому работнику, осуществляющему обработку персональных данных, независимо от целей обработки. Основные меры, принимаемые для защиты персональных данных, содержатся в памятке для лиц, осуществляющих обработку персональных данных;

– предоставлять субъекту персональных данных информацию о его персональных данных, а также о предоставлении его персональных данных третьим лицам, за исключением случаев, предусмотренных законодательными актами.



Обязанность обеспечивает реализацию прав субъекта персональных данных, предусмотренных ст.ст. 11 и 12 Закона 99-З;

– 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.



Данная обязанность является проявлением общего требования о необходимости обеспечения достоверности обрабатываемых персональных данных (п. 7 ст. 4 Закона 99-3»). Кроме того, она направлена на реализацию положений ст. 11 Закона 99-3 о праве субъекта

персональных данных на изменение персональных данных.

Использование работником неактуальных данных может иметь негативные последствия для субъекта персональных данных (например, отказ в реализации прав либо ошибка в идентификации субъекта персональных данных).

Вместе с тем указанная обязанность не означает, что работник обязан во всех случаях отслеживать актуальность обрабатываемых персональных данных, например, запрашивая такие сведения у субъекта персональных данных или требуя их предоставления. Обязанность внесения работником изменений в персональные данные возникает, когда:

получено заявление субъекта персональных данных об изменении персональных данных;

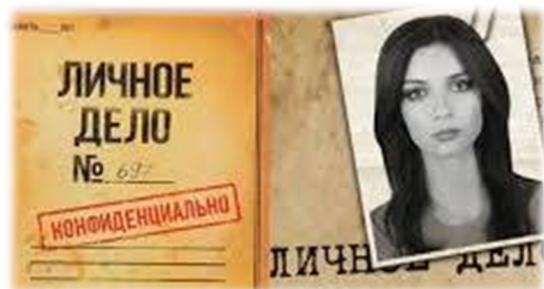
работнику становится известно, что персональные данные являются неполными, устаревшими или неточными (например, изменился адрес места жительства субъекта персональных данных, что выяснилось в ходе работы комиссии по улучшению жилищных условий);

– 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 законодательными актами.



Рассматриваемая обязанность призвана обеспечивать практическую реализацию права субъекта персональных данных, предусмотренного ст. 13 Закона 99-3.

Данная обязанность не подлежит исполнению в случае, когда работник обязан продолжить обработку персональных данных в силу требований законодательства (например, хранение личных дел работников);



– уведомлять ГЗПД о нарушениях систем защиты персональных данных незамедлительно после того, как стало известно о таких нарушениях.



Система защиты персональных данных – это совокупность правовых, организационных и технических мер, вытекающих из законодательства о персональных данных, предусмотренных локальными правовыми актами оператора, целью принятия которых является защита персональных данных, обрабатываемых оператором;

– осуществлять изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных субъекта персональных данных по требованию ГЗПД, если иной порядок внесения изменений в персональные данные, их блокирования или удаления не установлен законодательными актами.



Работник обязан по требованию ГЗПД осуществлять изменение, блокирование или удаление персональных данных в случае выявления:

*недостоверных персональных данных;
путем;*

– исполнять иные требования ГЗПД об устранении нарушений законодательства о персональных данных.

На основании подпункта 3.10 персональных данных, полученных незаконным пунктом 3 Положения о порядке осуществления внутреннего контроля за обработкой персональных данных

в ОАО «МТЗ» П 000-239-044-2024,

в целях обеспечения исполнения законодательства о персональных данных ГЗПД наделено полномочиями требовать от работников устранения нарушений законодательства о персональных данных;



– выполнять иные обязанности, предусмотренные локальными правовыми актами, в том числе Памяткой для лиц, осуществляющих обработку персональных данных.

ТЕМА 1.3. ОБЩИЕ ТРЕБОВАНИЯ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Сущность обработки персональных данных.



Сущность обработки персональных данных заключается в любых действиях или их совокупности (сбор, запись, систематизация, хранение, использование, передача, удаление и т.д.), совершаемых с личной информацией человека с помощью или без помощи технических средств, для достижения конкретных законных целей, с соблюдением принципов законности, справедливости, прозрачности и безопасности, как это определено законодательством. Это весь «жизненный цикл» данных, от момента их получения до уничтожения, с целью обеспечения прав субъектов и выполнения задач оператора.



§ Отдельные действия, совершаемые с персональными данными.

Блокирование персональных данных – прекращение доступа к персональным данным без их удаления.

Данная мера является альтернативой удалению, когда удаление по техническим причинам невозможно (например может привести к некорректной работе информационной системы). Так, согласно ч. 2 п. 2 ст. 13 Закона 99-3 при отсутствии технической возможности удаления персональных данных работник обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование, и уведомить об этом субъекта персональных данных в тот же срок.

В этой связи блокирование персональных данных при наличии возможности их удаления может привести к незаконному хранению таких данных и применению соответствующих мер ответственности.



Блокирование персональных данных может применяться и в иных случаях, например, когда есть жалоба на неправомерную обработку и нужно время для того, чтобы оценить ситуацию. В этой связи, чтобы исключить продолжение потенциально незаконной обработки, может применяться блокирование. По итогам рассмотрения жалобы обработка может быть продолжена либо данные должны быть удалены.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Например: введение идентификаторов (табельный номер, код подразделения, порядковый номер в штатном расписании).

Перед введением идентификаторов:

Наименование структурного подразделения	Фамилия и инициалы	Номер телефона	Сумма
УКадр	Иванов И.И.	8025-857-55-45	2500
ЮрУ	Петров П.П.	8044-545-85-52	3000

После введения идентификаторов:

Код	ID пользователя	Номер телефона	Сумма
913	User 001	802*-8*7-**-4*	2500
934	User 002	8044-*4*-8*-*2	3000

Предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц.

Как предоставление следует рассматривать, например, ситуации ответа на запрос персональных данных государственным органом в рамках предоставленных ему законодательством полномочий, направление характеристики при трудоустройстве, ознакомление с личным делом и др. При этом оценка действий как предоставления не зависит от правовой основы обработки персональных данных, например, необходимости получения согласия.



