Национальный центр защиты персональных данных
Республики Беларусь

Постатейный комментарий

к Закону Республики Беларусь ”О защите персональных данных“

2023
Минск

Авторы:
А.А. Гаев, В.И. Диско, С.В. Задиран, Е.М. Липлянин, А.А. Парфенчик, И.А. Пырко, Н.А. Саванович, Е.В. Синюк, Н.А. Швед, Д.А. Шевчук

Рецензенты:

О.Н. Здрок, директор учреждения образования ”Институт переподготовки и повышения квалификации судей, работников прокуратуры, судов и учреждений юстиции Белорусского государственного университета“, д-р юрид. наук, доцент

Р.Р. Томкович, доцент кафедры хозяйственного права юридического факультета Белорусского государственного университета, исполнительный директор открытого акционерного общества ”Белинвестбанк“, канд. юрид. наук, доцент

Н.В. Шакель, доцент кафедры международного права факультета международных отношений Белорусского государственного университета, старший юрист общества с ограниченной ответственностью ”Степановский, Папакуль и партнеры. Юридические услуги“, канд. юрид. наук, доцент

Оглавление

Список сокращений основных нормативных актов

ГК – Гражданский кодекс Республики Беларусь

ГПК – Гражданский процессуальный кодекс Республики Беларусь

Закон (если не определено иное) – Закон Республики Беларусь от 7 мая 2021 г. № 99-З "О защите персональных данных"

Закон "О здравоохранении" – Закон Республики Беларусь от 18 июня 1993 г. № 2435-XII "О здравоохранении"

Закон "О регистре населения" – Закон Республики Беларусь от 21 июля 2008 г. № 418-З "О регистре населения"

Закон "Об информации, информатизации и защите информации" – Закон Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации"

Закон "Об исполнительном производстве" – Закон Республики Беларусь от 24 октября 2016 г. № 439-З "Об исполнительном производстве"

Закон "О единой государственной системе регистрации и учета правонарушений" – Закон Республики Беларусь от 9 января 2006 г. № 94-З "О единой государственной системе регистрации и учета правонарушений"

КоАП – Кодекс Республики Беларусь об административных правонарушениях

Конвенция о защите физических лиц при автоматизированной обработке персональных данных – Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (г. Страсбург, 28 января 1981 г.)

Конституция – Конституция Республики Беларусь

ПИКоАП – Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях

Положение – Положение о Национальном центре защиты персональных данных, утвержденное Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 "О мерах по совершенствованию защиты персональных данных"

Приказ № 66 – приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 "О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449"

ТК – Трудовой кодекс Республики Беларусь

УК – Уголовный кодекс Республики Беларусь

Указ № 422 (если не определено иное) – Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 "О мерах по совершенствованию защиты персональных данных"

Указ № 510 – Указ Президента Республики Беларусь от 16 октября 2009 г. № 510 ”О совершенствовании контрольной (надзорной) деятельности в Республике Беларусь“

УПК – Уголовно-процессуальный кодекс Республики Беларусь

GDPR – Общий регламент защиты персональных данных от 27 апреля 2016 г. № 2016/679

Прочие сокращения

ОАЦ (если не определено иное) – Оперативно-аналитический центр при Президенте Республики Беларусь

ФИО (если не определено иное) – фамилия, имя, отчество (если таковое имеется)

Центр (если не определено иное) – Национальный центр защиты персональных данных Республики Беларусь

п. – пункт

подп. – подпункт

ч. – часть

ст. – статья

Введение

Желание иметь личную сферу, свободную от вторжения других лиц – естественное стремление человека. Большинство из нас не хотят широко афишировать взаимоотношения в семье, с родственниками, личные пристрастия, размер зарплаты, обладание имуществом, допускаемые правонарушения и др. Причины могут быть самые разные, начиная от опасения стать объектом неправомерных действий и заканчивая боязнью осуждения, насмешек, травли.

Поэтому во все времена люди старались оберегать и защищать личные сведения и основным инструментом был контроль над носителями такой информации, ограничение круга осведомленных лиц. Важным элементом были физические границы дома, квартиры, выступающие барьером для нежелательного вмешательства извне.

Но за последние десятилетия ситуация с контролем за своей личной информацией кардинальным образом изменилась. Различные технологии и гаджеты прочно вошли в нашу жизнь, изменив ее традиционный уклад. Сформировалась новая информационная реальность, в рамках которой большинство населения уже не представляет себя без карманных помощников в виде мобильных телефонов, позволяющих быстро найти необходимую информацию, выйти в любое время на связь с нужным человеком, совершить покупки или платежи, не выходя из дома, и др. Неотъемлемым элементом повседневной коммуникации становятся различные социальные сети и мессенджеры. Одновременно происходит повсеместный перенос данных (дублирование данных), содержащихся на физических носителях, в информационные ресурсы.

Но вместе с позитивными изменениями смартфоны, облачные сервисы, социальные сети и технологии больших данных способствуют возникновению нового общества наблюдения, которое создает серьезные угрозы конфиденциальности. В большинстве случаев условием получения интересующих услуг выступает указание своих персональных данных, предоставление согласия на их обработку, согласие с политиками конфиденциальности.

Обработка данных приобретает беспрецедентные масштабы. Пользуясь Интернетом, мы ежедневно совершаем бесчисленное количество онлайн-действий, просматривая, выбирая, комментируя, оценивая и др., что постоянно фиксируется, анализируется, систематизируется и используется. Данные становятся ”топливом“ множества бизнес-процессов, и для их сбора изобретаются все новые и новые способы, в том числе и обмен на разного рода бесплатные сервисы. Полученные данные используются для различных целей, начиная от рекламной рассылки и заканчивая массовым манипулированием поведением людей.

При этом обработка во многих случаях носит непрозрачный и непонятный для человека характер.

В таких условиях естественные барьеры приватности (дома, квартиры, физический контроль над носителями личной информации и др.) становятся весьма зыбкими.

Получение согласия как способ защиты персональной информации также становится все менее действенным. Люди настолько перегружены просьбами о согласии на использование их данных, что осознанный выбор, особенно при отсутствии альтернативы, становится в значительной степени иллюзией. В свою очередь, попытки ”отгородить“ себя от глобального информационного общества, ограничить объем предоставляемой личной информации приводят к существенному сужению возможностей, доступных человеку.

В итоге граждане постепенно утрачивают контроль над личной информацией, а риски и угрозы для сферы частной жизни возрастают.

К сожалению, законы, в той или иной степени регламентирующие отдельные аспекты защиты персональных данных, принятые в предыдущие годы, зачастую ”не успевают“ за развитием технологий, что приводит к серьезному разрыву между установленными данными законами стандартами защиты прав граждан и реально складывающимися в повседневной жизни ситуациями.

Вместе с тем право на защиту персональных данных выходит за рамки обычного права, охраняемого законодательством. Неспособность гарантировать право на защиту личных данных ставит ”под удар“ другие смежные права и свободы, включая свободу выражения мнения, свободу мирных собраний, доступа к информации, принцип недискриминации. Боязнь онлайн-слежки, прослушивания телефонов препятствует демонстрации своих взглядов, интересов, выражению своих мыслей.

В этой связи традиционные механизмы защиты персональных данных требуют пересмотра с целью адаптации под реалии современного информационного общества и создания действенных инструментов защиты охраняемых прав и свобод.

Отдельного внимания заслуживает вопрос об экономической природе персональных данных. Вошло в широкий оборот и стало общепринятым утверждение, что персональные данные являются новой валютой и ”новой нефтью“. Это повышает интерес бизнес-структур к таким данным, как следствие изыскиваются все новые и новые способы получения личной информации, лоббируется принятие на государственном уровне решений о раскрытии персональной информации, выведении отдельных категорий данных из-под действия законодательства о персональных данных (обезличенные персональные данные и др.).

Со стороны бизнеса формируется запрос на признание персональных данных товаром, предоставление возможности покупать и продавать такие данные.

На первый взгляд, это весьма логично. Ведь, по большому счету, регистрируясь на некоем бесплатном сайте, мы предоставляем возможность обрабатывать и использовать свои данные, монетизируя их. Участвуя в различных программах лояльности, мы фактически обмениваем свою личную информацию на небольшой дисконт (скидку), который потенциально можно получить. Еще более очевидной становится ситуация, когда мы имеем дело с моделями ”Pay or consent“ (”плати или соглашайся“). Это ситуации, когда лицо для использования сервиса должно или дать согласие на обработку его данных, или заплатить за использование сервиса без обработки персональных данных.

Тем не менее, последствия решения о признании персональных данных товаром будут весьма серьезными и могут привести к полному отторжению персональной информации от человека и, как следствие, кардинальной трансформации общества, в том виде, к которому мы привыкли.

