ЭЛЕКТРОННОЕ ПОСОБИЕ
ERZ.BY

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ:

работаем правильно

ООО «Информационное правовое агентство Гревцова»

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ:
работаем правильно

Минск
«Информационное правовое агентство Гревцова»
2022

Авторы:
А. Поторская, К. Шафеев, Т. Соколовская, О. Опимах, В. Самосейко, М. Городник
Под общей редакцией Я. Ероховец

Защита персональных данных: работаем правильно / А. Поторская [и др.] ; под общ. ред. Я. Ероховец. — Минск : Информационное правовое агентство Гревцова, 2022. — 112 с.

Настоящее пособие поможет вам в организации работы по обеспечению защиты персональных данных в вашей организации. На страницах пособия вы найдете ряд актуальных аналитических материалов, ответы на самые важные вопросы, а также полезные формы документов и интерактивные чек-листы.

СОДЕРЖАНИЕ*

* *Чтобы **перейти в необходимый раздел, кликните** на позицию в содержании.*

ПЕРЕЧЕНЬ ФОРМ ДОКУМЕНТОВ*

1. Примерный образец приказа о правовом режиме защиты персональных данных в организации здравоохранения
2. Примерный образец Политики оператора в отношении обработки персональных данных
3. Примерный образец Положения о правовом режиме защиты персональных данных в организации здравоохранения
4. Примерный образец выдержки из формы реестра ПД
5. Выдержка из Положения о работе с персональными данными (в части вопроса ПД работников)
6. Примерный анализ личного дела работника
7. Примерный образец Положения об уничтожении (удалении) персональных данных
8. Примерный образец приказа о создании комиссии по уничтожению персональных данных
9. Примерный образец акта об уничтожении материальных носителей персональных данных
10. Примерный образец журнала регистрации удаления персональных данных
11. Примерный образец докладной записки о нарушении работником режима защиты персональных данных
12. Примерный образец оформления требования нанимателя о представлении письменных объяснений
13. Примерный образец акта о результатах проверки по факту нарушения работником порядка обработки персональных данных
14. Примерный образец приказа об увольнении работника по п. 10 ч. 1 ст. 47 ТК

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ОБЗОР НОВОВВЕДЕНИЙ С 15 НОЯБРЯ 2021 Г.

15 ноября 2021 г. вступил в силу Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон). Законом введен ряд новых обязанностей для операторов персональных данных. Требования Закона уже должны быть выполнены в организациях здравоохранения. Расскажем, на что необходимо обратить внимание руководителю.

Алёна ПОТОРСКАЯ, *ведущий юрист REVERA*

Вопросы защиты персональных данных вышли на новый уровень развития с принятием Закона. Почему же они актуальны для руководителя? Ответ прост:

- с 1 марта 2021 г. ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях (далее — КоАП) введена административная ответственность за нарушение законодательства о защите персональных данных, а именно за незаконные сбор, обработку, хранение или предоставление персональных данных, нарушение прав субъекта данных, распространение персональных данных, несоблюдение мер обеспечения защиты персональных данных;
- 19 июня 2021 г. Уголовным кодексом Республики Беларусь (далее — УК) предусмотрена уголовная ответственность за нарушение законодательства о персональных данных (ст. 203^1 и 203^2 УК).

Таким образом, руководителю крайне важно соблюдать основные положения Закона, поскольку в случае их нарушения могут наступить неблагоприятные последствия.

КТО ЖЕ ТАКОЙ ОПЕРАТОР?

Согласно абз. 8 ч. 1 ст. 1 Закона о персональных данных **оператор** — это государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в т.ч. индивидуальный предприниматель, самостоятельно или совместно с указанными лицами организующие и (или) осуществляющие обработку персональных данных.

К определениям, которые косвенно затрагивают понятие оператора, относятся «персональные данные» и «субъект персональных данных».

Согласно абз. 9 ч. 1 ст. 1 Закона персональными данными является любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Субъект персональных данных — это физическое лицо, в отношении которого осуществляется обработка персональных данных (абз. 13 ч. 1 ст. 1 Закона).

Из анализа приведенных понятий следует, что **любая организация является оператором персональных данных.**

Организации здравоохранения в первую очередь являются операторами в отношении данных о пациентах, клиентах, своих работниках и др.

Таким образом, руководителям организаций здравоохранения необходимо изучить основные стандарты, установленные Законом, чтобы привести свою деятельность в соответствие с данными требованиями.

МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для приведения внутренних процессов организации в соответствие с Законом необходимо знать основные меры защиты персональных данных, закрепленные в ст. 17 (см. *схему 1*).

Схема 1

Обязанности организации в части защиты персональных данных

Справочно: *порядок осуществления технической и криптографической защиты персональных данных установлен Оперативно-аналитическим центром при Президенте Республики Беларусь.*

Зачастую в организациях работу по вопросам защиты коммерческой тайны или персональных данных возлагают на юристов. Однако руководителю необходимо помнить, что у юристов, как правило, отсутствуют знания ***о технической стороне защиты информации***. Поэтому в организации целесообразно создать небольшую группу из специалистов разных профилей. Это могут быть, например, юрист, специалист по кадрам, системный администратор и др.

ОПЕРАТОР И УПОЛНОМОЧЕННОЕ ЛИЦО: В ЧЕМ РАЗНИЦА?

Ранее законодательство Республики Беларусь не разграничивало роли субъектов в процессе обработки персональных данных. Со вступлением в силу Закона введены понятия, аналогичные понятиям Общего регламента защиты персональных данных, принятого в Евросоюзе (General Data Protection Regulation, далее — GDPR).

Так, Законом введены понятия «оператор» (аналог «контролера» в GDPR) и «уполномоченное лицо» (аналог «процессора» в GDPR).

Уполномоченное лицо — это 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 (абз. 16 ч. 1 ст. 1 Закона).

Оператора от уполномоченного лица отличить несложно. Если организация **сама принимает решение об обработке персональных данных**, она является **оператором**. Если же организация обрабатывает персональные данные **по указанию другого лица** (в т.ч. на основе договора), она является уполномоченным лицом.

Справочно: *в небольшой организации учет кадров, воинский и бухгалтерский учет может вести специализированная организация или индивидуальный предприниматель. В этом случае такая специализированная организация или ИП будут являться уполномоченными лицами, а организация, поручившая им обработку персональных данных, — оператором.*

Законом закреплены правила, указывающие на то, как должны быть урегулированы отношения между оператором и уполномоченным лицом.

Так, договор должен содержать:

- перечень действий, совершаемых с персональными данными;
- обязательство по соблюдению конфиденциальности персональных данных;

- цели обработки персональных данных;
- меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона (п. 1 ст. 7 Закона).

Если у организации уже имеется такой договор, он должен быть приведен в соответствие с требованиями Закона (дополнительно урегулированы пункты, перечисленные выше).

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

В п. 3 ст. 4 Закона закреплено, что обработка персональных данных осуществляется с согласия субъекта персональных данных.

Статьей 6 Закона предусмотрены случаи, при которых обработка персональных данных может осуществляться без согласия субъекта персональных данных. В частности, это получение персональных данных:

- на основании договора, заключенного с субъектом персональных данных, в целях совершения действий, установленных этим договором;
- при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством, и в других случаях.

К согласию, которое должно быть получено от субъекта персональных данных, Законом предъявляются определенные требования. Так, согласие должно быть **свободным, однозначным и информированным**.

Форма согласия установлена п. 2 ст. 5 Закона. Оно может быть получено в письменной форме, в форме электронного документа или в иной электронной форме.

Ранее законодательством Республики Беларусь предусматривалась возможность получения исключительно письменного согласия.

Перед получением согласия Закон **обязывает** оператора сообщить субъекту персональных данных некоторую информацию (предусмотренную ч. 1 п. 5 ст. 5 Закона), а также простым и ясным языком разъяснить субъекту персональных данных его права, механизм их реализации, последствия дачи согласия и отказа от него.

Если все вышеуказанные условия не будут соблюдены, то согласие на обработку персональных данных будет считаться недействительным.

СОБЛЮДЕНИЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Закон предоставляет субъекту персональных данных право определенным образом распоряжаться своими персональными данными. В частности, субъекты персональных данных получают права:

- на отзыв согласия (ст. 10 Закона);
- на получение информации об обработке данных (ст. 11 Закона);
- на изменение персональных данных (ст. 11 Закона);
- на получение информации о предоставлении данных третьим лицам (ст. 12 Закона);
- требовать удаления данных или прекращения их обработки (ст. 13 Закона).

При получении заявления субъекта персональных данных оператор обязан **в течение 15 дней (5 дней — в отношении права на получение информации об обработке персональных данных)** выполнить одно из действий (*схема 2*).

Схема 2

Действия оператора при рассмотрении заявления субъекта персональных данных

Субъект персональных данных в случае отказа от предоставления информации или выполнения действий **должен быть уведомлен** о причинах такого отказа.

КОНТРОЛЬ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ранее законодательство Республики Беларусь не регулировало вопросы передачи персональных данных за пределы государства. Закон же закрепляет правило, согласно которому передача данных за пределы Республики Беларусь в страны, где не обеспечен надлежащий уровень защиты данных, запрещается (п. 1 ст. 9 Закона).

Пункт 1 ст. 9 Закона предусматривает перечень условий, при которых возможна передача персональных данных. К таким условиям отнесены:

- наличие согласия субъекта персональных данных, который проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты;
- получение персональных данных на основании договора, заключенного 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;
- 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;
- получено соответствующее разрешение уполномоченного органа по защите прав субъектов персональных данных.

СПЕЦИФИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИЯХ ЗДРАВООХРАНЕНИЯ

Мы уже рассмотрели общие положения Закона о защите персональных данных. А теперь обратим внимание на отдельные вопросы защиты персональных данных, связанные со спецификой деятельности организаций здравоохранения.

Кирилл ШАФЕЕВ, *ассоциированный партнер, руководитель направления «Приватность и защита персональных данных» юридической компании ЮКОН*

В силу принятия в Республике Беларусь полноценного законодательства в сфере защиты персональных данных, а также появления соответствующего контролирующего органа — Национального центра по защите персональных данных — каждая организация, осуществляющая обработку персональных данных граждан Республики Беларусь, должна привести свою деятельность в целом и любые внутренние процессы в частности в соответствие с новым законодательством. Не исключение и организации здравоохранения.

Организации здравоохранения — это именно те организации, которые обрабатывают наиболее чувствительные типы персональных данных: информацию о здоровье и иные специальные персональные данные пациентов.

Соответственно, все организации здравоохранения обязаны:

- обеспечивать соблюдение режима врачебной тайны в соответствии с Законом Республики Беларусь от 18.06.1993 № 2435-XII «О здравоохранении» (в ред. от 11.12.2020);
- соблюдать правила обработки информации ограниченного распространения согласно Закону Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» (в ред. от 24.05.2021);
- выполнять требования Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон).

ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ ВСЕХ

Любой случай обработки персональных данных должен соответствовать правовым принципам, установленным ст. 4 Закона.

Так, обработка персональных данных должна быть:

- **справедливой** на всех этапах по отношению к субъекту персональных данных *(принцип справедливости)*;
- **основана на согласии субъекта** или обрабатываться при наличии оснований, позволяющих не брать согласие у субъекта *(принцип законности)*;
- **произведена** исключительно для достижения заранее заявленных и законных целей *(принцип ограничения целью)*.

Помимо указанных принципов необходимо соблюдать и принципы, представленные на *схеме* на следующей странице.

Перечисленные принципы являются обязательными для любых организаций независимо от сферы деятельности.

Тем не менее вид деятельности все же влияет на имплементацию принципов защиты персональных данных.

Схема

Правовые принципы работы с персональными данными

ЧТО УЧЕСТЬ ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Если взять принцип законности, то его реализация организациями здравоохранения имеет определенную специфику.

МНЕНИЕ АВТОРА

При обработке медицинской информации организации, не ведущие деятельность в сфере здравоохранения, вероятнее всего, будут вынуждены полагаться ***на согласие субъектов персональных данных*** *со всеми вытекающими юридическими сложностями (например, правом на отзыв согласия и необходимостью последующего удаления или блокирования персональных данных).*

Организации здравоохранения могут воспользоваться более органичными правовыми основаниями обработки медицинской информации, установ-

ленными п. 2 ст. 8 Закона: для организации оказания медицинской помощи или же для защиты жизни, здоровья и иных жизненно важных интересов субъектов персональных данных.

*Стоит обратить внимание и на вопросы секторального регулирования, которое предусматривает взятие согласия на обработку персональных данных пациента **даже** в случаях, когда такая обработка осуществляется **организацией здравоохранения**.*

Особый порядок обеспечения принципа законности возникает при применении:

- Положения об особенностях оказания медицинской помощи с применением телемедицинских технологий (утв. постановлением Министерства здравоохранения Республики Беларусь от 28.05.2021 № 65, далее — Положение № 65);
- постановления Министерства здравоохранения Республики Беларусь от 07.06.2021 № 74 (касается внесения персональных данных пациента в централизованную систему здравоохранения).

В частности, Положение № 65 требует вносить информацию о формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента **в порядок и условия оказания медицинской помощи с применением телемедицинских технологий**.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ДАННЫХ

Отдельно белорусский законодатель касается вопросов трансграничной передачи персональных данных.

***Справочно:** если организация направляет персональные данные за пределы Республики Беларуси, она обязана обеспечить надлежащий уровень их защиты в рамках этой процедуры.*

В деятельности организаций здравоохранения ситуация трансграничной передачи возникает в случае использования **информационных систем**, серверы которых находятся вне Республики Беларусь, для хранения персональных данных пациентов (например, облачные CRM-системы).

На данный момент определен перечень стран (это страны — подписанты Конвенции Совета Европы № 108), передача персональных данных

в которые **не обременяет оператора персональных данных дополнительными юридическими обязательствами**.

Если персональные данные белорусских пациентов будут храниться не в вышеуказанных юрисдикциях, оператор персональных данных обязан обеспечить надлежащий уровень защиты персональных данных самостоятельно.

Обеспечить уровень защиты самостоятельно — это значит, что оператору нужно:

- взять у субъекта персональных данных информированное согласие;
- обеспечить наличие договора с субъектом;
- получить разрешение Национального центра по защите персональных данных и т.д.

ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Одной из главных точек соприкосновения операторов и субъектов персональных данных является реализация нового и достаточно объемного списка прав субъектов.

В соответствии с Законом субъекты персональных данных могут обратиться за:

- отзывом своего согласия на обработку персональных данных;
- получением информации, касающейся обработки данных, и за их исправлением;
- получением информации о передаче их персональных данных третьим лицам;
- прекращением обработки данных и их удалением.

Реализация прав субъектов персональных данных имеет четкие временные границы: запросы должны исполняться в течение 15 календарных дней.

Единственным исключением из данного правила является право субъекта на предоставление информации, которое должно быть реализовано оператором в **5-дневный срок с момента получения соответствующего запроса**.

Права субъектов персональных данных не являются абсолютными, при реализации каждого из них предусмотрен **определенный перечень исключений**, которые позволяют защитить в т.ч. и законные интересы операторов персональных данных.

ЗАКЛЮЧЕНИЕ

Защита персональных данных и обеспечение приватности субъектов персональных данных является комплексной задачей, для решения которой необходимо привлечение значительного количества как внутренних, так и внешних ресурсов. Важно помнить, что комплексный характер задачи обеспечивается в первую очередь разнообразием внедряемых мер: некоторые аспекты требуют технической и даже бизнес-компетенции, а некоторые — юридического анализа.

ОРГАНИЗУЕМ КОМПЛЕКС МЕР ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Вопросы защиты персональных данных особенно важны для руководителей, ведь организации здравоохранения являются операторами персональных данных не только работников, но и пациентов (клиентов). Какой комплекс мер необходимо предпринять для обеспечения грамотного подхода к обработке персональных данных? Расскажем далее.

Татьяна СОКОЛОВСКАЯ, *ведущий юрисконсульт ГУ «Республиканский научно-практический центр онкологии и медицинской радиологии им. Н. Н. Александрова», старший преподаватель кафедры конституционного права юридического факультета БГУ*

Помимо Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон), который закрепляет общие понятия и принципы работы с персональными данными, вопросы персональных данных регулируются Указом Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных» (далее — Указ).

Данным Указом:

- создан Национальный центр защиты персональных данных Республики Беларусь;

- утверждено Положение о Национальном центре защиты персональных данных Республики Беларусь (далее — Положение);
- определен ряд обязанностей операторов персональных данных.

Справочно: *Национальный центр защиты персональных данных является уполномоченным органом по защите прав субъектов персональных данных.*

Учредителем Национального центра защиты персональных данных и государственным органом, осуществляющим от имени Республики Беларусь права собственника имущества этого учреждения, является Оперативно-аналитический центр при Президенте Республики Беларусь (п. 4 Положения).