Специфика предоставления персональных данных лучше всего иллюстрируется при сопоставлении с термином «распространение» таких данных. Если при предоставлении с данными знакомится конкретное лицо (круг лиц), то при распространении доступ к персональным данным получает неограниченный круг лиц.

Для признания факта предоставления не имеет значения, ознакомилось ли фактически лицо (лица) с персональными данными или нет. На это указывает примененный в Законе оборот «действия, направленные на ознакомление». Так, если файл с персональными данными был направлен на электронную почту лица и у него была возможность его прочитать, то предоставление будет иметь место независимо от того, воспользуется ли оно такой возможностью.

Предоставление может иметь место как в бумажном виде (например, распечатка сведений о лице из информационного ресурса, и передача иному лицу), так и в электронном виде (например, направление информации с использованием мессенджеров, предоставление возможности ознакомиться с информацией на экране компьютера и др.).

Следует также отметить, что в зависимости от квалификации действий как предоставления или распространения может зависеть и юридическая оценка допущенных нарушений. Так, например, ст. 23.7 КоАП устанавливает повышенную ответственность, если имеет место распространение персональных данных.

Распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц.



Типичными примерами распространения персональных данных являются случаи размещения персональных данных в открытом доступе в сети Интернет. Как распространение персональных данных будут рассматриваться и ситуации «перепоста» информации, содержащей

персональные данные, проставление в ее отношении «лайков», которые влекут появление данного материала в ленте «друзей» пользователя. Вместе с тем, когда настройки приватности ограничивают доступ к информации такого пользователя определенным кругом лиц («друзей»), то речь будет идти не о распространении, а о предоставлении персональных данных.

Распространение может иметь место и без использования сети Интернет, например, при вывешивании списков неплательщиков на дверях подъезда, размещении информации на стендах в местах, открытых для массового посещения и др.



Распространение персональных данных несет с собой наибольший риск для прав субъекта, поскольку в связи с доступом к таким данным неопределенного круга лиц субъект теряет контроль над возможными способами их использования. В результате персональные данные в зависимости от их содержания могут быть использованы в различных, в том числе неправомерных целях. В этой связи за незаконное распространение персональных данных КоАП устанавливает повышенную ответственность по сравнению с иными видами обработки.

§ Требования к обработке персональных данных.

Общие требования к обработке персональных данных: законность; соразмерность и справедливость; наличие правового основания; ограничение цели; запрет избыточности; прозрачность; ограничение хранения; достоверность.

Прежде всего **законность** обработки предполагает выполнение оператором (уполномоченным лицом) всех обязанностей, которые на него возлагаются Законом «О защите персональных данных».

Требование законности обработки также означает, что оператор должен учитывать не только требования самого Закона, но и положения отраслевого законодательства, регулирующие конкретный вид обработки. Так, например, оператор не может ссылаться на наличие у него правовых оснований для обработки персональных данных в соответствии с Законом «О защите персональных данных» в рамках осуществления деятельности, для которой требуется получение лицензии, а у оператора она отсутствует.

Обработка персональных данных должна быть соразмерна заявленным целям и обеспечивать на всех этапах обработки справедливое соотношение интересов всех заинтересованных лиц. Фактически этим закрепляются два самостоятельных требования – **соразмерность и справедливость**.

Соразмерность и справедливость при обработке персональных данных означают, что данные должны собираться и использоваться строго в рамках заявленных целей, быть необходимыми для них (никаких излишеств) и не причинять необоснованного вреда субъекту, обеспечивая при этом честное соотношение его интересов с интересами оператора на всех этапах обработки, с прозрачным информированием о целях.

Наличие правового основания для обработки персональных данных указывает на то, что обработка осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом «О защите персональных данных» 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.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее заявленных законных целей (**ограничение цели**). Это означает, что данные можно собирать и использовать только для четко определенных и законных задач, и нельзя их использовать для несовместимых целей или собирать больше, чем необходимо.

Обрабатываемые персональные данные не должны быть **избыточными** по отношению к заявленным целям их обработки. Сущность недопущения избыточности при обработке персональных данных заключается в сборе и обработке только тех данных, которые строго

необходимы для достижения конкретной, заранее определенной и законной цели. Это означает, что оператор не должен собирать избыточные данные (лишние), которые не служат заявленной цели, и должен гарантировать, что данные не будут использоваться для целей, несовместимых с первоначальными.

Сущность **прозрачности** обработки персональных данных заключается в том, что субъектам персональных данных необходимо предоставлять полную, понятную и легкодоступную информацию о том, как их данные собираются, используются, хранятся, передаются и защищаются, чтобы человек мог понимать и контролировать процесс обработки своих данных.

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.

Законом «О защите персональных данных» предусматривается, что хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта не дольше, чем этого требуют заявленные цели обработки. Требование **ограничения хранения** направлено на снижение рисков, связанных с обработкой персональных данных. Ведь до тех пор, пока данные хранятся, есть риск их неправомерного использования.

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

конкретная календарная дата (например, до 1 января 2024 г.);

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

комбинация различных критериев (1 год с момента последнего использования постоянного пропуски).

ТЕМА 1.4.

ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Правовые основания обработки персональных данных.

Основаниями обработки персональных данных являются **законные причины**, такие как согласие субъекта данных, исполнение договора, выполнение юридических обязанностей оператора (например, по закону), защита жизни (здоровья) субъекта или третьих лиц, или, когда обработка необходима для реализации прав и свобод человека (например, журналистика, творчество).

Главный принцип – если нет законного основания, обработка персональных данных **ЗАПРЕЩЕНА**.

Основные правовые основания для обработки персональных данных:

– **согласие субъекта персональных данных** (часть первая пункта 3 статьи 4 Закона 99-3);

– оформление трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством (абзац восьмой статьи 6 Закона 99-3);

– договор, заключенный (заключаемый) с субъектом персональных данных, в целях совершения действий, установленных этим договором; (абзац пятнадцатый статьи 6 Закона 99-3);

– документ, адресованный оператору и подписанный субъектом персональных данных, в соответствии с содержанием такого документа (абзац шестнадцатый статьи 6 Закона 99-3);

– защита жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно (абзац восемнадцатый статьи 6 Закона 99-3);

– обработка ранее распространенных 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 99-3 и иными законодательными актами (абзац девятнадцатый статьи 6 Закона 99-3);

– выполнение обязанностей (полномочий), предусмотренных законодательными актами (абзац двадцатый статьи 6 Закона 99-3).