Недопустимость такого подхода отмечена Европейским комиссаром по защите персональных данных (EDPS) и Европейским советом по защите персональных данных (EDPB). Европейский совет по защите данных (EDPB) в своем Руководстве 2/2019 по обработке персональных данных в контексте онлайн-сервисов заявил, что ”учитывая, что защита данных является основным правом, гарантированным ст. 8 Хартии Европейского союза по правам человека, и что одной из основных целей GDPR является предоставление субъектам данных контроля над информацией, относящейся к ним, персональные данные не могут рассматриваться как товар“[1]. EDPB пояснил, что обработка персональных данных отличается от денежных платежей по многим причинам, включая тот факт, что после утраты контроля над персональными данными он не обязательно может быть восстановлен.

EDPB и EDPS последовали той же аргументации в своем совместном мнении 2/2022. Хотя субъекты данных могут дать согласие на обработку своих персональных данных, они все равно не могут отказаться от своих основных прав. В этом отношении, по мнению EDPB и EDPS, перспектива ”коммерциализации“ персональных данных подорвет само понятие человеческого достоинства[2].

---

[1] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects [Электронный ресурс]. – Дата доступа: 11.11.2022.

[2] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [Электронный ресурс]. – Дата доступа: 11.11.2022.

В сложившейся ситуации возникает настоятельная необходимость выработки (обновления) правовых рамок работы с персональной информацией. Ситуация осложняется различиями в национальных правовых режимах, разными финансовыми и технологическими возможностями стран, невозможностью (неспособностью) влиять на политику крупных корпораций и др. Это требует от законодателя каждой страны определенной степени гибкости, чтобы, с одной стороны, не создавать излишних ограничений для бизнеса, когда защита данных становится дороже самих данных, а с другой – обеспечить практическую реализацию права на защиту персональных данных. В любом случае становится очевидным, что не все, что технически возможно и реализуемо, должно быть разрешено юридически.

Краткая история развития законодательства о персональных данных в Беларуси

Законодательство о персональных данных в любой стране является результатом определенной эволюции, отражающей специфику становления и существования конкретного государства. Не является в этом плане исключением и Беларусь. Ниже мы кратко остановимся на истории развития отечественного законодательства о персональных данных. В ней можно выделить несколько этапов.

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

На первоначальных этапах развития государственности на белорусских землях вопросам защиты личной информации особого внимания не уделялось. Первые упоминания об отдельных аспектах данного права появляются в Конституции БССР 1937 года в виде закрепления права граждан на тайну переписки.

В дальнейшем в ст. 54 Конституции БССР 1978 года предусматривалось, что личная жизнь граждан, тайна переписки, телефонных переговоров и телеграфных сообщений охраняется законом.

Конституция 1994 года в ст. 28 предусматривала, что каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство.

В это время общие вопросы права на защиту личной информации в законодательстве не рассматривались, как и место этого института в системе смежных институтов и правовых категорий. Не случайно, что и КоАП 1984 года, действовавший в это время, также не предусматривал ответственности за незаконные действия с персональными данными или информацией о частной жизни.

В целом вопрос о защите личных данных с учетом решаемых на этом историческом этапе задач в государстве не находился среди приоритетных.

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

Важным моментом в развитии рассматриваемого института законодательства стало принятие Закона Республики Беларусь от 6 сентября 1995 г. № 3850-XII ”Об информатизации“.

Хотя в данном Законе отсутствовал термин ”персональные данные“, в нем использовался близкий по содержанию оборот – информация о гражданах. В частности, в ст. 12 устанавливалось, что органы государственной власти, физические и юридические лица в пределах своей компетенции собирают, обрабатывают, хранят документированную информацию о гражданах и используют ее для выполнения возложенных на них функций и задач.

Положительным моментом было закрепление прав граждан в отношении собранной о них информации. Так, в соответствии со ст. 21 физическим и юридическим лицам предоставлялись права:

на доступ к документированной информации о них;

на уточнение этой документированной информации в целях обеспечения ее полноты и точности;

оспаривать эту документированную информацию в установленном законодательством порядке;

знать, кто и в каких целях накапливает или использует документированную информацию о них.

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

Фактически первым отечественным актом (не считая международных соглашений), в котором упоминались персональные данные, стала Инструкция Министерства внешних экономических связей Республики Беларусь от 25 сентября 1992 г. № 06/14 ”О порядке использования туристических ордеров/ваучеров предприятиями и организациями Республики Беларусь“. На уровне законодательного акта рассматриваемый термин впервые целенаправленно применен в Указе Президента Республики Беларусь от 6 апреля 1999 г. № 195 ”О некоторых вопросах информатизации в Республике Беларусь“. Данным Указом была утверждена концепция государственной политики

в области информатизации, которой предусматривалось, что для органов государственного управления в сфере информатизации приоритетными являются ряд направлений деятельности, в том числе защита персональных данных.

Серьезное влияние на развитие рассматриваемого института оказали два законодательных акта, принятых практически одновременно: Закон ”О регистре населения“ и Закон ”Об информации, информатизации и защите информации“.

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

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

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими должны были осуществляться с согласия данного физического лица, если иное не установлено законодательными актами.

Также закреплялось, что меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь. Последующая передача персональных данных разрешалась только с согласия физического лица, к которому они относились, либо в соответствии с законодательными актами.

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

В Законе ”О регистре населения“ персональные данные физических лиц определялись как совокупность основных и дополнительных персональных данных, а также данных о реквизитах документов, подтверждающих основные и дополнительные персональные данные конкретных физических лиц.

При этом к основным персональным данным относились:

идентификационный номер;

фамилия, собственное имя, отчество;

пол;

число, месяц, год рождения;

место рождения;

цифровой фотопортрет;

данные о гражданстве (подданстве);

данные о регистрации по месту жительства и (или) месту пребывания;

данные о смерти или объявлении физического лица умершим, признании безвестно отсутствующим, недееспособным, ограниченно дееспособным.

Несмотря на отсутствие четких признаков персональных данных, многие практические работники восприняли эту норму как собственно определение данного понятия. При этом использованный законодателем подход был весьма удобным для его применения, поскольку устранял дискуссии относительно признания конкретных сведений персональными данными.

Вместе с тем, очевидно, что данная норма в силу узости своего содержания не могла выступать в качестве базовой дефиниции рассматриваемого явления. Подобные определения содержались и в иных актах, например Законе Республики Беларусь от 13 июля 2006 г. № 144-З ”О переписи населения“ (далее – Закон ”О переписи населения“).

На этом этапе в законодательных актах постепенно начинают появляться нормы, связанные с обработкой персональных данных. В подавляющем большинстве случаев в них закреплялась возможность того или иного органа обрабатывать персональные данные без получения согласия граждан.

4 января 2014 г. в Закон ”Об информации, информатизации и защите информации“ включено дополнение, в котором впервые предпринята попытка дать универсальное определение персональных данных. Под персональными данными было предложено понимать основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

Данное определение, безусловно, стало серьезным шагом вперед по сравнению с определением в Законе ”О регистре населения“, отнеся к персональным данным любую информацию, которая позволяет идентифицировать лицо. Тем самым был выделен ключевой признак, характеризующий персональные данные, – способность идентифицировать лицо.

Но наряду с плюсами указанное определение сохраняло и очевидные недостатки. Использование словосочетания ”позволяющие идентифицировать лицо“, исходя из складывавшейся практики его применения, оставляло за рамками рассматриваемого понятия случаи, когда сами по себе данные лицо не идентифицируют, но вместе с иной имеющейся информацией позволяют его идентифицировать. Иными словами, все варианты косвенной идентификации оказались вне рамок правовой защиты.

С принятием данного Закона стало возможным обрабатывать персональные данные не просто с согласия лица, а лишь с согласия в письменном виде, что, видимо, было призвано повысить защищенность прав граждан.

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

3 этап. Формирование комплексного института законодательства о персональных данных.

Постепенное ”насыщение“ законодательства отдельными нормами о персональных данных, а также разрозненный характер имеющегося регулирования привели к необходимости упорядочения имеющегося нормативного массива, что завершилось принятием Закона Республики Беларусь от 7 мая 2021 г. № 99-З ”О защите персональных данных“. Данный Закон стал визитной карточкой соответствующего института законодательства, комплексно урегулировав вопросы обработки персональных данных.

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

Наконец нельзя не обратить внимание и на положения УК и КоАП. Новый КоАП, принятый в 2021 году, предусмотрел самостоятельную статью (ст. 23.7), устанавливающую ответственность за нарушение законодательства о персональных данных. В данной статье закреплена ответственность как для физического, так и для юридического лица, а максимальный размер штрафа в случае незаконного распространения персональных данных составляет 200 базовых величин.

Кроме того, в 2021 году УК дополнен двумя самостоятельными составами, предусматривающими ответственность за незаконные

действия в отношении персональных данных и за несоблюдение мер обеспечения их защиты.

Появление отдельного Закона, посвященного защите персональных данных, и увеличение числа нормативных правовых актов, регулирующих различные аспекты обработки персональных данных, обусловили необходимость внесения в Единый правовой классификатор Республики Беларусь, утвержденный Указом Президента Республики Беларусь от 4 января 1999 г. № 1, самостоятельной позиции 10.03.08.05 ”Персональные данные и их защита“.