ОБЯЗАННОСТИ ОПЕРАТОРА

Подпунктом 3.5 п. 3 Указа определено, что операторы, являющиеся государственными органами, юридическими лицами Республики Беларусь, иными организациями, устанавливают и поддерживают в актуальном состоянии:

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

Справочно: *классификация информационных ресурсов (систем), содержащих персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных установлена приказом Национального центра защиты персональных данных от 15.11.2021 № 12 «О классификации информационных ресурсов (систем)».*

2) категории персональных данных, подлежащие включению в такие ресурсы (системы).

Как правило, это такие категории, как:

- общедоступные персональные данные;
- специальные персональные данные (кроме биометрических и генетических персональных данных);
- биометрические и генетические персональные данные;
- персональные данные, не являющиеся общедоступными или специальными;

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

Справочно: *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 (ст. 1 Закона).

4) срок хранения обрабатываемых персональных данных.

Согласно подп. 3.6 п. 3 Указа операторы обязаны вносить в создаваемый Национальным центром защиты персональных данных государственный информационный ресурс «Реестр операторов персональных данных» сведения об информационных ресурсах (системах), содержащих персональные данные, а также обеспечивать актуализацию соответствующих сведений.

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии со ст. 17 Закона 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.

Оператор (уполномоченное лицо) определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты персональных данных, с учетом требований Закона и иных актов законодательства.

Приведем комплекс обязательных мер по обеспечению защиты персональных данных, который обязан реализовать оператор (уполномоченное лицо):

1) назначить структурное подразделение или лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных, издав соответствующий приказ;

2) подготовить локальные правовые акты, определяющие политику оператора (уполномоченного лица) в отношении обработки персональных данных;

3) ознакомить работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в т.ч. с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также организовать обучение указанных работников и иных лиц в порядке, установленном законодательством;

4) пройти обучение по вопросам защиты персональных данных;

5) установить порядок доступа к персональным данным, в т.ч. обрабатываемым в информационном ресурсе (системе);

6) осуществить техническую и криптографическую защиту персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные;

7) прекратить обработку персональных данных в определенных случаях.

НАЗНАЧЕНИЕ ОТВЕТСТВЕННЫХ ЛИЦ

Ни Законом, ни иными актами законодательства не установлено, какое именно структурное подразделение или лицо может быть назначено ответственным за осуществление внутреннего контроля за обработкой персональных данных. Следовательно, оператор по своему усмотрению может назначить такое лицо или структурное подразделение.

Представляется обоснованным назначение ответственным работника или структурное подразделение, которые имеют схожие, смежные функции, определенные должностными инструкциями, положениями о структурных подразделениях, соответствующий практический опыт в данной сфере, с учетом вида реализуемых мер.

МНЕНИЕ АВТОРА

Ответственным(-и) лицом(-ами) за осуществление внутреннего контроля за обработкой персональных данных субъектов персональных данных целесообразно назначить заместителя(-ей) руководителя организации здравоохранения (организационный блок).

Ответственное лицо назначается соответствующим приказом. Помимо назначения ответственного лица оператору (уполномоченному лицу) приказом необходимо утвердить:

- перечень лиц, имеющих доступ к персональным данным субъектов персональных данных;
- перечень лиц, осуществляющих обработку персональных данных субъектов персональных данных.

Примерный образец приказа о правовом режиме защиты персональных данных в организации здравоохранения*

Кроме того, руководителю необходимо возложить ряд обязанностей на кадровую и юридическую службы.

Так, на **кадровую службу (инспектора по кадрам)** возлагаются обязанности по:

- ознакомлению работников под роспись с требованиями законодательства в сфере обработки и защиты персональных данных и локальными правовыми актами оператора (уполномоченного лица);
- организации направления на обучение по вопросам защиты персональных данных лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных, а также лиц, непосредственно осуществляющих обработку персональных данных, не реже одного раза в пять лет;
- организации внесения в локальные правовые акты (положение о структурном подразделении, должностные инструкции и т.д.) работников отдела автоматизированных систем управления, лиц, имеющих допуск и осуществляющих обработку персональных данных, изменений и дополнений по вопросам защиты персональных данных.

На юридическую службу или юрисконсульта возлагаются обязанности по правовому сопровождению указанной работы, включая участие в подготовке соответствующих локальных правовых актов оператора (уполномоченного лица).

Обязанности по реализации технических мер 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 возлагаются ***на отдел автоматизированных систем управления (инженера-программиста и т.д.)***.

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ПОДГОТОВКА ЛОКАЛЬНЫХ ПРАВОВЫХ АКТОВ

Одним из таких документов является политика оператора — организации здравоохранения в отношении обработки персональных данных.

Примерный образец Политики оператора в отношении обработки персональных данных*

Кроме того, оператор персональных данных может разработать следующие документы:

- шаблон договора, который заключается с субъектом персональных данных,— если оператор персональных данных использует договор в качестве правового основания для обработки персональных данных;
- шаблон договора поручения на обработку персональных данных с уполномоченным лицом — если оператор персональных данных поручает обработку персональных данных уполномоченному лицу.

ОЗНАКОМЛЕНИЕ РАБОТНИКОВ

Оператору необходимо ознакомить работников и иных лиц, непосредственно осуществляющих обработку персональных данных, с

- положениями законодательства о персональных данных, в т.ч. с требованиями по защите персональных данных;
- документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Оператор обязан организовать обучение указанных работников и иных лиц в порядке, установленном законодательством.

МНЕНИЕ АВТОРА

*Обязанность по ознакомлению работников целесообразно возложить приказом **на руководителей структурных подразделений**, а при приеме на работу новых работников — **на отдел кадров** (инспектора по кадрам).*

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ПРОХОЖДЕНИЕ ОБУЧЕНИЯ

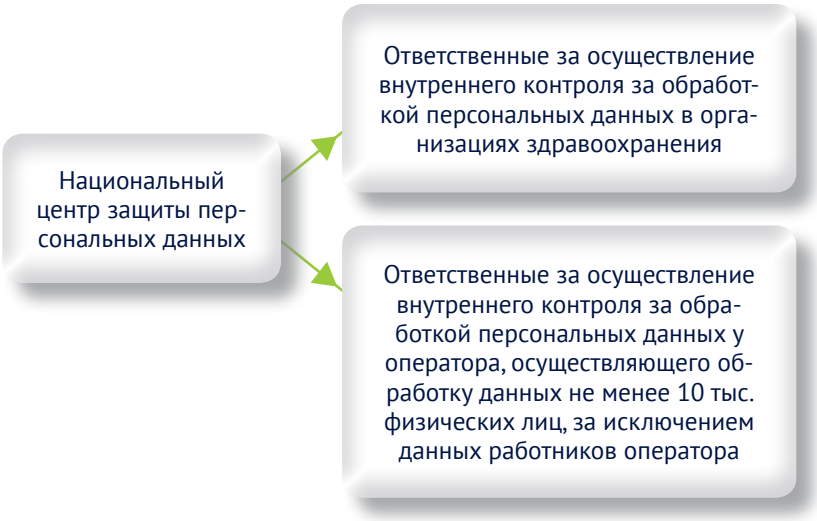
В соответствии с подп. 3.3 п. 3 Указа операторы (уполномоченные лица) организуют **не реже одного раза в пять лет** прохождение обучения по вопросам защиты персональных данных лицами, **ответственными за осуществление внутреннего контроля** за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных

Вопросы обучения регулируются приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12.11.2021 № 194 «Об обучении по вопросам защиты персональных данных».

Лица, которые проходят обучение в Национальном центре защиты персональных данных по программе повышения квалификации руководящих работников и специалистов, представлены на схеме.

Схема

Субъекты обучения
в Национальном центре защиты персональных данных



Что касается иных лиц, то они проходят обучение:

- 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 их знаний по вопросам защиты персональных данных (в форме собеседования, опроса, тестирования и других формах контроля знаний).

Операторы (уполномоченные лица) до 15 ноября каждого года должны обеспечить представление Национальному центру защиты персональных данных 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 Национальном центре защиты персональных данных.

УСТАНОВЛЕНИЕ ПОРЯДКА ДОСТУПА

Порядок доступа к персональным данным, в т.ч. обрабатываемым в информационном ресурсе (системе), целесообразно установить в Положении об обработке персональных данных.

Примерный образец Положения о правовом режиме защиты персональных данных в организации здравоохранения*

Руководителю необходимо учесть, что в Положении об обработке персональных данных обязательно должны быть отражены следующие вопросы:

- категории субъектов персональных данных;
- содержание и объем персональных данных;
- цели обработки персональных данных;
- правила обработки персональных данных;
- порядок получения согласия, отзыва согласия субъекта персональных данных и форма их получения, включая утверждение такой формы;
- хранение персональных данных;

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

- порядок использования, предоставления и распространения персональных данных;
- права и обязанности субъектов персональных данных;
- обязанности оператора (лиц, ответственных за обработку персональных данных);
- меры по обеспечению защиты персональных данных;
- обжалование действий (бездействия) и решений оператора и т.д.

При этом необходимо помнить, что для обработки персональных данных в некоторых случаях требуется получить согласие субъекта. Перед получением такого согласия оператору следует учесть некоторые особенности.

Предоставление информации

До получения согласия субъекта персональных данных оператор обязан в устной, письменной либо электронной форме, соответствующей форме выражения такого согласия, предоставить субъекту персональных данных информацию, представленную на *схеме* на следующей странице.

Исключительно в письменном виде данная информация предоставляется пациентам или лицам, указанным в ч. 2 ст. 18 Закона о здравоохранении. Пользователям сайта организации здравоохранения указанная информация предоставляется в электронном виде.

МНЕНИЕ АВТОРА

Представляется обоснованной подготовка для субъекта персональных данных соответствующего уведомления, содержащего указанную информацию.

Разъяснение прав

Оператор перед получением согласия 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 оператором субъекту персональных данных в устной, письменной либо электронной форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой ему информации.

Схема

Информация, предоставляемая субъектам персональных данных

Когда согласие субъекта не требуется

Статьей 6 Закона определен перечень случаев, когда согласие субъекта персональных данных не требуется. Например, согласие не требуется в следующих случаях:

- для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности;
- в целях осуществления контроля (надзора) в соответствии с законодательными актами;
- 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;
- **для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в т.ч. профессионального пенсионного страхования;**
- **при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством;**
- при получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;
- **для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;**
- в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;
- в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

Статья 8 Закона определяет порядок обработки ***специальных персональных данных***.

Обработка специальных персональных данных без согласия субъекта персональных данных запрещается, за исключением случаев, предусмотренных п. 2 ст. 8 Закона.

В соответствии с п. 2 ст. 8 Закона согласие субъекта персональных данных на обработку специальных персональных данных не требуется:

- если специальные персональные данные сделаны общедоступными персональными данными самим субъектом персональных данных;
- **при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством;**
- **в целях организации оказания медицинской помощи при условии, что такие персональные данные обрабатываются медицинским, фармацевтическим или иным работником здравоохранения, на которого возложены обязанности по обеспечению защиты персональных данных и в соответствии с законодательством распространяется обязанность сохранять врачебную тайну;**
- для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности;
- в целях обеспечения функционирования единой государственной системы регистрации и учета правонарушений;
- **для осуществления административных процедур;**
- **для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;**
- в случаях, когда обработка специальных персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами;
- в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка специальных персональных данных без согласия субъекта персональных данных.

МНЕНИЕ АВТОРА

В соответствии с ч. 13 ст. 44 и ч. 3 ст. 51 Закона Республики Беларусь от 18.06.1993 № 2435-XII «О здравоохранении» (в ред. от 11.12.2020) Министерством здравоохранения Республики Беларусь принято постановление

от 07.06.2021 № 74 «О формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента» (далее — постановление № 74), которое утвердило форму согласия на внесение и обработку персональных данных пациента.

Представляется, что форма согласия, утвержденная постановлением № 74, будет актуализирована с учетом вступившего в силу с 15 ноября 2021 г. Закона и принятых в его развитие актов законодательства.

Необходимо помнить, что оператор (уполномоченное лицо), являющийся юридическим лицом Республики Беларусь, иной организацией, индивидуальным предпринимателем, **обязан обеспечить неограниченный доступ**, в т.ч. с использованием сети Интернет, **к документам, определяющим политику оператора** (уполномоченного лица) в отношении обработки персональных данных, ***до начала такой обработки***. Как правило, это реализуется через сайт организации здравоохранения.

ТЕХНИЧЕСКАЯ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Одной из мер защиты персональных данных является осуществление оператором их технической и криптографической защиты в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Работу по технической и криптографической защите персональных данных следует организовывать с учетом:

- п. 4 Положения о порядке технической и криптографической защиты информации в информационных системах для обработки информации, распространение которой ограничено (утв. приказом 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»);
- пп. 9 и 10 Положения о технической и криптографической защите информации (утв. Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации»).

С учетом вышеуказанных нормативных правовых актов рассмотрим, кем могут выполняться работы по технической и криптографической защите информации у собственника (владельца) информационной системы.

Подразделение защиты информации

Выполнять работу по технической и криптографической защите информации может подразделение защиты информации или иное подразделение (должностное лицо), ответственное за обеспечение защиты информации.

Работники такого подразделения или должностное лицо должны иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации.

Специализированная организация

Такого рода работы могут выполнять организации, имеющие специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ (далее — специализированные организации).

Физические лица

Защита персональных данных может быть организована физическими лицами (в т.ч. индивидуальными предпринимателями) — собственниками (владельцами) информационных систем, в которых обрабатываются персональные данные, самостоятельно (без создания (назначения) подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации) либо с привлечением специализированной организации.

Справочно: *в данном случае нужно учитывать ограничения, предусмотренные п. 3 приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12.11.2021 № 195 «О технической и криптографической защите персональных данных».*

ПРЕКРАЩЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных должна ограничиваться достижением конкретных, заранее заявленных законных целей.

Согласно ч. 1 п. 4 ст. 4 Закона обработка персональных данных, не совместимая с первоначально заявленными целями их обработки, не допускается.

В соответствии с абз. 7 п. 1 ст. 16 Закона при отсутствии оснований для обработки персональных данных, предусмотренных данным Законом и иными законодательными актами, оператор персональных данных:

- прекращает обработку персональных данных, а также удаляет или блокирует их;
- обеспечивает прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом.

При этом согласно ст. 13 Закона субъект персональных данных имеет право потребовать прекращения обработки персональных данных, включая их удаление. В таком случае оператор обязан прекратить обработку персональных данных субъекта при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами. ◈

ПОДГОТОВКА К РАЗРАБОТКЕ ПОЛИТИКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ: ПРОВОДИМ АНАЛИЗ

Подготовка политики обработки персональных данных — одна из обязанностей операторов в соответствии с Законом Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон). Однако при ее составлении нужно учитывать много нюансов. Мы дадим вам рекомендации о том, какие шаги стоит предпринять и на какие моменты обратить внимание организациям здравоохранения при составлении такого документа.

Алёна ПОТОРСКАЯ, *ведущий юрист REVERA, руководитель проектов в сфере защиты персональных данных*

Ольга ОПИМАХ, *юрист REVERA*

Согласно Закону издание документов, определяющих **политику оператора** (уполномоченного лица) в отношении обработки персональных данных (далее — Политика обработки персональных дан-

ных), является одной из обязательных мер по обеспечению защиты персональных данных (далее — ПД).

Основное назначение Политики обработки персональных данных — разъяснить **субъектам ПД**, кто собирает, использует или иным образом обрабатывает их ПД, в каком объеме и для каких целей осуществляется обработка, какие права есть у субъектов в связи с этим и каков механизм реализации их прав.

Справочно: *при составлении Политики обработки персональных данных необходимо руководствоваться следующими документами:*

- *Законом;*
- *Рекомендациями от 07.12.2021 по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных (далее — Рекомендации), подготовленными Национальным центром защиты персональных данных (далее — НЦЗПД).*

Необходимость руководствоваться Законом обусловлена тем, что в данном Законе:

- закреплены основные дефиниции;
- определены общие принципы обработки ПД;
- названы правовые основания, на которых может осуществляться обработка ПД;
- установлены права субъектов ПД и т.д.

Что же необходимо предпринять организации здравоохранения при подготовке Политики обработки персональных данных? В первую очередь следует проанализировать процессы обработки ПД.

АНАЛИЗ ПРОЦЕССОВ ОБРАБОТКИ ПД

Перед написанием самой Политики обработки персональных данных необходимо определить те ключевые точки, в которых организация имеет дело с ПД. Ситуации, в которых организация здравоохранения может столкнуться с обработкой ПД, представлены на *схеме* на следующей странице.