Согласие субъекта персональных данных представляет собой свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных.

Согласие субъекта персональных данных может быть получено в письменной форме, в виде электронного документа или в иной электронной форме.

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.

Вариант письменной формы:

СОГЛАСИЕ

на получение расчетных листков посредством систем
дистанционного банковского обслуживания

Я, _____

(фамилия, имя, отчество (если таковое имеется))

(дата рождения)

(идентификационный номер, при отсутствии такого номера – номер документа, удостоверяющего личность)

в соответствии со статьей 5 Закона Республики Беларусь от 7 мая 2021 г. № 99-3 «О защите персональных данных» даю согласие на обработку моих персональных данных для передачи мне ОАО «Сбергательный банк «Беларусбанк» от имени ОАО «МТЗ» моих расчетных листков посредством систем дистанционного банковского обслуживания.

Согласие выражаю на 3 года с момента дачи согласия.

Одновременно подтверждаю, что мне разъяснены права, связанные с обработкой моих персональных данных ОАО «Сбергательный банк «Беларусбанк», являющегося уполномоченным лицом, в части их сбора, систематизации, хранения, предоставления и удаления.

(число, месяц, год)

(подпись)

(инициалы и фамилия)

Вариант электронной формы:



До получения согласия субъекта персональных данных РООПД в письменной либо электронной форме, соответствующей форме выражения такого согласия, обязан предоставить субъекту персональных данных информацию, содержащую:

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;

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

срок, на который дается согласие субъекта персональных данных;

информацию об уполномоченных лицах в случае, если обработка персональных данных будет осуществляться такими лицами;

перечень действий с персональными данными, на совершение которых дается согласие субъекта персональных данных, общее описание используемых оператором способов обработки персональных данных;

иную информацию, необходимую для обеспечения прозрачности процесса обработки персональных данных.

До получения согласия субъекта персональных данных **РООПД обязан** простым и ясным языком разъяснить субъекту персональных данных: его права, связанные с обработкой персональных данных;
механизм реализации таких прав;
последствия дачи согласия субъекта персональных данных или отказа в даче такого согласия.

Эта информация должна быть предоставлена РООПД субъекту персональных данных в письменной либо электронной форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой ему информации.

Субъект персональных данных при даче своего согласия РООПД указывает свои фамилию, собственное имя, отчество (если таковое имеется), дату рождения, идентификационный номер, а в случае отсутствия такого номера – номер документа, удостоверяющего его личность, за исключением случая, когда цель обработки персональных данных не требует обработки указанной информации.

Наличие подобной «идентифицирующей» информации направлено на исключение (минимизацию) возможных спорных ситуаций относительно лица, которое в действительности выражает согласие на обработку персональных данных.

В соответствии с ч. 2 п. 6 ст. 5 Закона 99-З, если цели обработки персональных данных не требуют обработки всей совокупности указанной информации, она не подлежит обработке РООПД при получении согласия субъекта персональных данных.

В случае смерти субъекта персональных данных, объявления его умершим согласие на обработку его персональных данных дают один из наследников, близких родственников, усыновителей (удочерителей), усыновленных (удочеренных) либо супруг (супруга) субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

В случае признания субъекта персональных данных недееспособным или ограниченно дееспособным, а также до достижения им возраста шестнадцати лет, за исключением вступления в брак до достижения возраста шестнадцати лет, согласие на обработку его персональных данных дает один из его законных представителей. Законодательными актами может быть предусмотрен иной возраст несовершеннолетнего, до достижения которого согласие на обработку его персональных данных дает один из его законных представителей.

Например: дача согласия на обработку персональных данных несовершеннолетнего, при оказании услуг по проведению занятий

в клубном формировании, студии, кружке, любительском творческом коллективе ДК МТЗ.

Обработка персональных данных для заключения или исполнения договора **не требует отдельного согласия**, если она необходима для совершения действий по договору и не выходит за его рамки (например, сбор данных для договора купли-продажи, оказания услуг), но требуется для данных третьих лиц (не сторон по договору), если нет других оснований, а также если обработка выходит за пределы договора (например, для маркетинга) – тогда согласие необходимо. **Основные принципы: обрабатывать только нужные данные, для заявленных целей, соблюдать конфиденциальность и не передавать без оснований.**

При оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством.



Данное основание охватывает два случая обработки персональных данных:

- при оформлении трудовых (служебных) отношений;
- в процессе трудовой (служебной) деятельности.

Вместе с тем наниматель может осуществлять обработку персональных данных лиц как до оформления трудовых (служебных) отношений (при рассмотрении резюме соискателей на трудоустройство), так и после прекращения этих отношений. В таких ситуациях рассматриваемое основание не применяется.

Данное основание также не используется, когда обработка персональных данных работника осуществляется в период трудовой (служебной) деятельности, но не связана непосредственно с трудовой функцией работника (например, при организации добровольного медицинского страхования, если это не предусмотрено коллективным договором или коллективный договор в организации отсутствует).

Есть случаи, когда обработка персональных данных и круг обрабатываемых персональных данных работников прямо предусматриваются в нормативных правовых актах, так и ситуации, когда в акте законодательства данная информация напрямую не указана, но необходимость такой обработки прямо вытекает из предписаний этого акта, возлагающего на нанимателя определенные обязанности или предоставляющего ему определенные полномочия.

Например, при приеме на работу работник заполняет ряд документов, в том числе личный листок по учету кадров, форма которого установлена приложением 2 к Инструкции

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. В этой связи объем персональных данных предопределен содержанием установленной формы.

В иных случаях у нанимателя остается определенная степень усмотрения в части круга обрабатываемых сведений. Например, ст. 133 ТК на нанимателя возложена обязанность по организации учета рабочего времени. Учет прихода на работу и ухода с нее ведется в табелях использования рабочего времени, годовых табельных карточках и других документах с указанием фамилии, инициалов работника, календарных дней учетного периода, количества отработанного времени и других необходимых сведений. При этом формы документов для учета прихода на работу и ухода с нее, а также порядок их заполнения утверждаются нанимателем.