Преамбула

В преамбуле комментируемого Закона отражены цели его принятия:

защита персональных данных;

защита прав и свобод физических лиц при обработке их персональных данных.

Сама по себе защита персональных данных вряд ли может рассматриваться как самостоятельная цель. В конечном итоге защищаются не сами персональные данные, а граждане, их права. Защита данных – это лишь механизм (инструмент) защиты прав человека. Наиболее показательным в этом отношении являются названия соответствующих международных актов в этой сфере. Так, фактически единственный обязательный международный документ в этой сфере – Конвенция о защите физических лиц при автоматизированной обработке персональных данных (подписана в г. Страсбурге, 28 января 1981 г.), направлен именно на защиту граждан, а не самих данных.

В этой связи указанные в преамбуле цели следует рассматривать не как самостоятельные и обособленные, а в качестве тесно взаимосвязанных и взаимообусловленных.

Перечисленные в преамбуле цели, на первый взгляд, могут показаться излишними и как бы сами собой разумеющимися.

Однако в действительности в восприятии населения предназначение Закона не так очевидно. Интересно, что первоначально законопроект имел другое название – ”О персональных данных“. Результаты публичного обсуждения проекта Закона показали, что для многих граждан разрабатываемый акт ассоциировался с желанием государства собирать информацию о своих гражданах и контролировать их, расширением возможностей для онлайн-слежки.

В этой связи изменение названия Закона и указание в преамбуле, что его целью является именно защита персональных данных, прав физических лиц призвано ”развеять“ подобные суждения и показать действительное предназначение этого акта.

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения

Комментарий к статье 1

Биометрические персональные данные.

В Законе биометрические персональные данные определяются как информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и другое).

Отпечатки пальцев рук, ладоней, радужная оболочка глаза и иные подобные характеристики человека являются неповторимыми, по ним можно однозначно идентифицировать личность. Вместе с тем именно уникальность и неповторимость таких данных требует особого внимания со стороны государства к регулированию их использования.

Утечка биометрических данных может иметь ощутимые последствия для заинтересованного лица. Биометрические персональные данные в силу своей неизменности и неоспоримости могут быть использованы, например, для возникновения сложно опровергаемых обвинений, осуществления мошеннических действий (появляется возможность авторизации под чужой личностью). При этом, если биометрические образцы гражданина будут ”украдены“, то их невозможно отменить либо выдать новые (документ заменить можно, а отпечаток пальца – нет), и такой гражданин может лишиться возможности надежно себя идентифицировать.

Для отнесения персональных данных к биометрическим данным необходимо, чтобы одновременно выполнялись два условия:

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

такая информация используется для уникальной идентификации соответствующего лица.

Последний признак предполагает наличие специальных технических средств, обеспечивающих уникальное сопоставление отпечатков пальцев и другого с имеющимся в базе образцом.

На практике весьма распространенной ошибкой является, например, отнесение к биометрическим персональным данным ксерокопий или отсканированных копий страниц паспортов, удостоверений с фотографиями. В качестве обоснования делается ссылка

на определение биометрических персональных данных, где изображение приводится как пример таких данных. Однако поскольку в таких случаях не осуществляется уникальная идентификация субъекта (как правило, происходит просто визуальное сопоставление фотографии на документе и лица, предъявившего такой документ), то оснований для отнесения фотоизображений к биометрическим персональным данным нет. Но они остаются персональными данными и на них распространяется действие Закона.

Справочно:

Как отмечается в п. 51 преамбулы к GDPR, обработка фотографий не должна считаться обработкой особых категорий персональных данных, так как они охвачены определением понятия "биометрические данные" только когда они обрабатываются посредством особых технических средств, позволяющих провести уникальную идентификацию или аутентичность физического лица.

Иная ситуация складывается, например, когда работнику выдается пропуск и при прохождении проходной с использованием специального программного обеспечения осуществляется распознавание лица посетителя и сопоставление его с образцом, сохраненным в базе данных. В такой ситуации имеет место обработка биометрических персональных данных.

Другими примерами биометрических персональных данных являются случаи включения телефона по отпечатку пальца, сканирование радужной оболочки глаз и др.

В ряде случаев в качестве биометрических персональных данных может использоваться голос. Такая возможность предусмотрена, например, Инструкцией об использовании программно-аппаратных средств и технологий, проведении процедур удаленной идентификации, удаленного обновления (актуализации), утвержденной постановлением Правления Национального банка Республики Беларусь от 19 сентября 2019 г. № 379 (абзац третий ч. 1 п. 2), в которой в качестве биометрических персональных данных наряду с фото- и видеоизображением допускается использование голоса.

Отнесение сведений к персональным данным или биометрическим персональным данным имеет важное практическое значение.

Прежде всего биометрические персональные данные являются разновидностью специальных персональных данных. Закон устанавливает в ст. 8 более ограниченный круг оснований для обработки специальных персональных данных по сравнению с обычными персональными данными (ст. 6). Так, например, Закон не предусматривает возможности обработки специальных персональных данных на основании заключенного с субъектом персональных данных договора.

Кроме того, согласно п. 3 ст. 8 Закона обработка специальных персональных данных допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных.

Наконец, к информационным ресурсам (системам), содержащим специальные персональные данные, предъявляются более серьезные требования с точки зрения технической защиты информации, что влияет на стоимость выполнения соответствующих мероприятий.

Блокирование персональных данных.

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

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

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

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

В отличие от удаления персональных данных, когда либо сам носитель данных уничтожается, либо данные необратимо стираются или иным образом удаляются (без возможности их восстановления), при блокировании персональные данные сохраняются. При этом администратором ресурса (системы) ограничивается доступ к таким данным и в дальнейшем они просто хранятся без возможности их использования.

Генетические персональные данные.

Генетические персональные данные определяются как 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.

Генетические персональные данные являются разновидностью специальных персональных данных и, соответственно, их обработка может осуществляться лишь с согласия лица или по основаниям, предусмотренным ст. 8 Закона.

Примером обработки генетических персональных данных могут быть положения Закона ”О здравоохранении“, в соответствии с которыми гражданам Республики Беларусь гарантируется медико-генетическая диагностика по медицинским показаниям в государственных учреждениях здравоохранения в целях медицинской профилактики возможных наследственных заболеваний у потомства.

Генетические персональные данные имеют определенную специфику в сравнении с иными данными, поскольку при обработке данных одного лица можно получить информацию не только о нем (например, о наследственных заболеваниях), но и о его родственниках. Иными словами, при даче согласия на обработку генетических данных человек фактически разрешает обработку информации и о своих родственниках.

В этой связи норма п. 3 ст. 8 Закона о том, что обработка специальных персональных данных допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных, в отношении обработки генетических данных особенно актуальна.

Обезличивание персональных данных[3] – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обезличиванию в настоящее время придается важное значение в вопросе минимизации рисков, связанных с обработкой персональных данных. Как отмечается в литературе, первое правило в защите персональных данных – не собирать такие данные, если они тебе не нужны, второе правило – если вам действительно нужны персональные данные, то начните с псевдонимизации этих данных[4]. В целом признается, что псевдонимизация является основополагающим

[3] В международных актах в контексте обезличивания используется термин псевдонимизация (см. GDPR, Конвенцию о защите физических лиц при автоматизированной обработке персональных данных). Данный термин отличают от анонимизации, то есть действий, в результате которых невозможно установить субъект, к которому данные относятся.

[4] Pseudonymous data: processing personal data while mitigating risks [Электронный ресурс]. – Дата доступа: 11.11.2022.

методом снижения рисков, связанных с обработкой персональных данных, особенно в случае их утечки.

Среди наиболее важных документов в этой сфере можно упомянуть Мнение о технологии анонимизации (Opinion 05/2014 on Anonymisation Techniques) от 10 апреля 2014 г.[5], принятое Рабочей группой 29 (WP 29) Директивы 95/46 (орган, предшествовавший Европейскому Совету по защите данных, – EDPB, созданному в соответствии с GDPR), Руководство по анонимизации и псевдонимизации (Guidance on Anonymisation and Pseudonymisation), утвержденное в 2019 году Ирландской комиссией по защите данных[6]. Также представляет интерес совместный документ испанского органа по защите персональных данных и европейского инспектора по защите данных (AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation)[7].

В Беларуси методы обезличивания персональных данных предусмотрены в приложении 5 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному Приказом № 66. К ним отнесены:

введение идентификаторов. Наиболее простой схемой обезличивания является, например, замена ФИО неким идентификатором и создание таблицы соответствия данных идентификаторов и замененных данных. Данный метод применяют при относительно небольшом количестве параметров персональных данных, чтобы не перегружать таблицу соответствия;

изменение состава. В этом случае определенные данные или удаляются из базы данных, или меняются на другие данные по заранее установленному алгоритму;

декомпозиция. При данном методе база персональных данных делится на несколько частей с отдельным хранением каждой из них и невозможностью по содержанию только одной таблицы идентифицировать субъекта. Одновременно создается таблица связей между частями разделенной базы данных. Такую модель следует отличать от ситуации, когда базы хоть и разделены и находятся на различных серверах, но имеют логическую связь и потому обрабатываются одновременно с одного рабочего места. В последнем случае говорить об обезличивании нет оснований;

---

[5] Opinion 05/2014 on Anonymisation Techniques [Электронный ресурс]. – Дата доступа: 11.11.2022.