Схема

Возможные случаи возникновения необходимости обработки ПД

Для того чтобы определить процесс обработки ПД для каждого случая, можно составить реестр обработки ПД в организации. Реестр позволит структурировать информацию и упростит написание Политики обработки персональных данных, так как все необходимые сведения о процессах обработки ПД уже будут собраны в одном месте.

РЕЕСТР ПД

Структуру такого реестра каждая организация здравоохранения может определить самостоятельно, но мы рекомендуем прописать в реестре следующее:

- цель обработки ПД;
- категории субъектов ПД, чьи данные обрабатываются;
- перечень ПД;
- правовое основание для обработки;
- срок хранения ПД;
- лица, которым поручается обработка ПД (уполномоченные лица);
- лицо (подразделение), ответственное за обработку ПД в организации.

Цель обработки

Определение цели обработки — это отправная точка при разработке реестра. Согласно Рекомендациям перечень ПД, правовое основание для их обработки и иное указываются **в отношении каждой конкретной цели**.

Цели обработки ПД могут основываться на:

- требованиях законодательства;
- положениях договоров;
- вытекать из осуществляемой организацией деятельности.

*Цели должны быть **конкретными** и позволять субъекту ПД понять, для чего будут обрабатываться его ПД.*

Примеры сформулированной цели:

- оказание платных медицинских услуг на основании договора, заключенного с субъектом ПД;
- получение обратной связи от пациента о качестве оказанных ему услуг и т.д.

Не допускается указание абстрактных или общих целей, которые не определяют пределов обработки и не позволяют субъекту ПД понять, для чего будут обрабатываться его ПД.

Так, не соответствуют критерию ***конкретности*** следующие формулировки:

- для совершенствования деятельности организации;
- для разработки новых услуг;
- для достижения общественно значимых целей.

Категории субъектов

В качестве субъектов ПД могут быть указаны: работники (в т.ч. уволенные); их родственники (члены семьи); соискатели на должность; контрагенты организации здравоохранения; посетители организации здравоохранения; пациенты; пользователи сайта организации и т.д.

Перечень ПД

Перечень ПД может быть прописан путем перечисления обрабатываемых ПД, отсылки к акту законодательства, перечисляющему ПД или устанавливающему форму ПД, а также через критерии, очерчивающие объем обрабатываемых данных.

ПРИМЕР

Перечень ПД можно сформулировать в следующем формате:

- *генетические ПД;*
- *фотографии, изображения с камер видеонаблюдения, записи голоса;*
- *информация, составляющая врачебную тайну в соответствии со ст. 46 Закона Республики Беларусь от 18.06.1993 № 2435-XII «О здравоохранении» (в ред. от 11.12.2020).*

Правовое основание

Закон устанавливает закрытый перечень правовых оснований обработки ПД.

Надлежащим основанием для обработки ПД в отношении каждой конкретной цели может быть только одно основание, перечисленное в Законе.

Закон разграничивает основания обработки специальных ПД и иных ПД (не относящихся к специальным).

Справочно: *абз. 12 ст. 1 Закона закрепляет понятие* ***«специальные ПД»*** *— это ПД, 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 ПД.*

Абзацем 2 ст. 1 Закона предусмотрено понятие биометрических ПД. ***Биометрические ПД*** *— это 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 др.).

В абз. 4 ст. 1 Закона содержится понятие генетических ПД. Так, ***генетические ПД*** *— это 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.*

Правовые основания обработки специальных ПД в организации здравоохранения — это:

- согласие (п. 1 ст. 8 Закона);
- иные основания, не связанные с согласием, — их всего 16 (п. 2 ст. 8 Закона).

Правовые основания обработки иных категорий ПД (не относящихся к специальным) — это:

- согласие (ст. 5 Закона);
- иные основания, не связанные с согласием, — их всего 20 (ст. 6 Закона).

Согласие — это последнее основание, к которому необходимо обращаться, если все иные основания, перечисленные в Законе, не являются надлежащими в отношении конкретной цели.

Основания для обработки ПД, не связанных с получением согласия (как для специальных ПД, так и для иных категорий ПД), наиболее актуальные для организаций здравоохранения, представлены в *таблице*.

Таблица

Правовые основания обработки ПД без получения согласия

Правовое основание	Специальные ПД	Иные категории ПД
Организация оказания медицинской помощи при условии, что ПД обрабатываются медицинским, фармацевтическим или иным работником здравоохранения, на которого возложены обязанности по обеспечению защиты ПД и в соответствии с законодательством распространяется обязанность сохранять врачебную тайну	+	

Правовое основание	Специальные ПД	Иные категории ПД
Защита жизни, здоровья или иных жизненно важных интересов субъекта ПД или иных лиц, если получение согласия субъекта ПД невозможно	+	+
Выполнение обязанностей (полномочий), предусмотренных законодательными актами	+	+
Законом и иными законодательными актами прямо предусматривается обработка специальных *ПД без согласия* субъекта ПД	+	
Специальные ПД сделаны общедоступными самим субъектом ПД	+	
Оформление трудовых (служебных) отношений, а также процесс трудовой (служебной) деятельности субъекта ПД в случаях, предусмотренных законодательством	+	+
Получение ПД оператором на основании договора, заключенного (заключаемого) субъектом ПД, в целях совершения действий, установленных этим договором		+
Персональные данные указаны в документе, адресованном оператору и подписанном субъектом ПД, в соответствии с содержанием такого документа		+
Распространенные ранее ПД до момента заявления субъектом ПД требований о прекращении обработки распространенных ПД, а также об их удалении (при отсутствии иных оснований для обработки ПД, предусмотренных Законом и иными законодательными актами)		+

Срок хранения ПД

Срок хранения ПД может быть установлен следующими способами:

- точный срок (дата или период времени), к примеру: 1 год, до 31 декабря 2022 г. и иное;
- с помощью критериев для определения срока, к примеру: 1 год с момента последнего взаимодействия пациента с организацией здравоохранения.

Уполномоченные лица

Анализ данного показателя проводится в том случае, если обработка ПД поручается организацией здравоохранения другому лицу от имени или в интересах организации.

Например, организацией могут быть привлечены сторонняя специализированная компания или индивидуальный предприниматель для ведения бухгалтерского учета, обеспечения охраны труда, кадрового и воинского учета в организации. В таком случае данные компании будут выступать уполномоченными лицами.

Ответственные за обработку ПД

В зависимости от конкретной цели обработки ответственными за обработку ПД могут выступать бухгалтерия, специалист по кадрам, служба охраны труда, лицо, ответственное за осуществление внутреннего контроля за обработкой ПД, и др.

ФОРМА РЕЕСТРА

Реестр можно вести в произвольной форме, например в виде таблицы.

***Примерный образец выдержки из формы реестра ПД**

Руководителю необходимо обратить внимание на то, что полноценный реестр должен отражать все цели обработки ПД. Составление реестра и проведение анализа вышеуказанных вопросов поспособствуют более грамотной разработке Политики обработки персональных данных в организации здравоохранения. ◈

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

СОСТАВЛЯЕМ ПОЛИТИКУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ ЗДРАВООХРАНЕНИЯ

Проведя анализ персональных данных, подлежащих обработке в рамках организации здравоохранения, необходимо перейти к разработке Политики обработки персональных данных. Мы расскажем, какие правила целесообразно соблюсти для того, чтобы грамотно составить данный локальный акт организации.

Алёна ПОТОРСКАЯ, *ведущий юрист REVERA, руководитель проектов в сфере защиты персональных данных*

Ольга ОПИМАХ, *юрист REVERA*

При составлении Политики обработки персональных данных рекомендуется обратить внимание на следующие моменты:

- форма политики;
- язык изложения политики;
- основные формулировки, отраженные в политике;

- содержание политики;
- доступность политики.

Рассмотрим их подробнее.

ФОРМА ПОЛИТИКИ

Политика может представлять собой как единый самостоятельный документ, так и несколько отдельных документов, определяющих порядок обработки персональных данных в определенных сферах или в связи с определенными бизнес-процессами.

Так, к примеру, могут быть разработаны отдельные документы, регулирующие:

- обработку персональных данных соискателей на должности, работников, их близких родственников (членов семьи), контрагентов;
- обработку персональных данных посетителей медицинских учреждений и пациентов.

Справочно: *при необходимости отдельный документ также может быть разработан в отношении посетителей сайта и пользователей мобильных приложений (при наличии).*

ЯЗЫК ИЗЛОЖЕНИЯ

Политику обработки персональных данных следует писать простым, ясным и доступным для лица без специальных знаний в области юриспруденции языком.

Для обеспечения лучшего восприятия рекомендуется избегать излишнего цитирования актов законодательства, использования большого числа специальных терминов, подробного описания технических аспектов обработки персональных данных.

ОСНОВНЫЕ ФОРМУЛИРОВКИ

Следует избегать общих фраз и незакрытых перечней. В частности, рекомендуется отказаться от использования таких фраз, как «может», «вероятно», «некоторый», «часто», «возможно», «в зависимости от ситуации», поскольку это указывает на то, что организация предоставляет информацию лишь частично.

СОДЕРЖАНИЕ ПОЛИТИКИ

В соответствии с Рекомендациями от 07.12.2021 по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных, подготовленными Национальным центром защиты персональных данных, в Политику обработки персональных данных стоит включить следующие разделы:

- общие положения;
- цели и правовые основания;
- категории субъектов;
- порядок и условия обработки ПД;
- права субъектов ПД;
- трансграничная передача ПД.

Общие положения

В данном разделе следует отразить как минимум наименование организации и процессы, на которые распространяется действие Политики (например, обработка персональных данных посетителей медицинских учреждений и пациентов).

Также в общих положениях целесообразно прописать основные понятия, отражающие специфику обработки персональных данных в организации здравоохранения (к примеру, включить определения специальных, биометрических, генетических данных).

Цели и правовые основания обработки персональных данных

Лучше всего отразить цели и правовые основания на стадии анализа и составления реестра персональных данных. Это значительно упростит их отражение непосредственно в Политике обработки персональных данных.

Категории субъектов ПД и перечень обрабатываемых ПД

Как цели и правовые основания, так и категории субъектов ПД и перечень обрабатываемых ПД также целесообразно проанализировать заранее и отразить в реестре.

Справочно: *если данная информация будет содержаться в реестре, то ее достаточно будет просто перенести в саму Политику.*

Важно помнить, что как при составлении реестра, так и при включении информации из реестра в Политику обработки персональных данных

необходимо отталкиваться от целей обработки персональных данных. При этом сопутствующая информация (такая как перечень персональных данных, правовые основания и иное) указывается к каждой конкретной цели.

Выполнить данное требование можно путем описания процессов в форме таблицы (по аналогии с тем, как они описаны в реестре) либо списком в следующем формате.

ПРИМЕР

1. Цель — ...:
категории субъектов: ...,
перечень данных: ...,
правовое основание: ...,
срок хранения: ...
и иное.

2. Цель — ...:
категории субъектов: ... и так далее.

Справочно: *в качестве примера можно рассмотреть Политику обработки персональных данных НЦЗПД.*

Пример Политики обработки персональных данных НЦЗПД*

Порядок и условия обработки ПД

В данном разделе следует указать перечень осуществляемых действий с персональными данными. В частности, это могут быть сбор, систематизация, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных или иные действия, совершаемые с персональными данными.

Здесь же стоит указать **источник получения** персональных данных (к примеру, сам субъект персональных данных, законный представитель и т.д.).

Если обработка персональных данных поручается уполномоченному лицу (что отражено в реестре), рекомендуется в Политике обработки персональных данных указать информацию о таких лицах, а именно:

- наименование и местонахождение уполномоченного лица или категории уполномоченных лиц;

* *Ссылка доступна* ***только при условии подключения к сети Интернет.***

- основания обработки персональных данных;
- перечень персональных данных, обработка которых поручена уполномоченному лицу;
- перечень действий с персональными данными, осуществляемых уполномоченным лицом.

Также если сроки хранения персональных данных уже были зафиксированы в реестре, на этапе составления Политики останется лишь перенести эти сведения в Политику обработки персональных данных.

Права субъектов ПД

В данном разделе следует не просто перечислить права субъектов ПД, но и расписать механизм подачи соответствующих заявлений и порядок их рассмотрения.

Также рекомендуется указать данные работника (структурного подразделения) оператора, ответственного за осуществление внутреннего контроля за обработкой персональных данных, к которому субъект сможет обратиться за содействием в реализации прав субъекта персональных данных.

Трансграничная передача ПД

Если организация планирует осуществлять трансграничную передачу персональных данных, следует отразить применительно к каждой **цели передачи:**

- субъекты (категории субъектов) в иностранных государствах, которым персональные данные могут быть переданы, с указанием возможного способа связи с ними;
- страны, на территории которых находятся такие субъекты (категории субъектов);
- основания для трансграничной передачи.

В этом разделе также нужно указать, относятся ли страны, в которые планируется производить трансграничную передачу персональных данных, к государствам, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных.

Справочно: *в перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных, включаются иностранные государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной*

обработке персональных данных, принятой в г. Страсбурге 28 января 1981 г. (приказ директора НЦЗПД от 15.11.2021 № 14 «О трансграничной передаче персональных данных»).

ДОСТУПНОСТЬ ПОЛИТИКИ

Согласно п. 4 ст. 17 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» организациям необходимо обеспечить неограниченный доступ к Политике обработки персональных данных.

Сделать это можно путем размещения Политики обработки персональных данных на сайте организации, на информационных стендах или иными способами.

При наличии у организации сайта Политика обработки персональных данных должна размещаться на этом сайте, как правило, на странице не ниже второго уровня, а также дополнительно может размещаться на иных интернет-ресурсах или распространяться другими способами.

РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ: ЧТО НУЖНО ЗНАТЬ НАНИМАТЕЛЮ

С 15 ноября 2021 г. наниматели работают по-новому, ведь большая часть открытой информации теперь не является таковой. Мы расскажем, что необходимо учитывать нанимателю при работе с данными работников с учетом действия Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон).

Владимир САМОСЕЙКО, *юрист, магистр права*

С 15 ноября 2021 г. в каждой организации были введены изменения в связи со вступлением в силу Закона. Не остались в стороне и организации здравоохранения, которые осуществляют работу не только с персональными данными работников, но и с персональными данными пациентов. Что же относится к персональным данным и имеются ли у них разграничения?

ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ИХ ПЕРЕЧЕНЬ

Под персональными данными понимается любая информация (ее совокупность), которая позволяет определить (идентифицировать) физическое лицо.

В Законе четко не поименован перечень информации, которая может относиться к персональным данным. Таким образом, этот перечень является открытым.

Получается, что для каждого конкретного случая необходимо определять индивидуально, относятся ли какие-то сведения к персональным данным.

Справочно: *поскольку организации здравоохранения будут отрабатывать не только данные своих работников, но и персональные данные пациентов, то вопрос о том, когда фото, видео, номер телефона, сетевые идентификаторы, зарплата и условия работы, профессия и образование будут являться персональными данными, зависит от ситуации.*

Примерный перечень данных, которые могут быть отнесены к персональным данным, приведен в *таблице*.

Таблица

Примерный перечень персональных данных (носит оценочный характер)

Общие персональные данные	
ФИО; дата, месяц и год рождения; идентификационный номер; серия и номер документа, удостоверяющего личность; конкретный адрес регистрации и проживания; семейное положение; образование; профессия; имущественное положение; размеры доходов; сетевые идентификаторы (IP-адрес, файлы cookie и др.); сведения о заработной плате и условия выполняемой работы	
Специальные персональные данные	
Биометрические персональные данные	– (цветное) цифровое фотографическое изображение лица; – отпечатки пальцев рук, ладоней; – радужная оболочка глаза; – характеристики лица
Генетические персональные данные	результаты медицинских исследований и т. п.
Иные персональные данные	– расовая либо национальная принадлежность; – политические взгляды; – членство в профессиональных союзах; – религиозные или другие убеждения; – здоровье (информация о нем); – половая жизнь; – привлечение к административной или уголовной ответственности

ПЕРСОНАЛЬНЫЕ ДАННЫЕ РАБОТНИКОВ

Перечень персональных данных работников достаточно обширен. При этом возникает вопрос, нужно ли затребовать с работника соответствующее согласие.

Из ст. 6 и 8 Закона следует, что получать согласие на обработку персональных данных при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных **не требуется в случаях, предусмотренных законодательством**.

МНЕНИЕ АВТОРА

Таким образом, при работе с персональными данными в случае оформления трудовых отношений оценочный подход к персональным данным недопустим, поскольку случаи, при которых согласие работника не нужно, должны быть предусмотрены законодательством.

Полагаем, что согласие работника на обработку персональных данных не требуется, когда необходимо составить документы или совершить действия, которые предусмотрены законодательством.