В ряде ситуаций ТК предусмотрены определенные гарантии для отдельных категорий работников (в связи с беременностью, наличием детей, инвалидностью, при служебных командировках, в связи с переездом на работу в другую местность и т.п.), которые наниматель обязан предоставить. Однако перечень документов, необходимых для предоставления гарантии, законодательством не установлен и определяется в каждой конкретной ситуации, исходя из существа гарантии.

Во всех указанных и подобных ситуациях правовым основанием для обработки персональных данных работников будет **являться абзац восьмой статьи 6 Закона 99-З.**

Рассматриваемое правовое основание применяется также при обработке персональных данных работников и членов их семей, которая необходима для выполнения нанимателем и профсоюзной организацией, созданной у нанимателя, обязанностей, предусмотренных коллективным договором. Что касается бывших работников и членов их семей, то обработка их персональных данных при выполнении обязанностей, предусмотренных коллективным договором, будет осуществляться на основании **абзаца двадцатого ст. 6 Закона 99-З и абзаца семнадцатого п.2 ст. 8 Закона 99-З (по специальным персональным данным).**

Вопрос о допустимости обработки на данном основании персональных данных третьих лиц, например, членов семьи работника, лиц, дающих рекомендации и т.п. заслуживает отдельного внимания. Если такая обработка напрямую предусмотрена законодательством (например, заполнение личного листка по учету кадров, личной карточки воинского учета по установленной форме) или обусловлена необходимостью выполнения возложенных на нанимателя законодательством обязанностей (например, при предоставлении социального отпуска при рождении ребенка, компенсаций в связи с переездом на работу в другую местность и т.п.), она осуществляется без согласия указанных лиц на основании

абзаца восьмого ст. 6 Закона 99-3. Иными словами, работник может предоставлять нанимателю сведения о родственниках без получения их согласия.

Если обработка персональных данных близких родственников (членов семьи) работника законодательством не предусмотрена, то требуется иное правовое основание (например, согласие), а также обеспечение соответствия обработки таких данных требованиям ст. 4 Закона 99-3 (прежде всего, соразмерность обработки и запрет избыточности).

При получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором.



Данное основание является одним из наиболее используемых в коммерческой деятельности операторов. Особое значение оно имеет при реализации товаров или услуг с помощью сети Интернет, когда у оператора отсутствует личный контакт с потенциальным клиентом. Тип договора законодателем не конкретизирован, однако с учетом основания, предусмотренного абзацем восьмым статьи 6 Закона 99-3, такое основание не применяется в отношении трудовых договоров.

Обработка персональных данных по этому правовому основанию будет соответствовать Закону 99-3, если:

оператор осуществляет обработку персональных данных только того физического лица, которое является (будет являться) стороной по договору, заключенному (заключаемому) с оператором. Если оператору необходимо обрабатывать персональные данные иных физических лиц (не являющихся стороной по договору, заключенному (заключаемому) с оператором), требуется согласие таких лиц или иное правовое основание, предусмотренное законодательными актами.

Например.

Статьей 23 Закона Республики Беларусь от 11 ноября 2021 г. № 129-3 «О туризме» определено, что оказание туристических услуг, услуг, связанных с организацией туристического путешествия, осуществляется в соответствии с этим Законом, Правилами оказания туристических услуг и иными актами законодательства. Правилами оказания туристических услуг, утвержденными постановлением Совета Министров Республики Беларусь от 11 августа 2022 г. № 523, установлена типовая форма договора, в соответствии с которой в приложении к договору необходимо указать также сведения о туристах, экскурсантах, которым оказываются туристические услуги. В этой связи в отношении лиц, которые не являются стороной договора, обработка осуществляется на основании абзаца двадцатого статьи 6 Закона 99-3;

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.

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.

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.

Так, распространенными примерами обработки персональных данных для целей заключения договора являются:

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.

Как обработку для целей исполнения договора следует расценивать ситуации:

информирования (напоминания) субъекта персональных данных о сроках исполнения договора;

осуществление гарантийного и постгарантийного обслуживания;

иные случаи, связанные с необходимостью надлежащей реализации прав и обязанностей сторон в рамках договора.

При обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа.



Данное 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.

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.

Примеры.

1. *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.*

2. *Человеку требуется экстренная операция, для проведения которой необходимы отдельные сведения из медицинских документов его родителей. Вместе с тем работники больницы по объективным причинам не могут связаться с ними и получить согласие на обработку их персональных данных.*

3. *В подъезде жилого дома в целях обеспечения сохранности имущества по решению более половины собственников квартир установлена камера 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 случаях, когда возможность получения согласия субъекта персональных данных на обработку персональных данных имеется (как в последнем примере), абзац восемнадцатый ст. 6 Закона 99-З не может быть применен.

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).

Например.

В соответствии с п. 1 ст. 44 Жилищного кодекса Республики Беларусь местные исполнительные и распорядительные органы ежегодно с 1 февраля до 1 мая уточняют данные, являющиеся основанием для сохранения права граждан состоять на учете нуждающихся в улучшении жилищных условий. Обработка персональных данных для этой цели местными исполнительными и распорядительными органами осуществляется без согласия субъекта персональных данных.

При этом в качестве обработки персональных данных, которая является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами, следует рассматривать как ситуации, когда полномочия прямо предусмотрены законодательными актами, так и случаи, когда законодательный акт содержит отсылочную норму к подзаконным актам об определении порядка реализации обязанностей (полномочий).

Например.

Законом Республики Беларусь от 5 ноября 1992 г. № 1914-XII "О воинской обязанности и воинской службе" предусмотрено ведение воинского учета призывников и военнообязанных в местных исполнительных и распорядительных органах, военных комиссариатах (обособленных подразделениях) и организациях в порядке, определяемом указанным Законом и Положением о воинском учете, утверждаемым Правительством Республики Беларусь.

Положением о воинском учете, утвержденным постановлением Совета Министров Республики Беларусь от 18 декабря 2003 г. № 1662, определено, что для ведения воинского учета руководители местных органов власти, ведущих воинский учет, должностные лица, ответственные за военно-учетную работу (работники по воинскому учету), обязаны вносить в книги учета и в карточки первичного учета изменения в части фамилии, собственного имени, отчества (если таковое имеется), семейного положения, состава семьи, уровня основного образования, места основной работы (учебы), занимаемой должности (специальности, профессии) по месту основной работы, состояния здоровья, места жительства и другие изменения и в месячный срок сообщать о произошедших изменениях в военный комиссариат района (города) (обособленное подразделение).