[6] Guidance on Anonymisation and Pseudonymisation [Электронный ресурс]. – Дата доступа: 11.11.2022.

[7] AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation [Электронный ресурс]. – Дата доступа: 11.11.2022.

перестановка. При этой модели разрабатывается механизм перестановки различных показателей в базе персональных данных (замена их местами). В отличие от метода изменения состава сам показатель не изменяется, но меняется его размещение в базе данных;

зашифрование. Шифрование не везде рассматривается как метод обезличивания, ведь основной целью обезличивания является возможность обработки персональных данных, что в данной ситуации затруднительно. В Российской Федерации, например, шифрование признается не методом обезличивания, а средством защиты персональных данных.

В отдельных сферах порядок обезличивания имеет определенную специфику и устанавливается соответствующими регуляторами.

Так, в сфере медицины действует постановление Министерства здравоохранения Республики Беларусь от 28 мая 2021 г. № 64 ”Об утверждении Инструкции о порядке обезличивания персональных данных лиц, которым оказывается медицинская помощь“. Регулятор предусмотрел три метода обезличивания: введение идентификаторов, замена состава, декомпозиция.

В отношении регистра населения порядок обезличивания установлен постановлением Министерства внутренних дел Республики Беларусь от 27 сентября 2012 г. № 341 “Об установлении порядка обезличивания персональных данных, содержащихся в регистре населения”. Так, предусматривается присвоение персональным данным конкретных физических лиц уникальных последовательных номеров, а также исключение из персональных данных определенного объема сведений. В данном случае фактически реализуется метод введения идентификаторов и метод изменения состава.

Конкретный метод обезличивания выбирается оператором в зависимости от целей обработки персональных данных. Методы обезличивания могут применяться каждый по отдельности или комбинироваться друг с другом. При этом важно, чтобы обезличивание могло обеспечивать не только защиту таких данных, но и возможность их обработки. Как правило, чем больше степень обезличивания данных, тем меньше их ценность для анализа. Кроме того, обезличивание должно быть обратимым, иначе это будут уже анонимные данные с совершенно иным правовым режимом.

Довольно распространенным среди правоприменителей является мнение о том, что получившийся в результате обезличивания результат – это более не персональные данные, ведь они не содержат сведений о конкретном лице (его ФИО и др.).

Подобный подход не соответствует Закону, который не выводит обезличенные данные из-под сферы своего действия, чтобы не создавать

возможности для обхода требований Закона. Не случайно в Законе не применяется термин ”обезличенные персональные данные“, а говорится лишь об их обезличивании. И обезличивание названо среди действий с персональными данными, которые охватываются обработкой.

Специфика обработки обезличенных персональных данных находит свое отражение в Законе, допускающем в ряде случаев обработку обезличенных персональных данных без согласия субъектов персональных данных. Так, согласно абзацу тринадцатому ст. 6 Закона допускается обработка персональных данных без получения согласия в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных.

Имеющиеся ошибочные трактовки обезличенных персональных данных как не подпадающих под действие Закона в значительной степени являются экстраполяцией подходов, ранее существовавших в законодательстве об информатизации, на новое законодательство без учета произошедших изменений в регулировании. Так, согласно ранее действовавшей ч. 3 ст. 32 Закона ”Об информации, информатизации и защите информации“ меры по защите персональных данных от разглашения должны приниматься до уничтожения персональных данных, либо до их обезличивания, либо до получения письменного согласия физического лица, к которому эти данные относятся, на их разглашение. Таким образом, закреплялся подход о том, что обезличенные персональные данные не подлежали защите.

Изменение отношения к обезличенным персональным данным во многом связано с развитием информационных технологий и расширением возможностей деобезличивания данных. Растет число примеров, когда, на первый взгляд, анонимные данные легко превращаются в самые обычные сведения о лицах.

Например, в 2006 году сервис потокового кино опубликовал набор данных, содержащий 10 млн. рейтингов фильмов, сделанных 500 000 клиентами, утверждая, что они были анонимными, но позже обнаружил, что злоумышленнику потребуется лишь немного знаний о подписчике, чтобы иметь возможность идентифицировать запись этого подписчика в наборе данных[8].

В этой связи не соответствует Закону подход, при котором со ссылкой на п. 8 ст. 4 Закона (хранение персональных данных должно осуществляться в форме, позволяющей идентифицировать субъекта персональных данных, не дольше, чем этого требуют заявленные цели обработки персональных данных) после достижения цели обработки персональные данные обезличиваются и продолжают храниться.

[8] AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation [Электронный ресурс]. – Дата доступа: 11.11.2022.

Указанная норма не может применяться, если в рассматриваемой ситуации сохраняется возможность идентификации лица. Вместе с тем, если будет исключена возможность идентификации лица, то такие данные становятся анонимными и могут продолжать храниться, а также использоваться для любых целей по сравнению с теми, для которых они были получены.

Следует учитывать, что применение обезличивания, к сожалению, не влияет на классификацию информационных ресурсов (систем), в которых обрабатываются персональные данные и, соответственно, не изменяет (понижает) требования к технической защите таких ресурсов. Так, если речь идет о специальных персональных данных, то к такому ресурсу (системе) будут применяться требования к ресурсу (системе) 3-спец или 4-спец в зависимости от подключения к открытым каналам передачи данных. В этой связи на сегодняшний день для организации нет серьезных стимулов к внедрению обезличивания, хотя в целом, как уже отмечалось, это весьма эффективный инструмент снижения рисков при обработке персональных данных.

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

Данный термин является одним из ключевых, поскольку именно в процессе обработки персональных данных на оператора возлагаются обязанности по соблюдению требований Закона.

В Законе термин обработка использован как обобщающий. Подобный подход характерен и для большинства международных и зарубежных актов (GDPR, Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ ”О персональных данных“, Закон Республики Молдова от 8 июля 2011 г. № 133 ”О защите персональных данных“ и др.). Интересно, что на стадии подготовки законопроекта в нем в качестве самостоятельных использовались термины ”сбор“, ”обработка“, ”предоставление“ и ”распространение“. Учитывая частоту употребления соответствующих терминов, это существенно усложняло и перегружало текст.

По смыслу Закона действиями с персональными данными являются как действия, которые осуществляются самим человеком, так и действия (операции), выполняемые под контролем оператора (уполномоченного лица) с использованием определенного алгоритма без непосредственного участия человека.

Разновидностями обработки в Законе названы:
сбор;
систематизация;
хранение;
изменение;
использование;
обезличивание;
блокирование;
распространение;
предоставление;
удаление.

Справочно:

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

Следует отметить, что приведенный в Законе перечень разновидностей обработки не носит исчерпывающего характера и является ориентиром для правоприменителя, о чем свидетельствует использованный законодателем оборот ”включая“.

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

Важно учесть, что все действия с персональными данными являются юридически равнозначными. Закон, за редким исключением, не устанавливает отличий в правовых режимах для осуществления таких действий.

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

Выделение общедоступных персональных данных обусловлено возможностью фактически любого лица получить доступ к таким

данным. В этой связи Законом установлен ”облегченный“ правовой режим обработки таких данных.

Прежде всего отнесение персональных данных к общедоступным дает возможность их обработки на основании абзаца девятнадцатого ст. 6 Закона без получения согласия субъекта персональных данных. Такой подход призван ”примирить“ жесткие правила Закона с реалиями повседневной жизни, например, наличием в сети Интернет множества личной информации, которая размещена без нарушения законодательства.

Немаловажным является и тот факт, что в соответствии с ч. 2 п. 1 Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного Приказом № 66, требования данного Положения могут не применяться собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные.

Закон выделяет два вида общедоступных персональных данных:

распространенные самим субъектом персональных данных или с его согласия. В этом случае необходимо сочетание двух признаков.

Первый – факт распространения данных, то есть действий, направленных на ознакомление с персональными данными неопределенного круга лиц. Типичным примером может быть размещение информации о лице в сети Интернет.

Второй признак – данные должны быть распространены самим субъектом или с его согласия. Этот признак вызывает серьезные сложности при его применении на практике, поскольку подтвердить факт распространения данных самим субъектом или с его согласия довольно сложно. В конечном итоге использование оператором находящихся в свободном доступе данных всегда несет в себе элемент риска, поскольку именно на операторе в конечном итоге лежит бремя доказывания законности обработки персональных данных.