Так, из ст. 6 и 8 Закона следует, что не нужно требовать согласие работника на обработку персональных данных при:

- удостоверении личности при оформлении приема на работу;
- проверке квалификации;
- проверке соответствия состояния здоровья по нужной работе;
- оформлении трудового договора и трудовой книжки;
- издании приказа о приеме на работу и формировании личного дела и т.п.

Отсутствие необходимости получения согласия совсем не означает, что наниматель (организация, оператор) не обязан обеспечивать сохранность и конфиденциальность (защиту) персональных данных.

Ярким примером в этом случае является практика Российской Федерации. Так, в РФ организация обязана обеспечить отдельное хранение персональных данных в зависимости от цели их обработки (чтобы обеспечить срок хранения (своевременность уничтожения) и не допустить избыточности при сборе персональных данных).

При этом необходимо помнить, что иногда в кадровом делопроизводстве оформляется ряд документов, не предусмотренных напрямую законодательством.

МНЕНИЕ АВТОРА

По нашему мнению, нужно получать согласие на обработку персональных данных в следующих случаях:

- *при анкетировании, в т.ч. психологическом при приеме на работу;*
- *при получении биометрических данных для оформления пропуска, для осуществления учета (контроля) рабочего времени;*
- *при получении сведений о членстве работника в профсоюзе, если на него не ведется личное дело, и т. п.*

ИСКЛЮЧЕНИЕ ИЗ ОБЩЕГО ПРАВИЛА

Если говорить об организации здравоохранения как о нанимателе, то помимо приведенных ранее общих случаев, при которых согласие на обработку персональных данных не требуется, можно выделить еще ряд целей, при которых организация здравоохранения может не требовать согласие на обработку персональных данных работника (с учетом норм ст. 6 Закона):

- при реализации норм законодательства о борьбе с коррупцией;
- для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в т.ч. профессионального пенсионного страхования;
- в целях назначения и выплаты пенсий, пособий;
- для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;
- при получении персональных данных оператором на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором.

Иногда цели использования персональных данных могут меняться. Так, у работника могут производиться удержания из заработной платы налогов, средств в возмещение ущерба, алиментов.

В таком случае цель обработки персональных данных изменяется и возникает вопрос с хранением таких данных с учетом целей их обработки.

ДОПУСК РАБОТНИКА К СВОИМ ПЕРСОНАЛЬНЫМ ДАННЫМ

В соответствии с п. 1 ст. 11 и ст. 12 Закона субъект персональных данных имеет право не только на получение информации, касающейся обработки своих персональных данных, но и на получение информации о предоставлении персональных данных третьим лицам.

В настоящее время порядок ознакомления работника с личным делом **законодательно не закреплен**.

В связи с этим возникает вопрос, как определить конкретный порядок доступа работников к своим персональным данным, а также ознакомления с личными делами (при их ведении).

ЧТО МОЖЕТ СДЕЛАТЬ НАНИМАТЕЛЬ

Несмотря на то, что в некоторых случаях, определенных Законом, обработка данных работников не требует получения согласия, все же некоторые сведения о работниках, которые обрабатывает наниматель, могут быть напрямую не связаны с трудовыми отношениями.

В связи с этим нанимателю нужно **обратить внимание** на то, какие сведения истребуются от работника, оценить их реальную необходимость для работы организации. Проведение и результат этого анализа целесообразно закрепить в Положении о работе с персональными данными.

Выдержка из Положения о работе с персональными данными (в части вопроса ПД работников)*

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ЗАКЛЮЧЕНИЕ

Для нашей страны институт защиты персональных данных совсем новый. Во многом у нанимателей могут возникать вопросы по их обработке и хранению.

Как показывает международный опыт, правоприменительная практика может быть различной. Так, например, в Российской Федерации, где институт персональных данных действует с 2006 г., отдельные суды относят номер мобильного телефона к персональным данным; другие же, напротив, не считают его персональными данными. Какая ситуация сложится в нашей стране, пока сказать сложно, это будет понятно с течением времени, по итогам практического применения норм Закона.

О НЕКОТОРЫХ ВОПРОСАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ: ПРАКТИЧЕСКИЕ СИТУАЦИИ И ИХ ПРАВОВОЕ ОБОСНОВАНИЕ

Общую политику обработки персональных данных работников можно определить исходя из анализа норм Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон), а также из предшествующего аналитического материала. Однако не стоит забывать, что не все ситуации стандартны. Мы предлагаем рассмотреть некоторые практические ситуации, которые могут возникнуть в рамках вашей организации.

***Владимир САМОСЕЙКО**, юрист, магистр права*

Одной из таких ситуаций может являться **размещение информации о работниках организации здравоохранения на сайте организации**. В данном случае возникает вопрос: насколько правомерно брать согласие работника и необходимо ли вообще его брать?

Разберем ситуацию с учетом норм действующего законодательства.

На сайте организации здравоохранения могут быть размещены фото работников с указанием их фамилии, имени и отчества, наименования должности и квалификационных характеристик.

РАЗМЕЩЕНИЕ ИНФОРМАЦИИ НА САЙТЕ: СИТУАЦИЯ 1

Размещение на сайте организации здравоохранения фотографий работников с указанием их фамилии, имени, отчества, наименования должности, квалификационных характеристик и др. фактически **должно быть отнесено к распространению персональных данных**, которое на практике нередко путают **с предоставлением таких данных**.

В таблице приведено сравнение двух форм передачи персональных данных согласно ст. 1 Закона.

Таблица

Сравнение двух форм передачи персональных данных

Критерии сравнения	Предоставление ПД	Распространение ПД
Определение	Действия, направленные на ознакомление с ПД определенного лица или круга лиц	Действия, направленные на ознакомление с персональными данными неопределенного круга лиц
Кому предоставляются ПД	Изначально определенным лицам (т. е. узкому, заранее определенному и контролируемому кругу лиц)	Неопределенному кругу лиц (т. к. фактически передаваемые персональные данные выходят из-под сферы контроля)
Правовой результат передачи ПД	Конфиденциальный характер персональных данных сохраняется, правовое основание для обработки персональных данных оператором, получившим их, определяется в зависимости от цели обработки и их состава	Персональные данные в таком случае меняют свою правовую форму: из конфиденциальных они становятся общедоступными персональными данными (т. е. уже не конфиденциальными)

Таким образом, распространение ПД без согласия субъекта персональных данных (работника организации) возможно **только в случаях, предусмотренных законодательством**. При этом необходимо различать цели распространения таких данных.

ЦЕЛИ РАСПРОСТРАНЕНИЯ

К целям распространения ПД можно отнести:

- выполнение требований законодательства (общедоступные данные);
- информационные цели в рамках трудовых отношений.

Выполнение требований законодательства

В данном случае размещение фотографий работников с указанием их фамилии, имени, отчества (при наличии такового) на сайте организации здравоохранения может быть организовано в рамках исполнения ст. 5 и 22[1] Закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации».

Справочно: *так, на интернет-сайте государственной организации здравоохранения размещаются сведения о руководителе и его заместителях (должность, фамилия, собственное имя, отчество (при его наличии), номер служебного телефона).*

В рамках трудовых отношений

Также размещение фотографий работников с указанием их ФИО на сайте организации здравоохранения может быть осуществлено в информационных целях в рамках трудовых отношений.

Согласно п. 2.3 Рекомендаций Национального центра защиты персональных данных (далее — НЦЗПД) размещение фотографии работника на сайте организации здравоохранения в информационных целях в рамках трудовых отношений может быть обусловлено **необходимостью рационально организовать труд работников, в должностные обязанности** которых входит активное контактирование с внешним контуром организации.

В каждом конкретном случае наниматель самостоятельно оценивает, насколько публичен может быть работник в силу порученных ему трудовых обязанностей.

Поэтому при ознакомлении работника с поручаемой работой важно заранее проинформировать его о возможности размещения его фотографий на сайте организации здравоохранения в информационных целях в рамках трудовых отношений, что обусловлено ст. 6 Закона.

ОРГАНИЗУЕМ ПОЕЗДКУ ДЛЯ РАБОТНИКОВ: СИТУАЦИЯ 2

Следующей ситуацией, которая может возникнуть на практике, является **направление группы работников в корпоративную поездку**, например, организуемую профсоюзом.

Нужно ли согласие работников при подготовке такой поездки (бронирование гостиницы, транспорт и т.д.)?

Правовое основание

В такой ситуации основанием для обработки персональных данных будет являться договор с субъектом персональных данных (ст. 6 Закона) или согласие работника – члена профсоюза.

Профсоюз: оператор или уполномоченное лицо?

Согласно абз. 8 ст. 1 Закона оператором признается юридическое лицо Республики Беларусь, самостоятельно или совместно с иными определенными данным Законом лицами организующее и (или) осуществляющее обработку персональных данных.

В свою очередь, исходя из положений ст. 1 и 2 Закона Республики Беларусь от 22.04.1992 № 1605-XII «О профессиональных союзах» (в ред. от 13.07.2016) профессиональный союз — это **добровольная общественная организация**, объединяющая граждан для защиты трудовых, социально-экономических прав и интересов.

Справочно: *при этом профсоюз и его организационные структуры в соответствии с законодательством и их уставами являются юридическими лицами.*

Таким образом, профсоюз, как юридическое лицо, является самостоятельным (отдельным) оператором, который, как и все иные операторы, должен предпринять меры по защите персональных данных, предусмотренные ст. 16 и 17 Закона.

ЛИЧНАЯ ИНФОРМАЦИЯ РАБОТНИКА: СИТУАЦИЯ 3

Следующая ситуация может возникнуть при обработке личной информации, которая не связана с трудовой деятельностью. Нужно ли согласие на обработку такой информации?

Необходимо отметить, что в данном случае **требуется получение согласия работника**.

В силу п. 2.6 Рекомендаций НЦЗПД обработка личной информации работника, не связанной с исполнением трудовых обязанностей, **не может рассматриваться как обработка в процессе трудовой (служебной) деятельности** в соответствии с абз. 8 ст. 6 и абз. 3 п. 2 ст. 8 Закона.

К подобной **личной информации** относятся (за исключением случаев, когда предоставление нижеперечисленной информации связано с осуществлением трудовой (служебной) деятельности):

- личные адреса электронной почты;
- аккаунты в социальных сетях;
- религиозные взгляды;
- участие в общественной деятельности;
- сведения о родственниках и др.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ КАНДИДАТОВ ПРИ ПРИЕМЕ НА РАБОТУ: НА ЧТО ОБРАТИТЬ ВНИМАНИЕ

В организации здравоохранения обрабатываются персональные данные не только пациентов, работников, но и кандидатов, которые потенциально могут быть приняты на работу в эту организацию. Вопрос обработки персональных данных кандидатов при приеме на работу сложный и неоднозначный. Далее мы проанализируем для вас информацию по этому вопросу.

Алёна ПОТОРСКАЯ, *ведущий юрист REVERA, руководитель проектов в сфере защиты персональных данных*

Ольга ОПИМАХ, *юрист REVERA*

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон) **не предусматривает** специального основания для обработки персональных данных кандидатов, так как трудовые отношения с кандидатами на этапе подачи анкеты или собеседования

еще не возникают. Иных требований законодательства, влекущих обработку персональных данных таких субъектов, также нет.

В качестве ключевого основания для обработки персональных данных Закон предусматривает **согласие субъекта**. Вместе с тем в ст. 6 и 8 (специальные персональные данные) Закона содержится перечень случаев, когда получение согласия субъекта на обработку его персональных данных не требуется.

Так, согласно ст. 6 Закона, если учитывать специфику поднимаемого вопроса, **согласие не требуется**, в частности:

- при оформлении трудовых отношений, а также в процессе трудовой деятельности субъекта персональных данных в случаях, предусмотренных законодательством;
- при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа;
- в отношении ранее распространенных персональных данных до момента заявления субъектом персональных данных требования о прекращении обработки или их удалении.

На каком же основании можно обрабатывать персональные данные кандидатов при приеме на работу? Давайте разбираться.

ОСНОВАНИЯ ДЛЯ ОБРАБОТКИ

Основания для обработки персональных данных кандидатов будут зависеть от того, как организация здравоохранения получает персональные данные кандидатов.

Рекрутинг в организации здравоохранения может осуществляться по следующим сценариям:

- организация размещает вакансии, на которые откликаются кандидаты;
- организация самостоятельно ищет работников (например, через социальную сеть для поиска и установления деловых контактов LinkedIn) и связывается с кандидатами по своей инициативе;
- организация осуществляет поиск кандидатов через кадровые агентства.

Далее мы рассмотрим наш вопрос в рамках каждого из указанных сценариев и прокомментируем их с точки зрения Закона, а также с учетом иностранной практики защиты персональных данных.

Отклик поступил от кандидата

В данном случае нужно учитывать, что отклик от кандидата может поступить различными способами.

1-й способ: кандидат откликается через сайт организации

Если у организации здравоохранения имеется сайт, где предусмотрена возможность заполнения заявки онлайн, то субъект может выразить согласие на обработку его персональных данных через **проставление отметки** на интернет-ресурсе (например, галочки в чек-боксе под формой заявки).

При этом организации здравоохранения необходимо помнить, что она обязана предоставить кандидату ряд сведений.

Справочно: *перечень сведений, которые должны быть предоставлены субъекту персональных данных до запроса его согласия на обработку, включает:*

- *наименование и место нахождения (адрес места пребывания) оператора;*
- *цели обработки персональных данных;*
- *перечень персональных данных, на обработку которых дается согласие;*
- *срок, на который дается согласие;*
- *информацию об уполномоченных лицах в случае, если обработка персональных данных будет осуществляться такими лицами;*
- *перечень действий с персональными данными, на совершение которых дается согласие;*
- *общее описание используемых оператором способов обработки персональных данных;*
- *иную информацию, необходимую для обеспечения прозрачности процесса обработки персональных данных.*

Организация здравоохранения **не имеет права запрашивать** у кандидата данные, которые не связаны с оценкой его соответствия требованиям вакансии, например, банковские данные, а цели обработки персональных данных кандидата должны быть ***ограничены оценкой соответствия кандидата требованиям вакансии***.

В данном случае получение согласия может происходить следующим образом: в форме для отправки заявки можно разместить *чек-бокс* (который не должен быть заранее отмечен), где субъект сможет выразить свое согласие.

При этом необходимо предоставить субъекту доступ к информации, предусмотренной п. 5 ст. 5 Закона.

Такой доступ может быть обеспечен путем размещения:

- отдельного уведомления, которое содержит соответствующую информацию;
- гиперссылки на отдельный документ (согласие на обработку персональных данных либо политику обработки персональных данных).

2-й способ: кандидат связывается с организацией по иным каналам (например, через электронную почту, по телефону)

Здесь важно понимать, что сам по себе факт отправки заявки не является выражением согласия с точки зрения Закона, поскольку согласие субъекта — это «свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных».

Когда кандидат откликается на вакансию (направляет потенциальному нанимателю свое резюме, оставляет контактные данные для связи и т.д.), у него нет всей необходимой информации о том, как будет осуществляться обработка его персональных данных (какой объем персональных данных и для каких целей будет обрабатываться, как долго будут храниться его персональные данные и кому они могут передаваться).

*В данном случае необходимо **запросить** согласие. Как вариант — направить кандидату ответ на его письмо с указанием всей необходимой информации в соответствии со ст. 5 Закона, а также попросить кандидата подтвердить, согласен ли он на обработку его персональных данных в соответствии с предоставленной информацией.*

В странах ЕС в соответствии с General Data Protection Regulation 2016/679 (GDPR) обработка данных кандидатов может осуществляться на основании легитимного интереса, основанного на балансе интересов сторон (соответственно, нет необходимости получать согласие кандидата). Так, легитимный интерес нанимателя заключается в необходимости провести оценку кандидата на предмет соответствия требованиям вакансии,

а легитимный интерес кандидата — в возможности установления трудовых отношений.

В нашей стране такого основания, как легитимный интерес, Закон **не предусматривает**.

Организация сама ищет кандидатов и связывается с ними

Организация здравоохранения может самостоятельно искать работников, например через социальную сеть для поиска и установления деловых контактов, и связываться с кандидатами по своей инициативе.

В случае, когда персональные данные были опубликованы самим субъектом в социальной сети или на иных интернет-площадках, они будут рассматриваться как общедоступные.

Из анализа норм Закона следует, что если субъектом не было заявлено требований о прекращении обработки или удалении распространенных персональных данных, согласие на их обработку не требуется. Соответственно, если кандидат разместил свое резюме на интернет-ресурсе, организация здравоохранения, заинтересованная в этом кандидате, может начать обработку персональных данных без запроса его согласия.

Однако важно помнить, что обработка общедоступных персональных данных также должна соответствовать общим требованиям к обработке персональных данных, закрепленным в ст. 4 Закона. Такая обработка должна ограничиваться достижением конкретных, заранее заявленных законных целей, а также обеспечивать справедливое соотношение интересов сторон.