В случаях, когда Законом 99-3 и иными законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

Это основание является частным случаем предыдущего основания, когда в законодательном акте прямо предусматривается возможность обработки персональных данных без согласия гражданина.

Примерами таких законодательных актов являются:

Закон Республики Беларусь от 28 октября 2008 г. № 433-3 «Об основах административных процедур», п. 2 ст. 20 которого предусматривает, что сбор, обработка, хранение, использование персональных данных граждан при осуществлении

административных процедур осуществляются без их письменного согласия с соблюдением требований, определенных законодательными актами, по защите информации, распространение и (или) предоставление которой ограничено;

Закон «О регистре населения», ст. 24 которого предусматривается предоставление отдельным организациям персональных данных из регистра без согласия физического лица.

§ Обработка персональных данных по поручению оператора.

Обработка персональных данных по поручению оператора осуществляется уполномоченными лицами.

Такие лица, равно как и оператор, обязаны соблюдать требования к обработке персональных данных, предусмотренные Законом 99-3 и иными актами законодательства.

В первую очередь, речь идет об основных требованиях к обработке персональных данных, закрепленных в ст. 4 Закон 99-3 а, а также мерах по обеспечению защиты персональных данных, предусмотренных ст. 17 Закона 99-3.

Взаимоотношения оператора и уполномоченного лица могут опосредоваться:

актом законодательства.

Например.

В соответствии с постановлением Министерства образования Республики Беларусь от 16 апреля 2019 г. № 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»;

решением государственного органа, являющегося оператором.

В большинстве случаев уполномоченным лицом, осуществляющим обработку персональных данных на основании акта законодательства или решения государственного органа, являются подчиненные (входящие в состав) государственные органы (организации);

договором между оператором и уполномоченным лицом.

Это могут быть самостоятельный договор или отдельные положения в заключенном для достижения какой-либо цели договоре, так как обычно обработка персональных данных является сопутствующей деятельностью по отношению к предмету взаимоотношений оператора и уполномоченного лица.

Такой договор должен заключаться в том числе с уполномоченным лицом, расположенным на территории иностранного государства.

Пунктом 1 ст. 7 Закона 99-3 установлены требования к содержанию соответствующих документов. В них должны быть определены:

цели обработки персональных данных;

перечень действий, которые будут совершаться с персональными данными уполномоченным лицом;

обязанности по соблюдению конфиденциальности персональных данных; меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона 99-3.

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. При этом в силу требований абзаца седьмого п. 1 ст. 16 Закона 99-3 такая обязанность должна распространяться в том числе на случаи, когда уполномоченное лицо находится за пределами Республики Беларусь.

Уполномоченное лицо не обязано получать согласие субъекта персональных данных. Если для обработки персональных данных по поручению оператора необходимо получение согласия субъекта персональных данных, такое согласие получает оператор.

В случае, если оператор поручает обработку персональных данных уполномоченному лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Уполномоченное лицо несет ответственность перед оператором.

§ Обработка специальных персональных данных.

Примеры специальных данных

- Расовая и этническая принадлежность.

Расовая принадлежность — это классификация людей на группы на основе физических особенностей, таких как цвет кожи, черты лица, тип волос и другие генетически наследуемые признаки).

- Политические, религиозные или философские убеждения.
- Членство в профсоюзах.
- Данные о здоровье, половой жизни, сексуальной ориентации.
- Генетические и биометрические данные для уникальной идентификации.

Основные виды биометрических данных: изображение лица – распознавание лиц, используемое в системах безопасности и контроля доступа; отпечатки пальцев – один из самых распространенных методов, анализирующий папиллярный узор; радужная оболочка глаза – сканирование уникального рисунка радужки; рисунок вен ладони – сканирование сосудистого узора, что обеспечивает высокую точность; голос – поведенческий признак, используемый для аутентификации; походка – особенности движения человека.

Ключевые основания для обработки персональных данных, предусмотренные в ст.ст. 6 и 8 Закона 99-3 сопоставлены в таблице:

Основания обработки по ст. 6	Основания обработки по ст. 8
согласие	согласие
при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности	при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности
получение персональных данных на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором	
в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных	
при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа	
для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно	для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно
в отношении распространенных ранее персональных данных	если специальные персональные данные сделаны общедоступными персональными данными самим субъектом персональных данных
обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами	обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами

ТЕМА 1.5.

ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Перечень прав субъекта персональных данных.

Субъекты персональных данных в соответствии с Законом 99-3 наделены широким кругом прав, которые принадлежат им вне зависимости от правового основания обработки персональных данных (на основании согласия либо без его получения).

К основным правам субъектов персональных данных относятся:

- право на отзыв согласия;
- право на получение информации, касающейся обработки персональных данных;
- право требовать внесения изменений в персональные данные;
- 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.

§ Порядок реализации прав субъекта персональных данных.

Субъект персональных данных вправе в любое время без объяснения причин отозвать свое согласие посредством подачи оператору заявления в порядке, установленном статьей 14 настоящего Закона 99-3, либо в форме, посредством которой получено его согласие.

На регистрацию и рассмотрение заявлений субъектов персональных данных распространяется действие Закона Республики Беларусь от 18 июля 2011 г. № 300-3 «Об обращениях граждан и юридических лиц» с учетом отдельных особенностей, установленных Законом о персональных данных, которыми, в частности, являются форма подачи заявлений субъектов персональных данных, более короткие сроки подготовки ответа.

Оператор обязан **в пятнадцатидневный срок 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 настоящим 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.

Распространенным исключением являются и случаи, когда хранение персональных данных в пределах установленного срока вытекает из требований законодательства, в частности, постановления Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 «О перечне типовых документов». В этой связи, если хранение документов, содержащих персональные данные, обусловлено необходимостью соблюдения

требований, указанных нормативных правовых актов, прекращение обработки и удаление персональных данных не осуществляется. Правовым основанием для продолжения такой обработки будет выступать абзац двадцатый ст. 6 Закона 99-3.

Отзыв согласия субъекта персональных данных не имеет обратной силы, то есть предшествующая отзыву обработка персональных данных не является незаконной. В этой связи отзыв согласия имеет действие только на будущее время и не затрагивает правомерность обработки персональных данных в прошлом.