В любом случае сам по себе факт доступности персональных данных в сети Интернет не может рассматриваться как подтверждение распространения их самим субъектом персональных данных или с его согласия. Так, например, персональные данные не могут рассматриваться как распространенные самим субъектом, когда информация содержится в пиратской копии базы и в других случаях, когда очевидно, что персональные данные субъекта распространяются не им;

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

распространение персональных данных;

наличие законодательного акта, в соответствии с которым осуществляется распространение.

Законодательные акты по-разному могут описывать возможность распространения персональных данных. В одних случаях необходимость распространения прямо предусматривается в таких актах. Например, Избирательным кодексом Республики Беларусь предусматривается опубликование деклараций о доходах кандидатов в Президенты Республики Беларусь. Законом Республики Беларусь ”Об информации, информатизации и защите информации“ закреплена необходимость указания на сайте государственного органа (организации) информации о руководителе, заместителе руководителя (должность, ФИО, номер служебного телефона).

В других случаях в законодательном акте содержится отсылка к подзаконному акту (например, к акту Совета Министров Республики Беларусь, Национального банка и др.), который призван определить порядок действий с персональными данными и предусматривает необходимость распространения персональных данных. По смыслу Закона подобные ситуации также рассматриваются как распространение в соответствии с требованиями законодательных актов.

Оператор.

Закон выделяет двух субъектов, которые обрабатывают персональные данные, – оператор и уполномоченное лицо[9].

Отнесение лица к оператору или уполномоченному лицу имеет важное правоприменительное значение, поскольку Закон по-разному определяет правовой статус таких лиц, характер их обязательств и степень ответственности.

От этого будет зависеть надлежащее определение правовых оснований обработки, обязанностей лица, осуществляющего обработку персональных данных, в том числе перед субъектами персональных данных и уполномоченным органом по защите прав субъектов персональных данных, ответственность за нарушение Закона, а также правильная организация сотрудничества с другими организациями и физическими лицами, осуществляющими обработку персональных данных.

Определение статуса лица, осуществляющего обработку персональных данных, должно осуществляться в каждом конкретном случае с учетом анализа всех обстоятельств, связанных с обработкой персональных данных. При этом признание такого лица оператором

[9] В европейском законодательстве (GDPR, Конвенция о защите физических лиц при автоматизированной обработке персональных данных) для обозначения аналогичных субъектов использованы термины ”контроллер“ и ”процессор“.

или уполномоченным лицом должно осуществляться, исходя из фактических обстоятельств обработки персональных данных независимо от того, как данные лица будут определены, например, в договоре.

На статус субъекта (оператор или уполномоченное лицо) не влияет и терминология отраслевого законодательства. Так, в Законе ”Об информации, информатизации и защите информации“ применяется термин ”оператор информационной системы“, под которым понимается субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги. Как правило, владельцу информационной системы в рамках законодательства об информации, информатизации и информации соответствует статус оператора в рамках Закона. В свою очередь оператору информационной системы соответствует статус уполномоченного лица.

В соответствии с абзацем восьмым ст. 1 Закона оператором является государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных.

Исходя из названного определения, оператору присущи следующие признаки:

1. статус.

В качестве оператора может выступать как организация, в том числе государственный орган, так и физическое лицо, осуществляющее обработку персональных данных, связанную с профессиональной или предпринимательской деятельностью.

Организация может являться оператором независимо от наличия либо отсутствия коммерческой выгоды от обработки персональных данных, а также от объема обрабатываемых персональных данных.

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

индивидуального предпринимателя;

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

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

Примеры.

а) Физическое лицо осуществляет сбор персональных данных своих родственников для составления ”генеалогического дерева“ в личных целях. Такая деятельность осуществляется для личного использования, не связана с профессиональной или предпринимательской деятельностью и, соответственно, действие Закона на нее не распространяется. Следовательно, данное физическое лицо, осуществляющее обработку персональных данных для указанной цели, не является оператором.

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

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

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

В самом общем виде оператор – это лицо, которое ответственно за обработку персональных данных.

Примеры.

Операторами, в частности, являются:

наниматель при обработке персональных данных своих работников;

учреждение образования при оказании образовательных услуг обучающимся;

учреждение здравоохранения при оказании медицинской помощи пациентам;

организация торговли при обработке персональных данных покупателей при реализации им товаров;

страховщик по отношению к застрахованным лицам.

Используемый оборот ”и (или)“ означает, что на практике могут иметь место следующие варианты действий операторов:

2.1. оператор только организует обработку персональных данных.

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

2.2. оператор организует и осуществляет обработку персональных данных.

Это означает, что оператор не только организует обработку персональных данных (то есть определяет ее ключевые параметры), но и непосредственно осуществляет с персональными данными необходимые операции (например, сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление и т.п.).

Пример.

Организация занимается продажей мебели и ведет базу данных клиентов для осуществления рекламной рассылки. В данном случае организация как оператор самостоятельно организует и осуществляет сбор сведений у клиентов (например, при заключении договоров), вносит соответствующие сведения в базу данных, пользуется такой базой, осуществляет при необходимости удаление персональных данных клиентов.

Тем не менее, это не означает, что оператор при данной модели все действия по обработке осуществляет исключительно самостоятельно. Так, в рассматриваемой ситуации организация может хранить базу своих клиентов на арендованном сервере, владелец которого будет выступать по отношению к ней уполномоченным лицом;

2.3. оператор осуществляет только обработку персональных данных.

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

При этом для признания организации оператором в понимании законодательства о персональных данных не требуется, чтобы в нормативном правовом акте это было прямо предусмотрено.

Пример.

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

При направлении запросов и предоставлении истребуемых персональных данных обработка персональных данных может осуществляться как в силу требований законодательства, так и на основании согласия. В подобных ситуациях отношения "оператор – уполномоченное лицо" не возникают. Как в первом, так и во втором случае организации, запрашивающие информацию, и организации, ее предоставляющие, являются самостоятельными операторами.

Оператор может организовывать и (или) осуществлять обработку персональных данных как самостоятельно, так и совместно с иными операторами. Лиц, совместно обрабатывающих персональные данные, принято называть **совместными операторами (сооператорами).**

Совместные операторы (сооператоры) – это операторы (юридические и (или) физические лица), которые совместно организуют и (или) осуществляют обработку персональных данных.

Типичным примером сооператорства является ведение (использование) общей базы данных несколькими операторами (программы лояльности, базы данных кандидатов на работу и др.).

Пример.

В торговой сети действует программа лояльности (бонусная, скидочная), в которой участвуют все субъекты торговли, входящие в одну группу лиц. При участии в данной программе субъекты торговли являются сооператорами.

Само по себе наличие взаимной выгоды (например, коммерческой), возникающей в результате деятельности, связанной с обработкой персональных данных, не приводит к сооператорству. Так, если юридическое лицо, участвующее в обработке персональных данных, не преследует собственных целей в отношении деятельности по обработке персональных данных, а просто получает оплату за оказанные услуги, оно действует как уполномоченное лицо, а не как совместный оператор.

В отличие от взаимоотношений "оператор – уполномоченное лицо", правовая основа отношений между совместными операторами Законом отдельно не определена. Поэтому на каждого из них возлагаются все обязанности, предусмотренные Законом в отношении операторов,

и каждый из них самостоятельно несет полную ответственность за несоблюдение его требований.

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

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

цели обработки;

персональные данные, которые подлежат обработке;

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

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

Распределение в упомянутом соглашении (договоре) компетенции сооператоров не зависит напрямую от объема обрабатываемых каждым из них персональных данных.

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

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

несет самостоятельное бремя доказывания получения согласия субъекта персональных данных в отношении себя.

Субъекты персональных данных могут требовать восстановления своих нарушенных прав от всех совместных операторов точно так же, как и от любого оператора в отдельности. Распределение ответственности между совместными операторами может быть отражено в заключенном ими соглашении (договоре).

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

Понятие персональных данных является ключевой категорией законодательства о персональных данных. Отнесение информации к персональным данным ”запускает“ применение законодательства о персональных данных, помещая оператора под довольно жесткий контрольный механизм как со стороны субъектов персональных данных, так и со стороны государственных органов.

Поступающие в Национальный центр защиты персональных данных запросы организаций зачастую содержат вопросы об отнесении тех или иных сведений к персональным данным. Характерной чертой многих запросов является стремление заявителей обосновать непризнание конкретных сведений персональными данными и тем самым сузить содержание этого термина.

Довольно распространенными являются ссылки на то, что поскольку та или иная информация не содержит фамилии, имени, отчества, то она не может рассматриваться в качестве персональных данных. Более того, по мнению отдельных организаций, наличие в информации ФИО также не позволяет относить сведения к персональным данным, поскольку возможны совпадения и нет возможности точно установить, о ком идет речь. Еще одним аргументом является указание на изменяемость данных (например, номер телефона может быть передан другому пользователю) и, соответственно, на возможность ошибки.