МНЕНИЕ АВТОРА

По нашему мнению, если субъект персональных данных опубликовал свое резюме в сети, предназначенной для поиска работы, он предполагает, что данные, размещенные в такой сети, будут использоваться для целей, связанных с потенциальным трудоустройством. Соответственно, обработка данных, размещенных на интернет-ресурсе, предназначенном для поиска работы, для целей установления контакта с кандидатами, не будет являться нарушением Закона.

Подход Российской Федерации к использованию общедоступных данных представляется более формальным. Так, с 1 марта 2021 г. вступили в силу

изменения в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», а с 1 сентября 2021 г. начал действовать приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». Согласно этим изменениям оператор перед обработкой данных, полученных из открытых источников (социальные сети, сайты по поиску работы), теперь должен ***проверять наличие согласия или другого основания для обработки таких сведений***. Для этого стоит уточнять у владельцев job-сайтов, есть ли согласие на распространение персональных данных и для каких целей оно получено у соискателя. Кроме того, оператор должен доказать законность сбора и последующего использования данных кандидатов из открытых источников.

Поиск кандидатов осуществляют агентства

Как правило, кадровое агентство совершает обработку персональных данных от своего имени и самостоятельно определяет порядок такой обработки. Соответственно, по смыслу Закона оно выступает оператором персональных данных и на нем лежит обязанность получения согласия кандидата на обработку его персональных данных.

Вместе с тем важно понимать, что кадровое агентство не может предусмотреть, как сама организация здравоохранения будет осуществлять обработку персональных данных кандидата (как долго будет хранить данные, кому данные будут передаваться и т.д.).

МНЕНИЕ АВТОРА

По нашему мнению, когда организация здравоохранения начинает самостоятельно осуществлять обработку переданных кадровым агентством данных кандидата (к примеру, приглашает кандидата на собеседование), то именно организация здравоохранения обязана получить согласие кандидата на дальнейшую обработку его персональных данных, предоставив ему всю необходимую информацию.

ПРОВЕДЕНИЕ СОБЕСЕДОВАНИЯ И ДЕЙСТВИЕ ЗАКОНА

Возникает вопрос: если после рассмотрения заявки организация здравоохранения приглашает кандидата на собеседование, подпадает ли сбор данных о кандидате в ходе собеседования под требования Закона?

Согласно п. 1 ст. 2 Закона Закон регулирует отношения, связанные с защитой персональных данных при их обработке, осуществляемой:

- с использованием средств автоматизации;
- без использования средств автоматизации, если при этом обеспечиваются поиск персональных данных и (или) доступ к ним по определенным критериям (картотеки, списки, базы данных, журналы и др.).

МНЕНИЕ АВТОРА

Например, база записей собеседований, сгруппированная по именам или хронологически, скорее всего, будет подпадать под требования Закона. Поэтому, если организация здравоохранения обрабатывает данные одним из вышеперечисленных способов, такая обработка должна соответствовать требованиям Закона.

ЗАКЛЮЧЕНИЕ

К вопросу обработки персональных данных кандидатов необходимо подходить ответственно, так как нарушение этого порядка может повлечь за собой неблагоприятные последствия в виде административной и уголовной ответственности.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВИДЕОНАБЛЮДЕНИИ

Большинство организаций здравоохранения оборудованы средствами системы видеонаблюдения. Системы видеонаблюдения могут быть установлены и в помещении регистратуры, и в холле организации, и в кабинете руководителя. Далее расскажем, как быть с организацией видеонаблюдения ввиду вступления в силу Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее – Закон).

Матвей ГОРОДНИК, *юрист Borovtsov & Salei*

Обработка персональных данных (далее — ПД) при ведении видеонаблюдения в организации имеет свою специфику. Рассмотрим, в чем она заключается.

Согласно абз. 2 и 12 ст. 1 Закона данные с записей камер видеонаблюдения, а именно изображения физических лиц, могут являться биометрическими ПД и, соответственно, специальными ПД.

Справочно: *к обработке таких ПД ст. 8 Закона предъявляет особые требования.*

Важно разграничить две ситуации при осуществлении видеонаблюдения:

1) видеонаблюдение за посетителями, пациентами (клиентами) организации здравоохранения;

2) видеонаблюдение за работниками организации здравоохранения.

Именно такое разделение имеет существенное значение для определения порядка работы с ПД в организации.

ВИДЕОНАБЛЮДЕНИЕ ЗА ПАЦИЕНТАМИ (КЛИЕНТАМИ)

Рассмотрим вопрос о правовом основании для обработки ПД посетителей, пациентов (клиентов) при осуществлении видеонаблюдения.

МНЕНИЕ АВТОРА

Полагаем, что применять общее правило об обработке ПД на основании согласия субъекта персональных данных (абз. 1 п. 3 ст. 4, п. 1 ст. 8 Закона) к рассматриваемой ситуации было бы нелогично.

Это обусловлено тем, что взять согласие субъекта ПД на ведение видеонаблюдения у каждого посетителя едва ли возможно. Также нужно учесть, что субъект ПД вправе в любой момент отозвать свое согласие (ст. 10 Закона), что не позволит оператору (которым в данном случае выступает организация здравоохранения) в дальнейшем обрабатывать его ПД.

Пунктом 2 ст. 8 Закона предусмотрены случаи обработки специальных ПД **без согласия субъекта**.

Проблема заключается в том, что указанные случаи ***не всегда можно применить для ситуации с видеонаблюдением за посетителями.***

Иногда обработка таких ПД необходима для выполнения обязанностей (полномочий), предусмотренных законодательными актами (абз. 16 п. 2 ст. 8 Закона).

Например, обязанность по организации видеонаблюдения может быть предусмотрена нормами:

- Указа Президента Республики Беларусь от 28.11.2013 № 527 «О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка» (в ред. от 20.05.2021);
- постановления Совета Министров Республики Беларусь от 30.12.2013 № 1164 «О критериях отнесения объектов к числу подлежащих обяза-

тельному оборудованию средствами системы видеонаблюдения за состоянием общественной безопасности» (в ред. от 28.07.2021, далее — постановление № 1164).

Справочно: *к примеру, система видеонаблюдения за состоянием общественной безопасности обязательна для объектов с возможностью единовременного массового пребывания граждан в количестве 100 и более человек, а также в организациях здравоохранения (пп. 2, 6 приложения к постановлению № 1164).*

Возникает вопрос: что делать в случае, если объект не подлежит обязательному оборудованию средствами системы видеонаблюдения?

Национальное законодательство в настоящее время не регулирует данный вопрос. Поэтому необходимо обратиться к международному опыту – в других странах подобные вопросы защиты ПД возникли значительно раньше.

Российский опыт

В Российской Федерации действует специальная норма, легализующая возможность обработки таких данных ***без согласия гражданина***. Так, в соответствии с абз. 2 ч. 1 ст. 152.1 Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ (далее – ГК РФ) согласие на получение и использование изображения гражданина **не требуется**, когда такое изображение получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования.

Справочно: *норма абз. 2 ч. 1 ст. 152.1 ГК РФ касается не согласия на обработку ПД по смыслу законодательства о защите ПД, а согласия на получение и использование изображения гражданина как сделки по смыслу гражданского законодательства (п. 46 постановления Пленума Верховного Суда РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации»).*

Применительно к законодательству о защите ПД существует подход, согласно которому в рассматриваемой ситуации такое законодательство вообще неприменимо. Так, при ведении видеонаблюдения за посетителями ***их идентификации не происходит***, а основная цель такого видеонаблюдения — обеспечение соблюдения общественного порядка и сохран-

ности имущества организации. Такой подход отражен в разъяснениях Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор) от 02.09.2013 «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки».

Указанные разъяснения стали неактуальными на основании письма Роскомнадзора от 19.11.2021 № 09-78548. Иных разъяснений в этой сфере Роскомнадзор пока ***не давал****.*

Так, в данных разъяснениях указывалось, что до передачи материалов видеосъемки в публичных местах и на охраняемой территории для установления личности снятого человека они **не являются биометрическими ПД**, обработка которых регулируется общими положениями Федерального закона «О персональных данных». Это связано с тем, что такие данные не используются оператором (владельцем видеокамеры или лицом, организовавшим ее эксплуатацию) для установления личности.

Справочно: *однако указанные материалы, используемые органами, осуществляющими оперативно-розыскную деятельность, дознание и следствие в рамках проводимых мероприятий, являются биометрическими ПД в случае, если цель их обработки — установление личности конкретного физического лица.*

Возможно, такой подход может быть использован и в Беларуси. Ведь с учетом абз. 2 ст. 1 Закона биометрические ПД — это 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 др.). Следовательно, если такие данные не используются «для уникальной идентификации», действие Закона не распространяется на эти отношения.

МНЕНИЕ АВТОРА

Таким образом, если система видеонаблюдения необходима исключительно для обеспечения общественного порядка и сохранности имущества организации или иных аналогичных целей, а не для идентификации посетителей,

*согласие субъекта ПД получать **не обязательно**, равно как и искать иное основание для обработки таких данных.*

В случае, если записи с камер видеонаблюдения будут переданы правоохранительным органам, а они будут осуществлять идентификацию посетителя (например, идентифицировать лицо, которое совершило административное правонарушение), будет действовать специальное основание для обработки ПД, исключающее необходимость получать согласие (абз. 7 п. 2 ст. 8 Закона).

В то же время, если камеры видеонаблюдения используются для идентификации посетителей (например, для того, чтобы распознавать предпочтения конкретного пациента, клиента), нормы Закона подлежат применению. В этой ситуации при отсутствии иных оснований, предусмотренных п. 2 ст. 8 Закона, применению подлежит **общее правило об обработке ПД** на основании согласия.

Цели использования видеонаблюдения рекомендуется детально описывать в соответствующем локальном правовом акте организации.

Европейский опыт

В Европейском союзе сформировался несколько иной подход. Так, в пп. 7 и 8 Руководящих принципов обработки персональных данных с помощью видеоустройств Европейский совет по защите данных (EDPB) указал, что по общему правилу записи камер видеонаблюдения **позволяют идентифицировать личность**, в связи с чем нормы Общего регламента защиты персональных данных (General Data Protection Regulation, GDPR) применяются к видеонаблюдению.

При этом GDPR не распространяется на обработку данных, которые не относятся к субъекту ПД, т.е. если его личность не может быть идентифицирована прямо или косвенно.

***Справочно:** в качестве примера таких случаев названо использование муляжей видеокамер или видеокамер в автомобиле для помощи при парковке.*

Однако GDPR закрепляет такое правовое основание обработки ПД, отсутствующее в белорусском законодательстве, как **легитимный интерес**. Именно это основание обычно используется при обработке ПД в рамках

видеонаблюдения. При текущем правовом регулировании в Беларуси перенять такой подход представляется проблематичным.

ВИДЕОНАБЛЮДЕНИЕ ЗА РАБОТНИКАМИ

В случае организации видеонаблюдения за работниками также возникает вопрос о правовом основании для обработки их ПД.

МНЕНИЕ АВТОРА

Представляется, что основание, предусмотренное абз. 3 п. 2 ст. 8 Закона, а именно обработка ПД при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта ПД в случаях, предусмотренных законодательством, не подходит к рассматриваемой ситуации, поскольку в законодательстве не установлены случаи, когда в рамках трудовых правоотношений необходимо видеонаблюдение.

Исключение может составлять, пожалуй, только ситуация использования видеонаблюдения для целей контроля и учета рабочего времени. Так, согласно п. 3 ч. 1 ст. 55 ТК при организации труда работников наниматель обязан вести учет фактически отработанного работником времени.

Также руководителю нужно помнить, что в соответствии с п. 2 ст. 4 Закона обработка ПД должна быть соразмерна заявленным целям их обработки и обеспечивать на всех этапах такой обработки справедливое соотношение интересов всех заинтересованных лиц.

Иные основания (за исключением случаев, когда объект подлежит обязательному оборудованию средствами системы видеонаблюдения), предусмотренные п. 2 ст. 8 Закона, также едва ли возможно применить при видеонаблюдении за работниками.

МНЕНИЕ АВТОРА

Таким образом, полагаем, что при видеонаблюдении за работниками следует брать их согласие на обработку ПД (кроме случаев, отмеченных ранее, когда, к примеру, согласно постановлению № 1164 в организациях здравоохранения видеонаблюдение обязательно), поскольку нанимателем будет проводиться их идентификация (например, для контроля за недобросовестным выполнением служебных обязанностей или неправомерным использованием имущества нанимателя в личных целях).

ЗАКЛЮЧЕНИЕ

Руководителю организации здравоохранения нужно учитывать необходимость истребования согласия в каждом случае индивидуально. Но при этом следует иметь в виду, что выбор надлежащего правового основания для обработки ПД работников не единственная забота. Необходимо помнить про обязанности оператора согласно ст. 16 Закона, а также про обязательные меры по обеспечению защиты ПД в соответствии с п. 3 ст. 17 Закона.

УДАЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: ВСЕГДА ЛИ ОНО НЕОБХОДИМО?

Обработка персональных данных не может осуществляться бесконечно. Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон) предусматривает возможность отзыва согласия субъекта на обработку персональных данных, что влечет их последующее удаление.

Как же организовать процесс удаления? И всегда ли данные необходимо удалять? Об этом мы расскажем далее.

Владимир САМОСЕЙКО, *юрист, магистр права*

Закон предусматривает именно понятие **«удаление персональных данных»** (далее — ПД). Так, согласно абз. 15 ст. 1 Закона удаление персональных данных — действия, 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.

Справочно: *на практике чаще все же можно слышать про «уничтожение». Если исходить из определения, которое приведено выше, то получается, что «уничтожение» – более узкое понятие, чем «удаление», и касается только материальных носителей ПД. На наш взгляд, это равнозначные термины.*

Из анализа ст. 10 и 13 Закона можно сделать вывод, что в общем случае оператор обязан прекратить обработку и уничтожить ПД в срок, не превышающий **15 дней** с даты достижения цели обработки ПД.

ПРИМЕР

Например, в ноябре 2021 г. работник обратился к нанимателю за материальной помощью в связи с необходимостью оплатить его лечение в январе 2022 г. и представил копии медицинских документов, а также справку о проживающих с ним иждивенцах. При этом решение о предоставлении материальной помощи принято руководителем в ноябре 2021 г., а выплата денежных средств была произведена в январе 2022 г. Полагаем, что датой достижения цели обработки будет являться ***день перечисления денег работнику****.*

Однако перед уничтожением документа необходимо четко понять, действительно ли данный документ подлежит уничтожению. Как это сделать?

АНАЛИЗ ДОКУМЕНТОВ

Рассмотрим ситуацию на примере документов соискателей, которых не приняли на работу.

Резюме

На собеседование соискателя пригласят, скорее всего, на основании резюме. В этом документе есть информация, по которой наниматель сделает выбор либо откажет в приеме на работу.

Справочно: *получать согласие на обработку резюме не нужно, если:*

- *документ получен от кандидата;*
- *кандидат опубликовал его в общем доступе на сайтах по поиску работы;*
- *резюме получено от кадрового агентства, которое действует от имени соискателя.*

Анкета соискателя

Если на собеседовании кандидату необходимо заполнять анкету, то для этого нужно оформить письменное согласие на обработку ПД, которые он изложит в анкете.

Нередко такая анкета содержит вопросы, которые не имеют отношения к деловым и профессиональным качествам, например о близких родственниках.

Справочно: *как правило, получение информации о родственниках и заполнение анкеты без получения согласия возможно только лишь при приеме на государственную службу, поскольку там анкета является обязательным документом.*

Иные документы

К иным документам можно отнести:

- сведения из государственной базы данных о правонарушениях (в отношении некоторых категорий работников);
- декларацию о доходах (входит в перечень обязательных документов для назначения на ряд должностей);
- медицинскую справку.

КАКИЕ ДОКУМЕНТЫ СОИСКАТЕЛЕЙ УНИЧТОЖАТЬ, А КАКИЕ СДАВАТЬ В АРХИВ?

Если при найме персонала организацией здравоохранения используется внешний кадровый резерв, то, возможно, придется хранить личные документы соискателей **дольше установленного срока**.

Для этого можно разработать локальные правовые акты о кадровом резерве и закрепить в них перечень личных документов соискателей, а также порядок и сроки их обработки до уничтожения или передачи в архив.

Важно понимать, что в данном случае вам придется обосновать необходимость обработки каждого документа и предоставить согласие на обработку всех персональных данных «резервистов».

Документы соискателей, которым вы отказали в найме или которых не включили в кадровый резерв, можно уничтожать в установленный срок. При уничтожении резюме, анкет или копий личных документов проблем возникнуть не должно, а вот если у вас остались некоторые оригиналы документов, например справки об отсутствии судимости, если они требуются для приема на работу, то их лучше попытаться вернуть владельцу или же передать в архив.