Закон 99-3 закрепляет право на получение субъектом персональных данных информации, касающейся обработки своих персональных данных. Наличие данного права является неотъемлемым условием эффективного контроля за соблюдением оператором законодательства о персональных данных и недопущением нарушения им прав и свобод субъекта персональных данных.

Перечень предоставляемой информации носит открытый характер и должен содержать:

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);

его персональные данные и источник их получения;

правовые основания и цели обработки персональных данных;

срок, на который дано согласие;

наименование и место нахождения уполномоченного лица, которое является государственным органом, юридическим лицом Республики Беларусь, иной организацией, если обработка персональных данных поручена такому лицу;

иную информацию, предусмотренную законодательством.

Для подготовки оператором ответа на заявление о получении информации установлен сокращенный в сравнении с иными сроками для реализации прав субъектов персональных данных срок – **5 дней с момента получения соответствующего заявления.**

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 статьей 14 настоящего Закона-99-3, с приложением соответствующих документов и (или) их заверенных в установленном порядке копий, подтверждающих необходимость внесения изменений в персональные данные.

Оператор обязан в пятнадцатидневный срок 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.

ТЕМА 1.6.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННЫМИ ЛИЦАМИ, УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ ЛИЦАМ, ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Организация работы с уполномоченными лицами.

Организация работы с уполномоченными лицами, обрабатывающих персональные данные работников оператора, включает:

определение целей и параметров обработки персональных данных (определение статуса уполномоченного лица).

Например действует от имени и в интересах оператора, но не определяет цели и основные параметры обработки персональных данных (кто, что, зачем и сколько), а лишь выполняет поручения оператора по фактической обработке (сбор, запись, хранение, уничтожение);

заключение письменных соглашений (договоров);

разработка внутренних документов (установление конкретных инструкций по обработке персональных данных);

обучение работников, осуществляющих обработку персональных данных, взаимодействию с уполномоченными лицами;

контроль уполномоченных лиц по соблюдению законодательства о персональных данных.

§ Условия предоставления персональных данных третьим лицам.

Предоставление персональных данных третьим лицам возможно в основном с согласия самого субъекта данных, которое должно быть свободным, информированным и однозначным, с указанием целей и получателя.

Исключения составляют случаи, предусмотренные законом (например, для правоохранительных органов или судебных исполнителей), а также передача данных внутри организации (холдинга) или привлеченным подрядчикам с соответствующими соглашениями

о конфиденциальности. Оператор обязан предоставлять информацию о передаче данных по запросу, а согласие должно быть получено на каждую цель отдельно.

В обращении, содержащем запрос на получение сведений (персональных данных), указывается:

основание предоставления сведений (указывается точная (до абзаца) норма, на которую делается ссылка, вид акта, дата принятия (издания) акта, регистрационный номер, название акта).

Например. Во исполнение пункта 11 Декрета Президента Республики Беларусь от 15 декабря 2014 г. № 5 «Об усилении требований к руководящим кадрам и работникам организаций» просим предоставить характеристику, на Иванова Ивана Ивановича 1977 года рождения, по форме, установленной приложением к постановлению Совета Министров Республики Беларусь от 14 октября 2021 г. № 585;

цель запроса (для принятия решения о приеме на работу, включения в резерв кадров, для проведения аттестации и т.д.);

перечень запрашиваемых данных (Ф.И.О., адрес регистрации (проживания), контактный номер телефона, иные).

§ Особенности трансграничной передачи персональных данных.

Трансграничная передача персональных данных определяется законодателем как передача персональных данных на территорию иностранного государства.

При трансграничной передаче персональные данные «выходят» из-под сферы действия белорусского законодательства и подпадают под юрисдикцию другого государства (законодательство «не следует» за данными).

Примеры трансграничной передачи персональных данных:

передача паспортных данных в посольство для оформления визы;

передача паспортных данных для оформления медицинских полисов, для бронирования номеров в отелях других стран;

отправка данных о сотрудниках в связи с осуществляемым родом деятельности;

пересылка документов с персональными данными иностранным партнерам по электронной почте;

использование мессенджеров (WhatsApp, Telegram), где данные могут передаваться.

Порядок трансграничной передачи персональных данных зависит от того, в какую страну передаются персональные данные:

в страну, на территории которой обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

в страну, на территории которой не обеспечивается надлежащий уровень защиты прав субъектов персональных данных.



Круг стран, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных, определен приказом директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 «О трансграничной передаче персональных данных».

К ним отнесены иностранные государства, являющиеся сторонами Конвенции о защите физических лиц при автоматизированной обработке персональных данных, а также иностранные государства, являющиеся членами Евразийского экономического союза. На сегодняшний день 55 стран являются сторонами Конвенции о защите физических лиц при автоматизированной обработке персональных данных. Это, прежде всего, страны Европейского союза, а также Российская Федерация, Армения, Грузия, Молдова, Украина, Мексика, Аргентина и др. В свою очередь, Казахстан, Кыргызстан являются членами Евразийского экономического союза. Российская Федерация и Армения подпадают под оба критерия.

Передача персональных данных на территорию таких государств осуществляется с соблюдением общих положений об обработке персональных данных (ст.ст. 4, 6 и 8 Закона 99-3) без ограничений и необходимости получения каких-либо дополнительных разрешений.

Вместе с тем факт осуществления трансграничной передачи персональных данных в такие государства отражается в соответствии с принципом прозрачности (п. 6 ст. 4 Закона 99-3) в документах, определяющих политику оператора в отношении обработки персональных данных. Если обработка осуществляется на основании согласия, то информация о трансграничной передаче данных дополнительно предоставляется субъекту до получения такого согласия.

В иные государства (в т.ч. США, Китай, Индию), не присоединившиеся к названной Конвенции и не являющиеся членами Евразийского экономического союза, по общему правилу, передача персональных данных запрещается, за исключением следующих ситуаций, когда:

дано согласие субъекта персональных данных при условии, что субъект персональных данных проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты;

персональные данные получены на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

персональные данные могут быть получены любым лицом посредством направления запроса в случаях и порядке, предусмотренных законодательством;

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;

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.