Позицию сторонников ”узкого“ понимания персональных данных можно отчасти объяснить желанием уменьшить издержки на администрирование работы с личной информацией, снизить риски возможных нарушений законодательства о персональных данных. Кроме того, признание сведений, обрабатываемых в информационной системе, персональными данными влечет необходимость ее аттестации, что требует финансовых затрат. Соответственно, организации пытаются избежать дополнительных издержек, в том числе и посредством ограничения круга сведений, которые необходимо защищать.

Но было бы ошибкой видеть в желании сузить понятие персональных данных только лишь стремление организаций упростить себе жизнь. Важным фактором, который нельзя игнорировать, является и потребность в формальной определенности юридических понятий, затруднительность настройки информационных систем и алгоритмов на оценку конкретной ситуации.

В целом, попытка узкого понимания персональных данных сводится к тому, что к персональным данным может относиться только та информация, которая сама по себе достаточна для идентификации лица и которая содержит, как минимум, его ФИО.

Подобный подход не соответствует законодательству и в условиях развития современных технологий (большие данные, интернет вещей, риски деобезличивания информации и др.), позволяющих сопоставлять и связывать воедино разрозненные блоки информации, в значительной степени обесценивает и делает оторванными от жизни положения законодательства о персональных данных, выводя из-под правовой защиты множество ситуаций, связанных с обработкой личной информации.

Дело в том, что нередко для обработки персональных данных оператору не требуется знать ФИО конкретного лица. Отслеживание поведения на сайтах, оценка предпочтений на основе анализа просмотренной информации позволяют прогнозировать с высокой степенью точности индивидуальные предпочтения и в последующем использовать данную информацию.

Ответом на соответствующие риски, которые несут новейшие технологии, во многих странах становится постепенное расширение круга сведений, которые относятся к персональным данным. Яркой иллюстрацией являются положения наиболее известного акта в сфере защиты персональных данных – GDPR, в котором все онлайн идентификаторы (IP-адрес, файлы cookie и др.) прямо отнесены к персональным данным.

Признаки персональных данных

Анализ дефиниции персональных данных позволяет выделить следующие признаки персональных данных:

информация;

относимость к лицу;

возможность идентификации лица.

Закон не предусматривает ограничений или требований к носителям информации для признания такой информации персональными данными. Таким образом, форма представления информации значения не имеет. Это может быть текстовая информация

на бумажном или электронном носителе, фотоизображение, видеозапись, аудиозапись и др.

Информация, составляющая персональные данные, охватывает как объективные данные (например, имя, возраст, место работы), так и субъективные мнения или оценки (например, уровень платежеспособности, результаты аттестации нанимателем работника).

Для признания информации персональными данными необходимо, чтобы эта информация ”относилась“ к лицу. Этот признак призван ограничить всеобъемлющий характер определения персональных данных.

Информация относится к конкретному лицу, когда эта информация:

об этом человеке (например, фото лица, история его болезни, обстоятельства рождения, место работы и др.);

не о самом лице, но она связана с деятельностью такого лица и может быть использована для оценки или влияния на поведение лица, реализации его прав и обязанностей (например, сведения GPS-навигатора, определяющие место нахождения транспортного средств, могут быть использованы для оценки маршрута водителя, история звонков с рабочего телефона – для оценки использования средств связи нанимателя работником в личных целях).

Рассматриваемый признак исключает отнесение к персональным данным информации, когда такая информация не предполагает оказания влияния на субъекта персональных данных.

Например, изображение на фотографии, иллюстрирующей открытие нового магазина, транспортных средств с различимыми номерами. В данном случае целью обработки не является оценка владельца транспортного средства или оказание на него определенного влияния. Соответственно, такая информация не должна признаваться персональными данными.

Иная ситуация складывается, когда на интернет-ресурсе размещаются фотографии автомобилей с различимыми номерами, которые демонстрируют нарушение автовладельцами правил дорожного движения (так называемые ”доски позора“). Целью размещения таких фото как раз и является привлечение внимания к допущенному нарушению, оказание влияния на лицо в целях недопущения последующих нарушений. Кроме того, соответствующие данные могут использоваться и правоохранительными органами для привлечения владельца транспортного средства к ответственности. Поэтому в этом случае размещение фотографии транспортного средства следует рассматривать как обработку персональных данных.

При решении вопроса о том, относится ли информация к конкретному лицу, следует учитывать различные обстоятельства, в том числе:

содержание информации (ее полнота, детализация, индивидуализированный характер и др.);

цель обработки (предполагается ли воздействие на субъекта и др.);

возможное влияние обработки на конкретного субъекта (возможность наступления неблагоприятных последствий, отказа в реализации прав и др.).

Но не вся информация, которая относится к лицу, будет считаться персональными данными, а лишь та, которая идентифицирует лицо или которая может быть использована для его идентификации.

Идентифицированным является лицо, личность которого известна, которое однозначно выделено среди других лиц (на него можно указать, к нему можно обратиться, мы знаем его и др.).

Наиболее распространенным вариантом использования информации об идентифицированном лице является указание его ФИО в совокупности с другими данными (адрес места жительства, место работы, дата и место рождения), которые однозначно выделяют такое лицо среди других. Например, Ковалев Михаил, который проживает по адресу г. Минск, ул. Руссиянова, 3-24.

Но даже если мы не знаем ФИО лица, то информация о нем может относиться к персональным данным как информация о физическом лице, которое может быть идентифицировано *(подробнее см. комментарий к соответствующему термину)*.

Категория персональных данных тесно связана с информацией о частной жизни и не может быть раскрыта полностью без анализа их соотношения[10].

В юридической литературе высказываются различные мнения относительно соотношения категорий ”информация о частной жизни“ и ”персональные данные“. Представляется, что наиболее обоснована позиция тех авторов, которые полагают, что данные категории частично пересекаются, а частично являются самостоятельными. Так, по мнению Савельева А.И., анализ положений законодательства о персональных данных позволяет сделать вывод, что регулируемые им отношения, с одной стороны, не в полной мере охватывают ситуации, которые подпадают под действие права на неприкосновенность частной жизни,

[10] Вопрос о соотношении рассматриваемых понятий активно обсуждается и в европейской литературе. Дискуссия касается в основном того, состоялось ли на сегодняшний день право на защиту персональных данных в качестве самостоятельного права или становление нового права еще не завершено. При этом можно отметить, что в последнее время наблюдается тенденция к закреплению на конституционном уровне права на защиту персональных данных в качестве самостоятельного, отдельного от права на защиту частной жизни, что нашло отражение, в том числе и в тексте Основного Закона Республики Беларусь.

а с другой – явно выходят за его рамки. Тем самым право на защиту персональных данных приобрело во многом самостоятельное значение[11].

С учетом положений ст. 2 Закона, определяющих сферу его действия, можно представить следующую модель взаимодействия правовых режимов персональных данных и информации о частной жизни.

Сведения о частной жизни, которые обрабатываются с помощью средств автоматизации и не предназначены для личного, семейного, домашнего и иного подобного пользования, фактически будут существовать в режиме удвоения правовой защиты, подпадая одновременно под режим как персональных данных, так и под режим информации о частной жизни.

Сведения о частной жизни, которые обрабатываются без использования средств автоматизации (например, вручную) и без создания системы поиска (например, систематизированных картотек), либо сведения о частной жизни, которые предназначены для личного, семейного, домашнего и иного подобного пользования (например, письма, справочник контактов в телефоне или список контактов в личном электронном почтовом ящике), будут подпадать лишь под правовой режим информации о частной жизни.

Наконец, сведения о лице, которые не касаются его частной жизни, например, информация об образовании, трудовой деятельности и др., будут подпадать лишь под правовой режим персональных данных.

Институты персональных данных и информации о частной жизни отличаются также и по содержанию.

Право на уважение частной жизни состоит из общего запрета на вмешательство в нее с рядом исключений, обусловленных наличием общественных интересов, которые могут оправдывать такое вмешательство в определенных случаях.

Институт персональных данных, напротив, призван обеспечить возможность обработки таких данных, определяя случаи и условия допустимой обработки, а также возлагая на оператора обязанности и предоставляя субъекту персональных данных набор прав, позволяющих контролировать проводимую обработку.

Предоставление персональных данных.

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

[11] Савельев, А. И. Научно-практический постатейный комментарий к Федеральному закону ”О персональных данных“ // КонсультантПлюс. Россия / ЗАО ”КонсультантПлюс“. – М., 2022.

Рассматриваемый термин практически не используется в Законе при формулировании конкретных норм. Исключением является ст. 12 Закона о получении информации о предоставлении персональных данных третьим лицам. Это обусловлено тем, что предоставление персональных данных является разновидностью их обработки и на указанные действия распространяются все положения Закона об обработке.

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

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

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

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

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

Распространение персональных данных.

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

Типичными примерами распространения персональных данных являются случаи размещения персональных данных в открытом доступе в сети Интернет. Как распространение персональных данных будут рассматриваться и ситуации ”перепоста“ информации, содержащей персональные данные, проставление в ее отношении ”лайков“, которые влекут появление данного материала в ленте ”друзей“ пользователя. Вместе с тем, когда настройки приватности ограничивают доступ к информации такого пользователя определенным кругом лиц (”друзей“), то речь будет идти не о распространении, а о предоставлении персональных данных.