А что же с документами работника, который уже принят на работу?

КАКИЕ ДОКУМЕНТЫ РАБОТНИКОВ МОЖНО ХРАНИТЬ?

Перечня документов работников, которые можно хранить, законодательством **не предусмотрено**.

Справочно: *законодатель только лишь отмечает обязанность нанимателя хранить трудовую книжку.*

По каждому документу, который вы получили от работника, задайте себе два вопроса (так же как и в отношении копий документов):

1. Зачем нам нужен этот документ: можно ли обойтись без него, когда оформляем кадровые документы, предоставляем работнику гарантии и компенсации? Может быть, эти сведения уже есть в учетных документах и их достаточно?

2. Как долго нам нужен этот документ: может быть, мы все уже выполнили, предоставили работнику и больше обращаться к документу не будем?

Если вы ответили «да» хотя бы на один из вопросов, верните работнику документ или уничтожьте его. Как это сделать, мы расскажем далее.

Отдельное внимание нужно уделить личным делам работников. Их необходимо проанализировать и проверить каждый документ. Решить, какие документы можно или нельзя оставить в личном деле.

В составе личных дел или в отдельных папках с документами по личному составу вы можете хранить документы работников, которые связаны с работой: о приеме на работу, ежедневной работе и увольнении.

Закон требует, чтобы вы обрабатывали только такую информацию о работнике, которая **обязательна** для трудовых отношений. Это значит, что вы должны доказать, что сведения в личных документах работников нужны организации, чтобы:

- соблюдать требования законодательства;
- содействовать работникам в трудоустройстве, получении образования и продвижении по службе;
- обеспечивать личную безопасность работников и сохранность имущества;
- контролировать количество и качество работы.

Примерный анализ личного дела работника*

Без опасений можно хранить в отделе кадров те документы, которые работник **заполнил сам**, даже если они содержат биографические данные. Например, при приеме на работу вы просите составить автобиографию. Или же новый работник заполняет для вас анкету и отвечает на вопросы, в т.ч. личного характера, например, о составе семьи, наличии иждивенцев и др.

КАК ВЕРНУТЬ РАБОТНИКУ ИЛИ УНИЧТОЖИТЬ ДОКУМЕНТЫ, КОТОРЫЕ ВЫ НЕ МОЖЕТЕ ХРАНИТЬ?

Вы должны вернуть работникам документы или их копии, если они не связаны с работой или вы достигли цели обработки персональных данных.

Не копируйте документы работников — это почти никогда не требуется. Незаверенная копия не имеет юридической силы документа, но сведения в ней от этого не теряют своего значения.

В копиях также содержится конфиденциальная информация, за хранение которой вы отвечаете. Целесообразнее брать сведения из оригиналов документов и тут же отдавать их работникам.

ПРИМЕР 1

При приеме на работу работник предъявил паспорт, диплом, военный билет. Правильнее проверить документы, внести данные в личную карточку и трудовой договор и сразу отдать документы работнику.

Если вы сделали копии документов работника, чтобы предоставить ему гарантии по законодательству, ЛПА, не храните их в отделе кадров. Верните их работнику, как только достигнете цели, для которой получали сведения, т.е. предоставите работнику гарантии или компенсации.

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

*Если работник откажется забрать копии документов или вы не сможете с ним связаться, **уничтожьте копии** документов с ПД.*

ПРИМЕР 2

Работница просит предоставить ей отпуск по уходу за ребенком и назначить пособие. К заявлению она приложила:

- *копию свидетельства о рождении ребенка;*
- *справку с работы мужа о том, что он не использует отпуск и не получает пособие.*

Необходимо проверить документы и оформить приказ о предоставлении отпуска, передать документы в бухгалтерию (при этом нужно проконтролировать, чтобы в бухгалтерии документы работницы снова не скопировали). После того как бухгалтер передаст документы в ФСЗН для возмещения расходов на выплату пособия по уходу за ребенком, необходимо передать эти копии документов работнице. Если же с ней не получится связаться или работница откажется забирать копии, следует их уничтожить.

Если вы все-таки пришли к тому, что документы подлежат уничтожению, нужно учитывать ряд факторов при уничтожении документов, которые содержат ПД.

СПОСОБЫ УНИЧТОЖЕНИЯ

Процесс уничтожения носителей с ПД зависит от типа носителя данных.

Бумажные носители

Персональные данные на бумажных носителях следует уничтожать путем измельчения. При этом измельчить нужно так, чтобы потом информацию нельзя было восстановить.

Измельчите документы с помощью шредера либо передайте их на переработку организациям, которые собирают вторсырье, т.е. в пункты приема макулатуры.

Машиночитаемые носители

Чтобы уничтожить персональные данные на машиночитаемых носителях, таким носителям нужно нанести неустранимое повреждение. Повреждение должно исключить возможность использовать носители, а также восстановить данные. Для этого можно деформировать носитель и нарушить его целостность.

Жесткий диск

Файлы с персональными данными, которые содержатся на жестком диске, нужно удалить средствами операционной системы компьютера. Когда допускается повторное использование носителя CD-RW, DVD-RW, то для уничтожения лучше применить программное удаление содержимого диска. Для этого можно отформатировать диск, а затем записать на данный носитель новую информацию.

АЛГОРИТМ УДАЛЕНИЯ ПД

Для того, чтобы грамотно организовать работу, связанную с удалением ПД, мы предлагаем следующий алгоритм действий.

ШАГ 1. РАЗРАБАТЫВАЕМ ЛПА ОБ УНИЧТОЖЕНИИ ПД

Порядок удаления ПД может быть прописан в Положении об обработке ПД, а также это может быть отдельное положение. В таком ЛПА нужно закрепить:

- в каких случаях наниматель (оператор) уничтожает ПД;
- какие способы уничтожения ПД необходимо использовать.

Примерный образец Положения об уничтожении (удалении) персональных данных*

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ШАГ 2. ОПРЕДЕЛЯЕМ ДОКУМЕНТЫ, КОТОРЫЕ НУЖНО УНИЧТОЖИТЬ

Исходя из Закона оператор обязан прекратить обработку ПД и уничтожить их в следующих случаях:

- по истечении срока хранения;
- по достижении цели обработки персональных данных.

Какие документы подлежат уничтожению, необходимо анализировать в каждом конкретном случае отдельно. После того, как перечень таких документов установлен, можно переходить к следующему шагу.

ШАГ 3. СОЗДАЕМ КОМИССИЮ ПО УНИЧТОЖЕНИЮ ПД

Не рекомендуем принимать решение об уничтожении ПД и их носителей единолично. Для этого целесообразно создать в организации специальную комиссию посредством издания соответствующего приказа.

В состав комиссии, как правило, входят председатель и как минимум еще два работника. Желательно включить в состав комиссии работника, ответственного за обработку документов, которые планируется уничтожить. Комиссия составляет перечень документов для уничтожения с учетом сроков их хранения.

Примерный образец приказа о создании комиссии по уничтожению персональных данных*

ШАГ 4. ФИКСИРУЕМ ФАКТ УНИЧТОЖЕНИЯ ПД

При комиссионном уничтожении персональных данных, как правило, составляется соответствующий акт.

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

В акте об уничтожении персональных данных можно отразить следующие сведения:

- когда было проведено уничтожение;
- кто несет ответственность за верность процедуры;
- количество и виды уничтоженных носителей;
- каково было основание для уничтожения, какой применялся способ.

Руководитель организации здравоохранения вправе провести самостоятельную оценку результатов ликвидации источников информации в тех случаях, когда он посчитает это нужным.

Примерный образец акта об уничтожении материальных носителей персональных данных*

ШАГ 5. ВЕДЕМ УЧЕТ ФАКТОВ УНИЧТОЖЕНИЯ ПД

Рекомендуется отражать в специальном журнале или акте, что были уничтожены документы, которые содержат ПД.

Справочно: *унифицированных форм акта и журнала нет, их утверждает сам наниматель.*

В журнале или акте можно указать:

- *какие документы были уничтожены;*
- *когда документы были уничтожены;*
- *способ уничтожения.*

Примерный образец журнала регистрации удаления персональных данных*

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПД: УПОЛНОМОЧЕННЫЕ ОРГАНЫ, ПОРЯДОК ПРОВЕДЕНИЯ, МЕРЫ ВОЗДЕЙСТВИЯ

Контроль за исполнением норм законодательства, затрагивающего вопросы защиты ПД, закреплен в нашей стране на законодательном уровне. Мы собрали для вас информацию о том, кто может осуществлять такой контроль, каков порядок его проведения, какие акты могут быть вынесены по результатам проведения такого контроля и т.д.

Татьяна СОКОЛОВСКАЯ, *ведущий юрисконсульт государственного учреждения «Республиканский научно-практический центр онкологии и медицинской радиологии им. Н. Н. Александрова», старший преподаватель кафедры конституционного права юридического факультета БГУ*

Реализация норм Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных», а также разъяснения по вопросам применения законодательства о персональных данных и проведение иной разъяснительной работы осуществляются ***уполномоченным органом по защите прав субъектов персональных данных***. Согласно Указу Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных» (далее — Указ № 422) таким органом является **Национальный центр защиты персональных данных Республики Беларусь** (далее — НЦЗПД).

Пунктом 2 Указа № 422 утверждено Положение о Национальном центре защиты персональных данных (далее — Положение о НЦЗПД).

Справочно: *Национальный центр защиты персональных данных является юридическим лицом, создается и действует в форме государственного учреждения, имеет самостоятельный баланс, текущий (расчетный) и иные счета в банках, в том числе в иностранной валюте, печать и бланк с изображением Государственного герба Республики Беларусь и со своим наименованием, другие необходимые для осуществления своей деятельности печати, штампы и бланки, а также собственную символику.*

Почтовый адрес Национального центра защиты персональных данных Республики Беларусь: 220004, г. Минск, ул. К. Цеткин, д. 24, этаж 3. Телефон для справок: 367-07-90. Электронный ящик: info@cpd.by. Телеграм-канал: https://t.me/cpd_by.

Учредителем Национального центра защиты персональных данных и государственным органом, осуществляющим от имени Республики Беларусь права собственника имущества этого учреждения, является **Оперативно-аналитический центр при Президенте Республики Беларусь** (ч. 2 п. 4 Положения о НЦЗПД).

ПРАВОВОЕ ОБОСНОВАНИЕ ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ

Контроль за обработкой персональных данных операторами (уполномоченными лицами) внесен в п. 23 Указа Президента Республики Беларусь от 16.10.2009 № 510 (в ред. от 28.10.2021) (далее — Указ № 510). Если учесть, что п. 23 Указа № 510 отражает виды контроля, на которые Указ не распространяет свое действие, то можно сделать вывод, что Указ № 510 не распространяет свое действие при осуществлении контроля за обработкой персональных данных.

Указанный контроль осуществляется Национальным центром защиты персональных данных в форме:

- проверок, проводимых в соответствии с планом проверок соблюдения законодательства о персональных данных, ежегодно утверждаемым директором Национального центра защиты персональных данных и размещаемым на официальном сайте Национального центра защиты персональных данных в глобальной компьютерной сети Интернет не позднее 30 декабря года, предшествующего году проведения проверки (далее — плановые проверки);
- проверок, проводимых без включения в названный план (далее — внеплановые проверки);
- камеральных проверок (п. 13 Положения о НЦЗПД).

Если плановые проверки проводятся исключительно в соответствии с планом проверок, то внеплановая проверка проводится без включения в план. Как правило, такие проверки могут быть проведены 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.

В свою очередь камеральные проверки проводятся по решению НЦЗПД.

Особенности проведения каждой из таких проверок представлены в *таблице*.

Таблица

Особенности проведения контроля за обработкой ПД операторами

Критерии разграничения	Вид проверки		
	Плановые	Внеплановые	Камеральные
Место проведения	Как правило, по месту нахождения оператора		По месту нахождения НЦЗПД
Периодичность	Не чаще 1 раза в 2 года	–	Не установлена
Максимальный срок проведения проверки	20 рабочих дней		Не установлен
Максимальный срок продления	10 рабочих дней		Не установлен
Количество продлений	1 раз		Не регламентировано
Выдача предписания на проведение проверки	Предусмотрена		Не предусмотрена
Срок, в течение которого НЦЗПД должно быть направлено уведомление о назначении проверки	10 рабочих дней		Не предусмотрен

Критерии разграничения	Вид проверки		
	Плановые	Внеплановые	Камеральные
Орган, проводящий проверку	НЦЗПД (комиссия)		НЦЗПД (детальнее указанные вопросы Положением о НЦЗПД не урегулированы)
Способы и методы проведения проверки	Определяет руководитель комиссии самостоятельно		Посредством изучения, анализа и оценки информации в СМИ, сети Интернет и документов
Составление акта по результатам проверки	Предусмотрено		Не предусмотрено
Требования к акту	Составление в двух экземплярах. Отражение в акте:· • соответствия или несоответствия мер по обеспечению защиты ПД оператора требованиям законодательства; • экспертной оценки комиссией достаточности принятых мер для защиты ПД; • выявленных нарушений законодательства о персональных данных либо вывода об отсутствии таких нарушений		Не предусмотрено
Максимальный срок оформления акта по результатам проверки	10 рабочих дней		–
Максимальный срок вручения акта проверки	3 рабочих дня		–
Возможность представить обоснованные возражения	Предусмотрена		Не предусмотрена
Максимальный срок предоставления возражений со дня поступления акта	15 рабочих дней		Не установлен
Максимальный срок рассмотрения возражений	10 рабочих дней с момента поступления возражений		–
Возможность составления нового акта по результатам рассмотрения возражений	Предусмотрена		Не предусмотрена

ПРЕДПИСАНИЕ 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)**.

Предписание может быть:

- 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 шести месяцев.

Справочно: *предписание составляется в двух экземплярах. Первый экземпляр в течение трех рабочих дней после его составления направляется проверенному оператору (уполномоченному лицу) или вручается его уполномоченному представителю, второй — остается в НЦЗПД.*

Выполнение предписания оператором

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 НЦЗПД возможность удостовериться (в том числе на месте) в устранении нарушений (при необходимости).

Однако в некоторых случаях можно продлить сроки устранения нарушений, содержащихся в требовании (предписании).

Порядок продления сроков

Рассмотрим порядок продления сроков устранения нарушений в случае вынесения в отношении организации здравоохранения требования (предписания) и невозможности их устранения в установленные НЦЗПД сроки.

1. Подача заявления оператором

Основанием для продления сроков является именно заявление оператора (уполномоченного лица) с указанием объективных обстоятельств,

не позволивших устранить нарушения, указанные в письменном требовании (предписании), в установленные в нем сроки.

При этом нужно отметить, что такое заявление может быть подано не позднее трех рабочих дней до дня истечения сроков устранения нарушений.

2. Рассмотрение заявления

Лицом, уполномоченным принимать решение по заявлению, является директор НЦЗПД. Сроки принятия такого решения — **не позднее двух рабочих дней** со дня поступления заявления.

При этом стоит отметить, что решение может быть как в пользу оператора, так и наоборот.

3. Уведомление оператора

Как только решение принято, в течение двух рабочих дней оператор (уполномоченное лицо) будет уведомлен о нем в письменной форме.

Возобновление обработки ПД

Поскольку предписанием может быть предусмотрено приостановление обработки ПД, то необходимо рассмотреть, каким образом может быть возобновлена такая обработка.

В части вопроса возобновления нужно учитывать следующее:

- лицо, уполномоченное принимать решение, — директор НЦЗПД;
- срок принятия решения — в течение 10 рабочих дней после устранения нарушений;
- оператор (уполномоченное лицо) обязательно будет уведомлен в письменной форме в течение двух рабочих дней со дня принятия решения.

Обжалование предписания НЦЗПД

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***.

Справочно: *таким образом, можно сделать вывод, что основные подходы, закрепленные Положением о порядке организации и проведения проверок, утвержденным Указом № 510, применительно к плановым и внеплановым проверкам сохранены и использованы в Положении в отношении аналогичных мероприятий НЦЗПД.*

РЕЗУЛЬТАТЫ КАМЕРАЛЬНЫХ ПРОВЕРОК

Особенности принимаемых мер по результатам камеральных проверок состоят в том, что по результатам их проведения оператору (уполномоченному лицу) **могут быть** направлены **рекомендации** об устранении выявленных нарушений законодательства о персональных данных.

Таким образом, анализ норм законодательства позволяет сделать вывод, что направление рекомендаций **не является обязательным**.

Справочно: *порядок проведения камеральных проверок на законодательном уровне урегулирован недостаточно по сравнению с плановыми и внеплановыми проверками, в связи с чем в практике правоприменения возможно возникновение спорных ситуаций.*

ОСУЩЕСТВЛЕНИЕ КОНТРОЛЯ ПРИ ПОСТУПЛЕНИИ ЖАЛОБЫ

Порядок рассмотрения жалоб, направляемых заявителями в НЦЗПД, урегулирован главой 5 Положения о НЦЗПД.