Рисками, возникающими в связи с отсутствием надлежащего уровня защиты персональных данных в иностранных государствах, являются:

отсутствие специального законодательства, регулирующего обработку персональных данных, в том числе требований по соблюдению таких норм;

отсутствие независимого уполномоченного государственного органа по защите прав субъектов персональных данных;

ограниченный круг прав субъектов персональных данных;

использование ненадлежащих способов получения персональных данных;

незаконная обработка персональных данных, в результате чего персональные данные могут стать доступными неограниченному кругу лиц.

ТЕМА 1.7.**ПОРЯДОК РАБОТЫ С ОБРАЩЕНИЯМИ И ЗАЯВЛЕНИЯМИ
СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ****§ Обращение субъекта персональных данных.**

Обращение субъекта персональных данных – это официальное заявление гражданина (работника) к оператору (РООПД) с целью реализации своих прав, таких как отзыв согласия, требование внесения изменений (уточнение, удаление) данных, получение информации об обработке или обжалование действий оператора (РООПД), которое подается в письменной форме или в виде электронного документа.

Адресатом заявления Закон 99-3 определяет оператора.

Оператор рассматривает адресованные ему заявления субъектов персональных данных путем назначения ответственным за рассмотрение заявления субъекта персональных данных, того РООПД в компетенцию которого входит предмет заявления. При этом независимо от того, кто из РООПД готовит проект ответа, сам ответ направляется тем РООПД (оператором), кому было адресовано заявление.

§ Содержание заявления субъекта персональных данных.

Предусматривается, что 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 (для заявления в письменной форме) или электронную цифровую подпись (для заявления в виде электронного документа) субъекта персональных данных.

Ответ на заявление направляется субъекту персональных данных в форме, соответствующей форме подачи заявления, если в самом заявлении не указано иное.

§ Сроки подготовки ответов.

Сроки ответа на заявления субъектов персональных данных зависят от типа запроса, но в целом они составляют 5 рабочих дней для получения информации об обработке и 15 календарных дней для внесения изменений или прекращения обработки, согласно Закону № 99-З, при этом оператор должен уведомить о причинах отказа в установленный срок.

5 рабочих дней – для предоставления информации субъекту персональных данных об обработке персональных данных (ст. 11 Закона 99-З).

15 дней (календарных, если не указано иное) для:

внесения изменений в персональные данные и уведомления об этом;

предоставления информации о передаче персональных данных третьим лицам (один раз в год бесплатно);

для прекращения обработки персональных данных (их удаления, блокирования) и уведомления об этом.

Важные нюансы:

отказ – если оператор не может выполнить запрос, он обязан уведомить об этом субъекта в установленный срок, указав причины;

законодательство – в некоторых случаях законодательством или договором могут быть установлены более короткие сроки.

ТЕМА 1.8.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Виды мер по обеспечению защиты персональных данных.

Оператор (уполномоченное лицо) обязан принимать 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.

Как меры по обеспечению защиты персональных данных следует рассматривать не только сугубо технические меры защиты персональных данных (например, применение криптографических мер), но и мероприятия, которые способствуют надлежащей реализации мер, направленных на недопущение неправомерных действий в отношении персональных данных, а также исполнению иных обязанностей оператора по обеспечению требований Закона 99-З (например, осуществление внутреннего контроля за обработкой персональных данных, ведение реестра обработок, внесение изменений в должностные инструкции).

При выборе перечня мер, подлежащих принятию, следует учитывать в первую очередь потенциальные риски, связанные с обработкой персональных данных, которые определяются оператором самостоятельно с учетом своей деятельности. Это отражает содержание риск-ориентированного подхода.

В целом обеспечение защиты персональных данных и принятие в этой связи необходимых мер является динамическим, а не статическим процессом. Это означает, что принятые единожды меры подлежат постоянному пересмотру и совершенствованию с целью повышения их эффективности, что обусловлено появлением как новых технологий, так и новых рисков, и угроз.

§ Обязательные меры обеспечения защиты персональных данных.

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.

§ Памятка для лиц, осуществляющих обработку персональных данных (минимально принимаемые РООПД меры по защите персональных данных).

При выполнении должностных обязанностей, связанных с обработкой персональных данных **ЗАПРЕЩЕНО**:

производить несанкционированные сбор, обработку, предоставление, распространение, удаление и изменение персональных данных;



предоставлять персональные данные устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, либо реализации законодательства;



оставлять без присмотра документы и другие носители информации, содержащие персональные данные разрешать их фотографирование или копирование;

хранить документы и другие носители, содержащие персональные данные, в условиях, допускающих доступ к ним посторонних лиц;

передавать ключи от мест хранения персональных данных посторонним лицам;

передавать личные атрибуты доступа (логин, пароль) к информационным системам (базам данных), в которых обрабатываются персональные данные;



использовать чужие атрибуты доступа (логин, пароль) для обработки персональных данных;



выносить документы и другие носители информации, содержащие персональные данные, за пределы ОАО «МТЗ», если это не требуется для выполнения служебных обязанностей;

использовать в качестве черновиков документы, содержащие персональные данные;

производить уничтожение документов способом, позволяющим восстановить информацию, содержащую персональные данные;

обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме должностных лиц, уполномоченных на обсуждение данных вопросов.



ТЕМА 1.9.

ВИДЫ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНУЮ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ Комментарий статьи 19 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»

В соответствии с п. 1 ст. 19 Закона 99-З лица, виновные в нарушении данного Закона, несут ответственность, предусмотренную законодательными актами.

Так, за нарушение законодательства о персональных данных в Республике Беларусь предусмотрена:

дисциплинарная ответственность (п. 10 ч. 1 ст. 47 ТК);

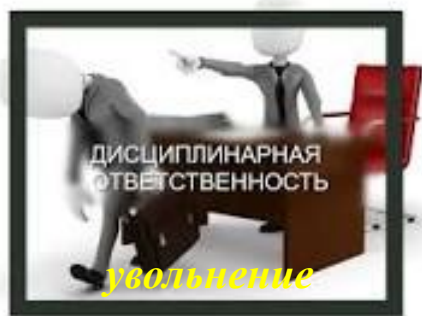
административная ответственность (ст. 23.7 КоАП);

уголовная ответственность (ст.ст. 203¹, 203² УК);

гражданско-правовая ответственность (п. 2 ст. 19 Закона предусматривает возмещение морального вреда, имущественного вреда и понесенных субъектом персональных данных убытков).