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

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

Специальные персональные данные.

Закон не дает определения и не выделяет признаки специальных персональных данных, а просто перечисляет конкретные сведения, которые признаются специальными персональными данными. Это персональные данные, касающиеся:

расовой либо национальной принадлежности;

политических взглядов;

членства в профессиональных союзах;

религиозных или других убеждений;

здоровья;

половой жизни;

привлечения к административной или уголовной ответственности.

К специальным персональным данным относятся также биометрические и генетические персональные данные.

Выделение Законом в отдельную группу специальных персональных данных обусловлено тем, что связанные с ними нарушения потенциально несут повышенный риск для прав и свобод человека. Их раскрытие может привести к дискриминации, травле лица, преследованию за определенные убеждения, разрыву дружеских

или семейных связей и др. В этой связи Законом для обработки специальных персональных данных предусматривается особый правовой режим:

круг оснований для их обработки (п. 2 ст. 8 Закона) уже круга оснований для обработки ”обычных“ персональных данных. Например, нет возможности обработки данной категории персональных данных без согласия лица для целей заключения и исполнения договора;

обработка специальных персональных данных допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных (п. 3 ст. 8 Закона). Как правило, это выражается в ограничении круга лиц, имеющих доступ к таким данным, сокращении срока их хранения, использовании методов обезличивания, получении согласия в письменной форме, если обработка осуществляется на основе согласия, и др.;

информационные системы, содержащие специальные персональные данные, относятся к более высокому классу типовых информационных систем (4-спец) по сравнению с ”обычными“ персональными данными и требуют реализации более серьезных мер по технической защите таких данных.

Субъект персональных данных.

Согласно Закону субъект персональных данных – это физическое лицо, в отношении которого осуществляется обработка персональных данных.

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

Важное практическое значение имеет вопрос о том, является ли индивидуальный предприниматель субъектом персональных данных. С учетом отсутствия каких-либо оговорок в Законе индивидуальных предпринимателей также следует относить к субъектам персональных данных, поскольку они охватываются формулировкой физические лица[12]. В свою очередь, обработка данных, в том числе контактных

[12] При этом круг правовых оснований для обработки их данных будет несколько отличаться, поскольку законодательство предусматривает, что часть информации об индивидуальных предпринимателях

данных юридического лица, не влечет признания его субъектом персональных данных и, соответственно, такое лицо не пользуется механизмом защиты, предусмотренным Законом.

По общему правилу, умершие не признаются субъектами персональных данных[13]. Тем не менее, Закон хоть и ограниченно, но регулирует обработку персональных данных таких лиц. Так, если отсутствуют правовые основания для обработки персональных данных умершего, то их обработка возможна с согласия одного из наследников, близких родственников или иных лиц, указанных в ч. 1 п. 9 ст. 5 Закона. В этом случае указанные лица пользуются правами субъекта персональных данных.

Субъект персональных данных – активный участник правоотношений, связанных с обработкой персональных данных. Независимо от правовых оснований обработки (в том числе, когда обработка осуществляется без согласия лица) он наделяется целым набором прав, что позволяет ему влиять на сбор и использование данных о нем. Это отражает одну из ключевых идей законодательства о персональных данных – принадлежность персональных данных непосредственно человеку и недопустимость отторжения личной информации от него.

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

При трансграничной передаче персональные данные ”выходят“ из-под сферы действия белорусского законодательства и подпадают под юрисдикцию другого государства (законодательство ”не следует“ за данными). При отсутствии правил о трансграничной передаче существовала бы возможность обхода требований Закона посредством переноса обработки в иные страны с упрощенными требованиями к обработке данных.

В этой связи институт трансграничной передачи персональных данных направлен на обеспечение защиты прав субъектов персональных данных на уровне не ниже, чем предусмотрен законодательством Беларуси.

Примерами трансграничной передачи могут быть следующие ситуации:

должна быть общедоступна (например, информация в Едином государственном регистре юридических лиц и индивидуальных предпринимателей, включая адрес места жительства).

[13] Ряд зарубежных законов прямо указывают, что субъектом персональных данных могут быть только живые люди.

использование облачной инфраструктуры для персональных данных, когда соответствующие серверы размещаются за пределами Беларуси;

направление организацией, входящей в группу компаний, персональных данных работников материнской компании, расположенной в другой стране;

хранение собранных данных клиентов на Google Диск, Яндекс Диск и др.

Трансграничная передача персональных данных характеризуется следующими признаками.

1. Передача персональных данных.

1.1. Суть трансграничной передачи персональных данных в том, что данные, собранные (находящиеся) на территории одного государства, передаются с территории этого государств на территорию иного государства. При их обработке с использованием сети Интернет такие данные с сервера, размещенного на территории Беларуси, передаются на сервера, расположенные на территории другого государства, где осуществляется обработка таких данных, в том числе хранение.

В этой связи не является трансграничной передачей технический ”транзит“ данных через территорию иных государств без доступа к содержанию передаваемой информации и ее сохранения.

1.2. Передача персональных данных осуществляется оператором или уполномоченным лицом.

Передача персональных данных является разновидностью их обработки, которая в соответствии с Законом осуществляется лишь оператором (уполномоченным лицом). В этой связи, если персональные данные передаются самим субъектом персональных данных, институт трансграничной передачи не применяется. В подобных ситуациях имеет место не трансграничная передача, а трансграничный сбор от субъекта персональных данных.

Таким образом, не может классифицироваться как трансграничная передача персональных данных, например, регистрация гражданином в социальной сети, на сайте, заказ билетов у зарубежной авиакомпании, покупка товаров в Aliexpress и др. При этом не имеет значения, с помощью каких ресурсов или мессенджеров собираются данные (Google, Yandex, Viber и др.).

На применимость правил о трансграничной передаче не влияют ни цели обработки, ни ее характер (возмездный или безвозмездный), ни возможность сохранности данных на территории Беларуси.

1.3. Сам по себе факт распространения персональных данных на сайте, расположенном на сервере в Беларуси, и доступность данных

на территории других стран не может рассматриваться как трансграничная передача. В этом случае ”получение“ персональных данных, например, скачивание, является результатом активных действий зарубежного пользователя. Такая ситуация квалифицируется как распространение персональных данных, что в свою очередь требует наличия надлежащего правового основания.

2. Передача осуществляется на территорию иностранного государства.

Трансграничная передача имеет место лишь в случае передачи данных с территории Беларуси на территорию иностранного государства, но не в обратном порядке.

Так, например, при передаче в Беларусь персональных данных независимо от того, с территории какого государства они передаются, положения ст. 9 Закона не применяются.

Получателем персональных в иностранном государстве может быть любой субъект (международная организация, государственный орган, иная организация, физическое лицо). Следует, однако, учитывать, что если трансграничная передача осуществляется в процессе личного, семейного, домашнего и иного подобного использования, то Закон, в том числе и правила о трансграничной передаче данных, не применяются *(подробнее см. комментарий к ст. 2 Закона)*.

Удаление персональных данных.

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.

Механизм удаления во многом зависит от того, в каком виде и в каких документах содержатся персональные данные.

1. Удаление персональных данных, содержащихся в документах, включенных в номенклатуру дел с установленными сроками хранения.

1.1. Удаление персональных данных, содержащихся в документах на бумажных носителях.

Государственные органы, иные организации и индивидуальные предприниматели согласно ст. 26 Закона Республики Беларусь от 25 ноября 2011 г. № 323-З ”Об архивном деле и делопроизводстве“ (далее – Закон об архивах) обязаны соблюдать нормы и требования, предъявляемые к порядку оформления документов, их обработке и хранению. В развитие этой статьи постановлением Министерства юстиции Республики Беларусь от 19 января 2009 г. № 4 утверждена

Инструкция по делопроизводству в государственных органах, иных организациях (далее – Инструкция по делопроизводству).

На основании положений абзаца третьего п. 16 Инструкции по делопроизводству удаление персональных данных из документов, по общему правилу, осуществляется одновременно с уничтожением таких документов.

Порядок уничтожения документов и дел с истекшими сроками хранения определен Правилами работы архивов государственных органов и иных организаций, утвержденными постановлением Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 143, и главой 16 Инструкции по делопроизводству. Так, предусматривается, что документы и дела с истекшими сроками хранения включаются в акт о выделении к уничтожению, если установленный срок их хранения истек к 1 января года, в котором этот акт составлен.

После составления акта отобранные к уничтожению документы и дела передаются организациям, ведающим заготовкой вторичного сырья. Вместе с тем в целях обеспечения защиты персональных данных документы на бумажных носителях, содержащие специальные персональные данные, иные персональные данные, распространение которых создает высокий риск для прав и свобод физических лиц (круг таких данных определяется самим оператором), целесообразно передавать организациям, ведающим заготовкой вторичного сырья после предварительного измельчения.