Порядок рассмотрения жалоб физических лиц, направляемых в НЦЗПД, отличается от порядка рассмотрения жалоб и иных обращений, установленного Законом Республики Беларусь от 18.07.2011 № 300-З «Об обращениях граждан и юридических лиц» (в ред. от 17.07.2020, далее — Закон об обращениях).

Прежде всего это касается сроков рассмотрения жалоб. Письменные обращения в соответствии с Законом об обращениях рассматриваются в течение 15 дней (с возможностью продления до 1 месяца). Положение о НЦЗПД устанавливает ***месячный срок рассмотрения жалобы****.*

Срок в данном случае исчисляется со дня, следующего за днем регистрации жалобы в НЦЗПД. Пункт 31 Положения о НЦЗПД предусматривает, что в случае, если жалоба потребует дополнительного изучения и проверки, указанный срок может быть продлен НЦЗПД не более чем **на 1 месяц**. При этом НЦЗПД обязан уведомить заявителя.

Таким образом, сроки рассмотрения жалоб в отношении персональных данных увеличены вдвое по сравнению с жалобами, рассматриваемыми согласно Закону об обращениях.

Если в рамках рассмотрения жалобы будут подтверждены факты нарушения при обработке персональных данных, указанных в жалобе, НЦЗПД обязан принять необходимые меры по защите нарушенных прав, свобод и законных интересов субъекта персональных данных, подавшего жалобу; об этом также уведомляется заявитель.

Если же содержащиеся в жалобе сведения о нарушениях при обработке персональных данных не подтверждаются, НЦЗПД оставляет такую жалобу без удовлетворения и информирует об этом заявителя, подавшего жалобу, с разъяснением порядка обжалования такого решения (ч. 2 п. 32 Положения о НЦЗПД).

Таким образом, руководителю организации здравоохранения необходимо понимать, что в случае поступления от пациента (клиента) или работника жалобы в НЦЗПД в отношении организации здравоохранения также может быть проведена проверка в части соблюдения законодательства о защите ПД. ◈

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ВОПРОСЫ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ИХ ЗАЩИТЕ

Мы плавно перейдем к вопросам ответственности за нарушение порядка защиты персональных данных и рассмотрим особенности привлечения к такой ответственности.

Татьяна СОКОЛОВСКАЯ, *ведущий юрисконсульт государственного учреждения «Республиканский научно-практический центр онкологии и медицинской радиологии им. Н. Н. Александрова», старший преподаватель кафедры конституционного права юридического факультета БГУ*

В соответствии со ст. 19 Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон) лица, виновные в нарушении данного Закона, несут ответственность, предусмотренную законодательными актами.

Так, за нарушение законодательства о защите персональных данных могут быть применены следующие виды ответственности:

- дисциплинарная;
- гражданско-правовая;
- материальная;

- административная;
- уголовная.

ДИСЦИПЛИНАРНАЯ ОТВЕТСТВЕННОСТЬ

По общему правилу дисциплинарная ответственность применяется за противоправное, виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей (дисциплинарный проступок).

Справочно: *за совершение дисциплинарного проступка наниматель может применить к работнику следующие меры дисциплинарного взыскания:*

- *замечание;*
- *выговор;*
- *лишение полностью или частично стимулирующих выплат на срок до 12 месяцев;*
- *увольнение (пп. 6–11 ст. 42, пп. 1, 1^2, 5^1, 9 и 10 ч. 1 ст. 47 ТК).*

Самостоятельным дополнительным основанием для прекращения трудового договора с работником является нарушение последним порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных (п. 10 ч. 1 ст. 47 ТК).

> ***Указанное основание увольнения как дисциплинарного взыскания действует с 30 июня 2021 г. — даты вступления в силу изменений, внесенных в ТК Законом Республики Беларусь от 28.05.2021 № 114-З «Об изменении законов по вопросам трудовых отношений».***

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ

Административная ответственность за нарушение законодательства о защите персональных данных предусмотрена ст. 23.7 КоАП. Правовые последствия соответствующих административных правонарушений представлены в *таблице* на следующей странице.

Таблица

Нарушения и ответственность в сфере защиты персональных данных (КоАП)

Правонарушение	Санкция
Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных	Штраф в размере до 50 БВ
Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных, лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью	Штраф в размере от 4 до 100 БВ
Умышленное незаконное распространение персональных данных физических лиц	Штраф в размере до 200 БВ
Несоблюдение мер обеспечения защиты персональных данных физических лиц	Штраф в размере от 2 до 10 БВ В отношении ИП — от 10 до 25 БВ В отношении юрлиц — от 20 до 50 БВ

С учетом требований по защите персональных данных, предусмотренных Законом, можно выделить следующие нарушения, за которые организацию здравоохранения могут привлечь к административной ответственности:

- не создан обязательный пакет документов по обеспечению защиты персональных данных (абз. 2–5 п. 3 ст. 17 Закона);
- не обеспечена сохранность персональных данных (абз. 6 п. 3 ст. 17 Закона);
- не обеспечен неограниченный доступ к документам, определяющим политику оператора в отношении обработки персональных данных, до начала такой обработки (п. 4 ст. 17 Закона).

Максимальный размер штрафа за такого рода нарушения для юридических лиц составляет 50 БВ.

Если говорить о таком нарушении, как умышленное незаконное распространение персональных данных физических лиц, то нужно напомнить, что согласно абз. 11 ст. 1 Закона под распространением понимают

действия, направленные на ознакомление с персональными данными неопределенного круга лиц.

МНЕНИЕ АВТОРА

К такого рода нарушениям можно отнести, например, размещение на сайте организации здравоохранения отзыва физического лица с указанием его ФИО и фотографией, когда согласия этого физического лица не имеется.

Частью 2 ст. 23.9 КоАП предусмотрена административная ответственность за нарушение требований законодательных актов по учету и хранению персональных данных пользователей интернет-услуг.

Размер штрафа за такого рода правонарушение составляет до 15 БВ.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

Уголовная ответственность в сфере защиты персональных данных предусмотрена за:

- умышленные незаконные сбор, предоставление персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина (ст. 203^1 УК);
- несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим их обработку, повлекшее по неосторожности их распространение и причинение тяжких последствий (ст. 203^2 УК).

За преступления, предусмотренные ч. 1 ст. 203^1 УК, может быть назначено наказание в виде *общественных работ, или штрафа, или ареста, или ограничения или лишения свободы на срок до двух лет*.

За преступления, предусмотренные ст. 203^2 УК,— наказание в виде *штрафа, или лишения права занимать определенные должности или заниматься определенной деятельностью, или исправительных работ на срок до одного года, или ареста, или ограничения свободы на срок до двух лет, или лишения свободы на срок до одного года*.

Действия, предусмотренные чч. 1 и 2 ст. 203[1] УК, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга, наказываются ограничением свободы на срок до пяти лет или лишением свободы на тот же срок со штрафом.

ГРАЖДАНСКО-ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ

Оператор может быть привлечен к гражданско-правовой ответственности в случае необходимости компенсации морального вреда и возмещения убытков.

Справочно: *моральный вред подлежит возмещению независимо от того, возмещались ли физическому лицу имущественный вред и понесенные им убытки.*

Согласно п. 2 ст. 19 Закона ответственность оператора в данном случае может наступить, если нарушены:

- права физического лица, установленные Законом;
- правила обработки персональных данных;
- требования к защите персональных данных.

МНЕНИЕ АВТОРА

Из этого следует, что параллельно с привлечением к административной и (или) уголовной ответственности может возникнуть ситуация, когда организация здравоохранения должна будет выплатить физическому лицу компенсацию и возместить убытки, если суд примет такое решение.

В соответствии с ч. 2 ст. 152 ГК при определении размера компенсации суд учитывает степень вины и степень страданий гражданина.

При этом убытки суд взыщет в том случае, если будут доказаны:

- факт наступления вреда;
- противоправность действий организации здравоохранения;
- вина организации здравоохранения;
- причинно-следственная связь между противоправными действиями и наступившими последствиями.

МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Работник при нарушении порядка работы с персональными данными может быть привлечен к материальной ответственности.

Справочно: *привлечение к материальной ответственности возможно при одновременном наличии следующих условий:*

- *ущерба, причиненного нанимателю при исполнении трудовых обязанностей;*
- *противоправности поведения (действия или бездействия) работника;*
- *прямой причинной связи между противоправным поведением работника и возникшим у нанимателя ущербом;*
- *вины работника в причинении ущерба.*

При этом при определении размера ущерба учитывается только реальный ущерб, упущенная выгода не учитывается, за исключением случая полной материальной ответственности (ст. 404 ТК).

Порядок привлечения работников к материальной ответственности за ущерб, причиненный нанимателю при исполнении трудовых обязанностей, предусмотрен главой 37 ТК.

НАРУШЕНИЕ РАБОТНИКОМ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПД: АЛГОРИТМ УВОЛЬНЕНИЯ

С 30.06.2021 в ТК внесено новое основание увольнения, предусмотренное п. 10 ч. 1 ст. 47 ТК. Теперь наниматель вправе уволить работника за нарушение им порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных. Каков алгоритм увольнения работника по этому основанию, рассмотрим далее.

Владимир САМОСЕЙКО, *юрист, магистр права*

В первую очередь необходимо отметить, что основание увольнения, предусмотренное п. 10 ч. 1 ст. 47 ТК, а именно нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных, применяется без учета требований ст. 43 «Порядок и условия расторжения трудового договора по инициативе нанимателя» и ст. 46 ТК «Расторжение трудового договора по инициативе нанимателя с предварительного уведомления профсоюза или согласия профсоюза».

Справочно: *это обусловлено тем, что данное основание не относится к основаниям увольнения по инициативе нанимателя (не предусмотрено ст. 42 ТК).*

Но поскольку указанное основание увольнения является мерой дисциплинарного взыскания (п. 4 ч. 1 ст. 198 ТК), то при такого рода увольнении следует соблюсти требования главы 14 ТК «Дисциплинарная ответственность работников».

Рассматриваемое основание увольнения также прямо не поименовано в подп. 6.14[1] п. 6 Декрета Президента Республики Беларусь от 15.12.2014 № 5 «Об усилении требований к руководящим кадрам и работникам организаций» (далее — Декрет № 5) как увольнение по дискредитирующим обстоятельствам.

ЧТО ЯВЛЯЕТСЯ ОСНОВАНИЕМ УВОЛЬНЕНИЯ?

Увольнение по п. 10 ч. 1 ст. 47 ТК может быть произведено в случае **нарушения порядка обработки персональных данных**.

В Законе Республики Беларусь от 07.05.2022 № 99-З «О защите персональных данных» (далее — Закон) используется обобщенный термин — «обработка персональных данных».

Справочно: *в ст. 1 Закона под обработкой персональных данных понимается любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных.*

На самом деле обработка персональных данных формально шире перечня действий, который приведен в указанном определении, и этот перечень **не является исчерпывающим**.

АЛГОРИТМ УВОЛЬНЕНИЯ РАБОТНИКА

Увольнение по п. 10 ч. 1 ст. 47 ТК является одной из мер ответственности за противоправное поведение работника (нарушение условий трудового договора, внутреннего распорядка, режима защиты персональных данных и т. п.).

Так, для увольнения работника по п. 10 ч. 1 ст. 47 ТК нанимателю необходимо выполнить следующие действия.

ШАГ 1. ФИКСИРУЕМ ФАКТ НАРУШЕНИЯ

Документами, подтверждающими факт нарушения работником порядка обработки персональных данных (нарушение работником порядка

сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения, предоставления, удаления персональных данных), могут быть:

- докладные (служебные) записки работников нанимателя, обнаруживших факт такого нарушения;
- соответствующий акт и т. п.

Примерный образец докладной записки о нарушении работником режима защиты персональных данных*

ШАГ 2. ПРОВЕРЯЕМ СОЗДАНИЕ НЕОБХОДИМЫХ УСЛОВИЙ

Нанимателю следует выяснить: были ли созданы условия для режима защиты персональных данных? На наш взгляд, самого по себе нарушения порядка обработки персональных данных недостаточно для увольнения работника по п. 10 ч. 1 ст. 47 ТК.

Для увольнения по рассматриваемому основанию необходимо убедиться в том, что наниматель создал условия для соблюдения режима защиты персональных данных, в частности:

- выполнил требования ст. 17 Закона;
- включил в трудовой договор и (или) должностную инструкцию работника обязанность по соблюдению порядка обработки персональных данных;
- работник ознакомлен под роспись с локальными правовыми актами, регламентирующими порядок обработки персональных данных;
- работник нарушил порядок обработки персональных данных, к которым он имел право допуска (право на их обработку) в силу своих трудовых обязанностей.

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

ШАГ 3. ВЫЯСНЯЕМ ВИНУ РАБОТНИКА И ЗАТРЕБУЕМ ОБЪЯСНЕНИЕ

Согласно ч. 1 ст. 199 ТК до применения дисциплинарного взыскания наниматель обязан затребовать письменное объяснение работника.

Формы такого затребования законодательством **не предусмотрены**.

Это может быть требование, изложенное как в устной, так и в письменной форме (например, в виде уведомления).

Примерный образец оформления требования нанимателя о представлении письменных объяснений*

ШАГ 4. ПОЛУЧАЕМ ОБЪЯСНЕНИЯ ИЛИ ФИКСИРУЕМ ОТКАЗ

Объяснение причин совершения нарушения (дисциплинарного проступка) работник исходя из ч. 1 ст. 199 ТК излагает в объяснительной записке.

Справочно: *рекомендательная форма такой записки содержится в Унифицированной системе организационно-распорядительной документации, утвержденной приказом директора Департамента по архивам и делопроизводству Министерства юстиции Республики Беларусь от 28.11.2019 № 41.*

Работник может отказаться от дачи (предоставления) письменного объяснения. Согласно ч. 2 ст. 199 ТК отказ работника от дачи письменного объяснения, невозможность получения от него объяснения по поводу совершенного дисциплинарного проступка **не являются препятствиями для применения дисциплинарного взыскания** и оформляются актом с указанием присутствовавших при этом свидетелей.

ШАГ 5. ПРОВОДИМ СЛУЖЕБНУЮ ПРОВЕРКУ

Наниматель в случае увольнения работника по п. 10 ч. 1 ст. 47 ТК должен соблюсти п. 7 Декрета № 5, то есть провести проверку наличия нарушений со стороны работника и оформить результаты такой проверки актом или

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

служебной запиской, в которых отражаются факты и обстоятельства, повлекшие допущенные нарушения.

Срок проведения такой проверки может быть закреплен в соответствующем локальном правовом акте организации или в приказе (распоряжении) о проведении проверки.

Примерный образец акта о результатах проверки по факту нарушения работником порядка обработки персональных данных*

ШАГ 6. ПРОВЕРЯЕМ НАЛИЧИЕ ВСЕХ УСЛОВИЙ ПЕРЕД УВОЛЬНЕНИЕМ

В частности, нанимателю нужно проверить следующие условия для применения такой меры дисциплинарной ответственности, как увольнение по п. 10 ч. 1 ст. 47 ТК:

- является ли работник лицом, допущенным к обработке персональных данных;
- был ли работник обучен в соответствии с законодательством работе с персональными данными, надлежащим образом ознакомлен с требованиями по работе с персональными данными;
- имело ли место в действительности нарушение порядка обработки персональных данных, а также была ли вина работника;
- соблюдены ли все процессуальные требования (запрос письменных объяснений) (ст. 199 ТК), сроки наложения дисциплинарного взыскания (ст. 200 ТК).

Если все условия соблюдены, можно переходить к следующему шагу.

ШАГ 7. ИЗДАЕМ ПРИКАЗ (РАСПОРЯЖЕНИЕ) ОБ УВОЛЬНЕНИИ РАБОТНИКА

Приказ об увольнении работника по п. 10 ч. 1 ст. 47 ТК необходимо оформить в соответствии с требованиями Инструкции по делопроизводству в государственных органах, иных организациях, утвержденной поста-

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

новлением Министерства юстиции Республики Беларусь от 19.01.2009 № 4 (в ред. от 17.10.2019).

Примерный образец приказа об увольнении работника по п. 10 ч. 1 ст. 47 ТК*

ШАГ 8. ВКЛЮЧАЕМ КОПИЮ ПРИКАЗА В ЛИЧНОЕ ДЕЛО

Согласно п. 8 Инструкции о порядке формирования, ведения и хранения личных дел работников, утвержденной постановлением Комитета по архивам и делопроизводству при Совете Министров Республики Беларусь от 26.03.2004 № 2 (далее — Инструкция о личных делах), в процессе ведения личного дела в него включаются копии (выписки) приказов (распоряжений, решений, постановлений) об увольнении.