Дисциплинарная ответственность.

В соответствии со ст. 197 ТК дисциплинарная ответственность наступает за противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей (совершение дисциплинарного проступка).



Основные обязанности работника закреплены в ст. 53 ТК, в правилах внутреннего трудового распорядка, коллективных договорах, должностных (рабочих) инструкциях и иных локальных правовых актах нанимателя (соглашениях, положениях, инструкциях по охране труда и технике безопасности и т.д.), а также дисциплинарных уставах.

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.

Законом Республики Беларусь от 28 мая 2021 г. № 114-З «Об изменении законов по вопросам трудовых отношений» в ТК введено новое основание прекращения трудовых отношений – нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных (п. 10 ч. 1 ст. 47 ТК). Увольнение как мера дисциплинарного взыскания по данному основанию возможна, если работник исполнил свою трудовую обязанность ненадлежащим образом либо она не исполнена вовсе. При этом совершенное действие или бездействие должно быть виновным, а поведение работника должно быть противоправным.

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.

Статьей 23.7 КоАП предусмотрена административная ответственность за нарушение законодательства о защите персональных данных.

Частью 1 ст. 23.7 КоАП ответственность установлена за умышленные незаконные сбор, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных.

В ч. 2 ст. 23.7 КоАП предусмотрен квалифицированный состав правонарушения: деяния, предусмотренные ч. 1 рассматриваемой статьи, совершенные лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью.

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.

Например.

В качестве подобного нарушения можно рассматривать, например, распространение сведений о заработной плате по просьбе знакомых и др.



***до 200 базовых
величин***

Содержанное по ч. 2 ст. 23.7 КоАП влечет наложение штрафа в размере от четырех до ста базовых величин.

В ч. 3 ст. 23.7 КоАП установлена ответственность за умышленное незаконное распространение персональных данных физических лиц. Законодатель предусмотрел самостоятельное деяние, устанавливающее ответственность за распространение персональных данных, то есть действия, направленные на ознакомление с персональными данными неопределенного круга лиц.

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).

Например.

Распространением является размещение чужих персональных данных без согласия субъекта персональных данных в открытом аккаунте в социальных сетях, оглашение персональных данных в публичном выступлении, публикация на сайте организации, размещение на информационном стенде, размещение на дверях подъезда и др.

Указанное деяние влечет наложение штрафа в размере до двухсот базовых величин.

Уголовная ответственность.

На сегодняшний день в УК существуют две статьи, касающиеся защиты персональных данных и информации о частной жизни. Так, в ст. 203¹ УК устанавливается ответственность за незаконные действия в отношении информации о частной жизни и персональных данных, а в ст. 203² УК – ответственность за несоблюдение мер обеспечения защиты персональных данных.

ч. 1 ст. 203¹ УК сформулирована как 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.

Следует отметить, что рассматриваемая статья УК применяется независимо от того, распространяется на обработку персональных данных действие Закона или нет, поскольку в данном случае речь может идти об обработке персональных данных физическими лицами в процессе в том числе личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью.

Общественно опасное деяние представлено в виде двух альтернативных действий: незаконный сбор или незаконное предоставление. Каким образом производится сбор и предоставление

соответствующей информации другим организациям, гражданам или общественности, не имеет значения.

Обязательным элементом объективной стороны рассматриваемого состава является отсутствие согласия субъекта персональных данных или иных правовых оснований для обработки персональных данных.

В ч. 1 ст. 203¹ УК 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-летнего возраста.



Обращаем внимание, что только деяние, предусмотренное ч. 1 ст. 203¹ УК влечет уголовную ответственность по требованию потерпевшего. Степень вреда и целесообразность уголовной ответственности в данном случае определяются потерпевшей стороной, и именно требование потерпевшего инициирует возбуждение уголовного дела.

В ч. 2 ст. 203¹ УК установлен квалифицированный состав преступления, касающийся распространения информации о частной жизни и (или) персональных данных при аналогичных последствиях.

Формы распространения могут быть различными: это может быть распространение информации в сети Интернет или в социальных сетях, средствах массовой информации, посредством доведения информации до широкого круга лиц путем расклейки объявлений (сообщений) на информационных стендах, дверях подъездов, местах массового скопления людей и т.п. Как распространение информации следует рассматривать также устное озвучивание информации неопределенному кругу людей (например, в коллективе) и др. Часть 3 ст. 203¹ 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. Таким образом, данной нормой установлены особые

требования к потерпевшему, и наступление уголовной ответственности зависит от установления его особого статуса.

В ст. 203² УК установлена ответственность за несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение и причинение тяжких последствий.

Субъект преступного посягательства специальный – лицо, осуществляющее обработку персональных данных.

Под лицом, осуществляющим обработку персональных данных, в качестве субъекта преступления следует понимать работника оператора (уполномоченного лица) и иных лиц, не являющихся работниками оператора (уполномоченного лица), на которых возложена обязанность непосредственно осуществлять 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.

Гражданско-правовая ответственность.

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. Этот институт пригоден для принуждения виновных лиц к полному или частичному возмещению имущественного вреда, нанесенного гражданину в результате неприятия мер, предусмотренных Законом, а также нарушения его прав незаконными действиями оператора или уполномоченного лица.

Так, 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 ему противоправными действиями (бездействием) при исполнении им служебных, должностных или иных трудовых обязанностей вреда, он может быть взыскан в судебном порядке.

Удержание причиненного ущерба из заработной платы работника допускается в соответствии с требованиями ст. 107 ТК.

В п. 2 ст. 19 Закона особо отмечается, 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, поскольку право гражданина на компенсацию (материальное возмещение) морального вреда гарантировано Конституцией (ст. 60) и является способом защиты гражданских прав, неприкосновенности и достоинства личности в установленном законом порядке.

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.

Например.

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.

Содержание морального вреда заключается в том, что действия причинителя вреда обязательно должны найти отражение в сознании потерпевшего, вызвать определенную психическую реакцию, как правило, негативную.

Таким образом, включение законодателем в ст. 19 Закона нормы о возмещении морального вреда направлено на повышение уровня защиты нематериальных благ субъекта персональных данных.