ШАГ 9. ПРОИЗВОДИМ ОКОНЧАТЕЛЬНЫЙ РАСЧЕТ

При увольнении работника все выплаты, причитающиеся ему от нанимателя на день увольнения (кроме выплат, установленных системами оплаты труда, размер которых определяется по результатам работы за месяц или иной отчетный период), производятся **не позднее дня увольнения**.

Справочно: *если работник в день увольнения не работал, то соответствующие выплаты должны быть произведены не позднее дня, следующего за днем предъявления работником требования о расчете (ст. 77 ТК). При задержке расчета работник имеет право взыскать с нанимателя заработок за каждый день задержки (ст. 78 ТК).*

ШАГ 10. ВНОСИМ ЗАПИСЬ В ТРУДОВУЮ КНИЖКУ

Согласно ч. 5 ст. 50 ТК, п. 26 Инструкции о порядке ведения трудовых книжек, утвержденной постановлением Министерства труда и социальной защиты Республики Беларусь от 16.06.2014 № 40 (в ред. от 10.01.2020, далее — Инструкция о ведении трудовых книжек), **основанием для внесения в трудовую книжку записей об увольнении является приказ (распоряжение) нанимателя**.

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

Запись, точно соответствующая формулировке приказа (распоряжения), вносится после его издания в день увольнения.

Примерный образец оформления записи в трудовой книжке об увольнении*

ШАГ 11. ВНОСИМ СВЕДЕНИЯ В ЛИЧНУЮ КАРТОЧКУ (НА УСМОТРЕНИЕ НАНИМАТЕЛЯ)

В настоящий момент отсутствует унифицированная форма личной карточки, нормативно не определен порядок ее ведения и заполнения.

Следовательно, наниматель самостоятельно разрабатывает форму личной карточки работника и порядок ее ведения.

Справочно: *за основу можно взять ранее действовавшую форму № Т-2, утвержденную постановлением Государственного комитета СССР по статистике от 28.12.1989 № 241 «Об утверждении форм первичной учетной документации для предприятий и организаций».*

Примерный образец оформления записи об увольнении работника в личной карточке*

ШАГ 12. ВЫДАЕМ РАБОТНИКУ ТРУДОВУЮ КНИЖКУ

Работнику в день увольнения (в последний день работы) выдается трудовая книжка (ч. 6 ст. 50 ТК).

При получении трудовой книжки в связи с увольнением работник расписывается в книге учета движения трудовых книжек и вкладышей к ним, собственноручно указав дату получения (ч. 6 п. 79 Инструкции о ведении трудовых книжек).

Примерный образец заполнения книги учета движения трудовых книжек и вкладышей к ним*

* *Чтобы* ***открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов*** *в формате .docx (на панели слева).*

Если при открытии пособия ***формы документов*** *у вас* ***не отобразились*** *слева, то* ***нажмите на «Вложения» (Attachments, скрепка)****.*

Чтобы ***использовать форму, сохраните*** *уже открытую на свой компьютер.*

ШАГ 13. СДАЕМ ЛИЧНОЕ ДЕЛО В АРХИВ

Личные дела уволенных работников подлежат передаче в архив организации по описи (п. 23 Инструкции о личных делах).

Личные дела уволенных работников вносятся в опись дел по личному составу по году увольнения и систематизируются по алфавиту фамилий. Допускается составлять отдельную опись личных дел уволенных работников.

ШАГ 14. НАПРАВЛЯЕМ СВЕДЕНИЯ В ВОЕНКОМАТ

Об увольнении с работы граждан, состоящих или обязанных состоять на воинском учете, необходимо в месячный срок сообщать в военные комиссариаты (обособленные подразделения) (абз. 2 ч. 1 ст. 9 Закона Республики Беларусь от 05.11.1992 № 1914-XII «О воинской обязанности и воинской службе», в ред. от 10.12.2020).

ШАГ 15. ОФОРМЛЯЕМ ПУ-2

Оформление документов персонифицированного учета производится в соответствии с постановлением правления Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь от 19.06.2014 № 7 «О некоторых вопросах заполнения и приема-передачи форм документов персонифицированного учета» (в ред. от 24.12.2021), которым в том числе утверждена Инструкция о порядке заполнения форм документов персонифицированного учета.

В свою очередь порядок и сроки их представления определяются Правилами индивидуального (персонифицированного) учета застрахованных лиц в системе государственного социального страхования, утвержденными постановлением Совета Министров Республики Беларусь от 08.07.1997 № 837 (в ред. от 25.03.2022).

Примерный образец заполнения ПУ-2 в случае увольнения (как основного работника) *

* *Чтобы **открыть нужную форму документа, кликните на ней дважды в списке вложенных файлов** в формате .docx (на панели слева).*

*Если при открытии пособия **формы документов** у вас **не отобразились** слева, то **нажмите на «Вложения» (Attachments, скрепка)**.*

*Чтобы **использовать форму, сохраните** уже открытую на свой компьютер.*

У ВАС ВОПРОС — У НАС ОТВЕТ

В рамках пособия мы подготовили ответы на вопросы, с которыми уже столкнулись организации здравоохранения в части обработки персональных данных (далее — ПД) и применения норм Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее — Закон).

*Отвечает **Алёна Поторская**, ведущий юрист REVERA, руководитель проектов в сфере защиты персональных данных.*

? *Существует ли минимум требований для того, чтобы данные можно было назвать персональными и они подпадали под действие Закона? Практический пример: проводится опрос при предварительной записи на прием, пациент называет свои ФИО, телефон, описывает проблемы со здоровьем. Являются ли такие данные персональными? Ведь они не подтверждены документально субъектом.*

! Понятие «персональные данные» напрямую содержится в Законе, а именно в ст. 1. Если рассмотреть конкретную приведенную ситуацию, то такие данные будут являться персональными. Документальное подтверждение данных не является обязательным критерием для отнесения их к персональным. Организациям при этом нужно понимать, что к ПД относится очень широкий спектр данных, и если возникают сомне-

ния в отношении каких-либо данных, лучше исходить из утверждения, что они являются персональными.

Обязательно ли в организации здравоохранения вводить штатную единицу — ответственного за информационную безопасность?

Создавать отдельную штатную единицу необязательно. Эти обязанности можно возложить и на текущего работника/работников организации.

Правоохранительные органы в рамках расследования дел часто запрашивают у организаций здравоохранения стационарные и амбулаторные карты пациентов. В соответствии с Законом каждый гражданин может обратиться к оператору с целью предоставления сведений, когда, какие и кому им передавались персональные данные. Необходимо ли в таком случае указывать информацию о том, что сведения, содержащиеся в медицинской карте пациента, передавались в правоохранительные органы?

Указывать такую информацию необходимо, поскольку в настоящее время предоставление такой информации субъекту персональных данных предусмотрено Законом. Никаких ограничений, разъяснений и запретов на этот счет нет.

Как должна оформляться передача сведений и документов, содержащих персональные данные пациентов, между организациями здравоохранения?

В настоящее время конкретных требований о том, как должна оформляться передача таких сведений, не существует. Поэтому целесообразно просто вести учет документов согласно общим правилам делопроизводства.

Какой срок действия целесообразно установить для согласия пациента на обработку ПД в частной стоматологии?

Чтобы понять, какой срок необходимо установить, нужно определить цель обработки конкретных ПД. Установление сроков напрямую будет зависеть от цели обработки ПД. При этом при установлении срока следует учитывать его оптимальность и адекватность, так как уста-

новленные сроки в случае проведения проверки контролирующими органами необходимо обосновать. Приведем пример с рассылкой: очень сложно обосновать срок рассылки в течение 100 лет, а вот срок в 1 год с момента последнего посещения вполне поддается логичному обоснованию.

Что делать частным лабораториям, которые не ведут медицинские карточки и у которых нет определенных сроков хранения ПД (но по факту данные хранятся столько же, сколько и медкарты)?

Если в отношении хранения документации срок хранения установлен на законодательном уровне, то нужно хранить ее в соответствии с этими сроками. Если же установленного срока нет, то необходимо установить срок хранения самостоятельно и грамотно его обосновать. При этом срок может быть не только конкретным, но и начинать свое течение с наступления определенных событий.

Законом предусмотрено, что субъект, выразивший желание отозвать согласие на хранение ПД, должен написать заявление с широким перечнем ПД (среди них идентификационный номер паспорта, место жительства). Что делать с заявлением субъекта? Сохраняя его, мы начинаем вести базу данных лиц с ПД, которые против сохранения этих самых ПД.

Эта ситуация действительно спорная. Рекомендуем после исполнения запроса по заявлению сохранять заявление субъекта, чтобы в случае спорной ситуации иметь возможность доказать, что действия с ПД были совершены по просьбе самого субъекта. Но при этом следует максимально анонимизировать такое заявление (к примеру, сохранить только ФИО субъекта, удалив/скрыв иные персональные данные).

Каким образом удалять ПД о пациенте из базы поликлиники, в частности те, которые необходимы продолжительное количество лет для экспертиз и оказания медицинской помощи?

ПД следует хранить до того момента, пока они нужны для заявленных целей обработки. В частности, если в законодательстве есть требование хранить данные в определенных целях в течение определенного периода времени,— до истечения этого периода. Даже в случае получения запроса субъекта на удаление ПД необходимо продолжать хранить такие ПД.

В п. 5 постановления Министерства здравоохранения Республики Беларусь от 07.06.2021 № 74 «О формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента» (далее — постановление № 74) указано, что согласие пациентом дается однократно при первичном посещении государственной организации здравоохранения. Что означает «первичное посещение пациента»: посещение учреждения здравоохранения по месту жительства либо первичное посещение различных организаций здравоохранения?

В соответствии с разъяснениями Министерства здравоохранения согласие у пациента берется однократно по месту его регистрации. Это сделано для того, чтобы несколько снизить нагрузку на учреждения здравоохранения, и с учетом занесения согласия пациента в централизованную информационную систему здравоохранения.

При проведении мониторинга проверяющими не были приняты документы, в том числе согласие на обработку ПД, разработанные в соответствии с Законом, в связи с необходимостью получения согласия по постановлению № 74. Правомерны ли требования контролирующих органов?

Согласие, предусмотренное постановлением № 74, предполагает именно включение в централизованную систему здравоохранения. Если речь идет о согласии для целей включения пациента в данную систему, то необходимо руководствоваться постановлением № 74. Если же речь идет не о внесении в систему, то ситуация неоднозначная. На наш взгляд, согласие на обработку ПД, если оно разработано в соответствии с Законом, является правомерным документом. Вероятно, данный вопрос будет урегулирован позднее, когда среди всех органов будет выработана единая стратегия работы в рамках Закона.

Ведение медицинской карты можно осуществлять только с согласия пациента?

На наш взгляд, согласие для ведения медкарты не требуется. Однако, поскольку ведение медкарт — это вопрос общереспубликанский, рекомендуем дождаться официальной позиции Национального центра защиты персональных данных по данному вопросу.

Требуется ли согласие пациента при передаче его ПД между организациями здравоохранения посредством запроса (различные выписки)?

Если требование о направлении запроса и предоставлении выписок напрямую предусмотрено на законодательном уровне, то согласие на передачу данных третьему лицу не нужно. Причем это касается обеих сторон – как той, которая делает запрос, так и той, которая будет предоставлять сведения. Если же прямой обязанности предоставления ПД на законодательном уровне не установлено, то для передачи таких данных требуется согласие субъекта.

Если бригада скорой медицинской помощи приехала на вызов к пациенту и ей необходимо получить от него ПД (ФИО, паспортные данные и т. д.), должна ли она вначале получить письменное согласие пациента на их обработку?

В данном случае получать согласие не нужно, так как есть возможность сослаться на отдельное основание (оказание медицинской помощи) в рамках действующего Закона.

Что означает абз. 13 ст. 6 Закона касательно договорных отношений? В каких случаях нужно брать согласие на обработку ПД, а в каких – нет? Нужно ли брать согласие на обработку ПД при заключении договоров на платные услуги в организациях здравоохранения?

Все достаточно просто: если данные обрабатываются только с целью заключения и исполнения договора, то согласие субъекта на обработку ПД не нужно. Если же преследуются еще и дополнительные цели, то получение согласия обязательно. Это необходимо учитывать прежде всего частным медицинским организациям, так как многие используют данные в договоре для рассылки. В настоящее время для того, чтобы обработать данные пациента (клиента) для рассылки, нужно получить его согласие.

Если в организации заключается договор на платные услуги, который потом передается на хранение в бухгалтерию организации, нужно ли брать согласие на обработку ПД?

Если данные передаются бухгалтерии в рамках исполнения договора или для исполнения обязанностей, возложенных на организацию на законодательном уровне (к примеру, для выставления счетов

по договору, проверки расчетов, расчета и уплаты налогов и т.д.), согласие субъекта не требуется. Во всех иных случаях согласие необходимо.

Если пациент отказывается подписывать согласие, как и отказ от дачи согласия, можно ли оказать ему медицинскую услугу?

Если пациент обратился в организацию здравоохранения за медицинской помощью либо на бесплатной основе, либо на условиях заключенного договора, то у него не нужно брать согласие на обработку ПД и оснований для отказа в медицинской услуге нет. Согласие, как правило, влечет за собой дополнительные цели обработки ПД, от которых субъект может отказаться, но это никак не повлияет на оказание ему медицинской услуги.

Рассмотрим ситуацию: работнику организации здравоохранения выдается ходатайство на выделение общежития коммунальной собственности. Организация здравоохранения передает его персональные данные (ФИО, место работы и должность) в организацию-балансодержатель общежития. Необходимо ли брать согласие работника на передачу этих данных?

Надлежащим основанием в данном случае может выступать письменный документ, подписанный работником (к примеру, заявление о выдаче ходатайства, в котором работник может указать, что он осведомлен о том, что его ПД будут переданы третьему лицу). Если же никакой письменный документ с работника не запрашивается, то необходимо получить согласие работника на передачу таких данных.

Пациент записался на первичный прием посредством телефонной связи. Можно ли в данном случае отправить пациенту СМС с напоминанием времени и даты приема и запросить от него подтверждение записи через ссылку?

В данном случае для направления такой информации и запроса ответной информации необходимо согласие субъекта на обработку ПД. Ведь на момент записи пациента договор еще не заключен, соответственно ссылаться на договор как на основание обработки ПД нельзя.

Каким образом получать согласие на использование ПД при первичном звонке для СМС-рассылки? По факту организация здравоохранения не может в рамках звонка предоставить политику обработки ПД пациенту (клиенту)?

Есть возможный вариант действий, если необходимо получить согласие от пациента (клиента) в рамках звонка. Оператор сообщает о том, что информация об обработке ПД размещена в политике организации, а политика — размещена на сайте, либо озвучивает всю требуемую информацию об обработке в рамках звонка.

Врач назначил пациенту контрольный осмотр через 3 месяца. Для напоминания пациенту необходимо отправить СМС или совершить звонок. Нужно ли для таких действий согласие пациента на обработку ПД?

Согласие в данном случае не требуется при условии, что цель таких звонков и СМС — напомнить о записи и такая обработка осуществляется в рамках исполнения заключенного с пациентом договора. Если же заключенного договора нет или организация будет дополнительно использовать номер телефона для рекламной рассылки или звонков, то согласие однозначно требуется.

Если есть согласие пациента на отправку ему результатов обследования по e-mail, можно ли вставить ссылку в тексте письма с просьбой пройти опрос о качестве обслуживания в медицинском центре (если при опросе ПД требоваться не будут)?

Ссылку вставить можно, однако следует уделить особое внимание информации, которая будет обрабатываться в рамках опроса. Если опрос не будет содержать ПД клиента, то согласие не нужно. Если же некоторые данные все-таки будут обработаны, то необходимо получение отдельного согласия.

ЧЕК-ЛИСТЫ

Мы подготовили для вас практические чек-листы, которые можно заполнить как в режиме онлайн, так и скачать на персональный компьютер. Представленные чек-листы помогут вам оптимизировать некоторые процессы организации работы с персональными данными в вашей организации. Доступ к чек-листам возможен только при наличии подключения к сети Интернет.

Чек-лист «Внедряем меры по защите персональных данных в организации здравоохранения»

Чек-лист «Разрабатываем политику обработки персональных данных»

Чек-лист «Осуществляем удаление персональных данных»

Чек-лист «Осуществляем трансграничную передачу персональных данных»

Чек-лист «Увольняем работника за нарушение законодательства о персональных данных»

Производственно-практическое издание

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ:
работаем правильно

Редактор Я. Ероховец
Компьютерный дизайн и верстка О. Бурова

Общество с ограниченной ответственностью
«Информационное правовое агентство Гревцова».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий
№ 1/433 от 03.10.2014.
Логойский тракт, 22а, пом. 57, 220090, г. Минск.