1.2. Удаление персональных данных, содержащихся в документах в электронном виде (за исключением удаления из систем хранения данных, иного серверного оборудования).

Согласно Инструкции по делопроизводству документы в электронном виде подлежат хранению в течение сроков, установленных для аналогичных документов на бумажном носителе. Выделение к уничтожению электронных дел и документов в электронном виде осуществляется в соответствии с требованиями Инструкции по делопроизводству.

Уничтожение документов в электронном виде и электронных дел, не подлежащих хранению, осуществляется согласно главе 9 Правил работы с документами в электронном виде в архивах государственных органов, иных организаций, утвержденных постановлением Министерства юстиции Республики Беларусь от 6 февраля 2019 г. № 20.

1.3. Удаление персональных данных, содержащихся в электронных документах.

В отношении удаления персональных данных, содержащихся в электронных документах, следует руководствоваться положениями п.п. 89 и 90 Инструкции о порядке работы с электронными документами

в государственных органах, иных организациях, утвержденной постановлением Министерства юстиции Республики Беларусь от 6 февраля 2019 г. № 19, определяющей порядок отбора электронных дел к уничтожению и составления акта о выделении к уничтожению электронных документов и электронных дел.

2. Удаление персональных данных из документов, не включенных в номенклатуру дел с установленными сроками хранения.

На персональных компьютерах, в общих сетевых ресурсах, на бумажных носителях у работников могут накапливаться материалы, послужившие основанием для разработки документов, а также их копии, проекты писем и др. В целях эффективного выполнения оператором своих обязанностей по удалению персональных данных после уничтожения документов и дел с истекшими сроками хранения подлежат удалению (уничтожению) и эти материалы, и копии, и проекты.

Порядок удаления (уничтожения) таких материалов определяет оператор.

Проведение проверок своевременного удаления (уничтожения) документов, материалов к ним, их копий и проектов целесообразно возлагать на лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных.

3. Удаление персональных данных, содержащихся в информационных системах (ресурсах).

В соответствии с Законом оператор обязан удалить персональные данные при отсутствии правовых оснований для их обработки. Данное требование распространяется в том числе и на ситуации, когда персональные данные содержатся в информационных ресурсах (системах) соответствующего оператора (например, локальной вычислительной сети, интернет-сайте, бухгалтерской информационной системе, системе электронного документооборота, системе видеонаблюдения и др.).

Порядок удаления информации из информационных систем (ресурсов) в законодательстве не определен, за исключением отдельных государственных информационных систем (ресурсов). В этой связи в целях выполнения соответствующей обязанности оператору следует самостоятельно разработать порядок удаления персональных данных. Он может быть предусмотрен в отдельном локальном правовом акте, локальном акте, определяющем порядок функционирования такой информационной системы (ресурса), в политике информационной безопасности.

Законодательством не предусматривается в этих случаях обязательное составление акта об удалении на бумажном носителе. Так,

в случае автоматического удаления персональных данных из информационной системы (ресурса) достаточно указать сроки хранения этой информации. В частности, в системах видеонаблюдения запись видеоизображения осуществляется в циклическом режиме, когда самые старые записи заменяются новыми.

В иных случаях целесообразно создавать лог-файлы и настраивать их ведение таким образом, чтобы в эти файлы вносились записи об удалении персональных данных, но без информации, позволяющей идентифицировать физических лиц (например, запись сведений о дате удаления и объеме удаленных сведений).

Составлять акт об удалении персональных данных целесообразно в случаях разового удаления персональных данных, например удаления на основании заявления субъекта персональных данных, на основании требования Центра, в иных случаях, когда необходимо подтвердить факт совершения этого действия.

Из информационных систем (ресурсов) персональные данные следует удалять таким образом, чтобы их невозможно было восстановить обычному пользователю. Например, простое ”перемещение в корзину“ не является надлежащим выполнением обязанности по удалению персональных данных. При этом сама по себе возможность применения специальных технических средств по восстановлению информации не может рассматриваться как свидетельство невыполнения оператором обязанности по удалению персональных данных.

Законом (ч. 2 п. 2 ст. 13) предусматривается, что при отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование.

В констексте Закона данная мера является альтернативой удалению, когда удаление по техническим причинам невозможно (например, может нарушить работу всей системы). По своим последствиям блокирование является равнозначным удалению и должно исключать использование, предоставление, распространение персональных данных и др.

Уполномоченное лицо.

В соответствии с абзацем шестнадцатым ст. 1 Закона 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.

К основным признакам уполномоченного лица можно отнести следующие:

1. статус.

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

Уполномоченное лицо должно быть отдельным юридическим или физическим лицом по отношению к оператору. При этом на возможность признания организации уполномоченным лицом не влияет ее взаимосвязь с оператором (аффилированное лицо, зависимое хозяйственное общество, дочернее хозяйственное общество, статус учредителя и др.).

С точки зрения законодательства о персональных данных не рассматриваются в качестве самостоятельных операторов или уполномоченных лиц работники организации. Оператором в данном случае выступает наниматель, у которого работник работает по трудовому договору.

Что касается физических лиц, выполняющих работу на основании гражданско-правового договора, то их статус при обработке персональных данных должен определяться в каждом конкретном случае. Если такое лицо осуществляет обработку персональных данных под контролем оператора и с использованием принадлежащих оператору информационных ресурсов, то его по аналогии с работниками оператора следует рассматривать как ”часть“ оператора. Данный подход подтверждается и положениями ст. 17 Закона, в соответствии с которыми на оператора возложена обязанность по ознакомлению с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, а также по обучению не только работников, но и иных лиц, осуществляющих обработку персональных данных;

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

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

Примеры.

а) Организация ”А“ продает товары через Интернет, предлагая доставку товара курьером. С целью исполнения обязательств по доставке организация ”А“ запрашивает у покупателя контактные данные, необходимые для доставки, – адрес, собственное имя и контактный телефон. Поскольку организация ”А“ не имеет собственной курьерской службы, она нанимает организацию ”Б“, которая имеет свой штат курьеров и занимается доставкой товаров. Организация ”А“ передает собранные ею персональные данные покупателей организации ”Б“ для доставки товара.

В данном случае организация ”А“ определила цель обработки (доставка товара), лиц, чьи персональные данные будут обрабатываться (покупатели), и перечень обрабатываемых персональных данных (адрес, имя и контактный телефон). В свою очередь, организация ”Б“, используя собранные персональные данные, от имени организации ”А“ доставила товар. В этой связи организация ”А“ является оператором, организация ”Б“ – уполномоченным лицом.

б) Организация ”А“ передала системное администрирование локальной сети на аутсорсинг организации ”Б“. Для организации ”Б“ обработка персональных данных, содержащихся в локальной сети организации ”А“, не является целью, однако возложение обязанностей по администрированию локальной сети не может осуществляться без доступа к ним. В данной ситуации организация ”А“ является оператором, а организация ”Б“ – уполномоченным лицом, осуществляющим обработку персональных данных в интересах оператора.

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

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

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

Передача части своих функций, связанных с обработкой персональных данных, на аутсорсинг другой организации (ведение бухгалтерского учета, системное администрирование локальной сети, транспортные услуги, IT-поддержка и т.п.) является распространенной

практикой для организаций. В большинстве таких случаев организация-исполнитель услуг действует в соответствии с инструкциями (поручениями, указаниями и т.п.) организации-заказчика, закрепленными в договоре, от его имени или в его интересах. В подобных ситуациях организация-заказчик выступает оператором, а организация-исполнитель является уполномоченным лицом.

Вместе с тем не во всех случаях взаимоотношения организации-заказчика и организации-исполнителя соответствуют конструкции ”оператор – уполномоченное лицо“. Отношения могут также строиться и по модели ”оператор – оператор“, когда каждая организация действует в своих интересах и самостоятельно определяет ключевые параметры обработки персональных данных.

Пример.

Организации заключили договор поставки. В договоре, доверенности и первичных учетных и иных документах, прилагаемых к договору, содержатся в том числе персональные данные представителей этих организаций (сторон договора). При передаче персональных данных организациями друг другу каждая из них осуществляет обработку этих персональных данных для собственных целей (заключение договора и т.п.) и, соответственно, при данной обработке каждая из них выступает в качестве оператора.

Важной особенностью взаимоотношений между оператором и уполномоченным лицом является то, что после окончания обработки уполномоченное лицо должно прекратить обработку соответствующих персональных данных (такие данные передаются оператору либо удаляются (блокируются). Порядок подтверждения передачи, удаления или блокирования персональных данных целесообразно определить в договоре между оператором и уполномоченным лицом. Как правило, эти процессы оформляются соответствующим актом или отчетом.

Законодательными актами могут быть предусмотрены исключения из правила о необходимости удаления (блокирования) персональных данных, обрабатываемых уполномоченным лицом. Например, если организация (уполномоченное лицо) заключала по поручению оператора договоры, то в силу требований законодательства в сфере архивного дела и делопроизводства она обязана сохранять такие договоры в течение определенного срока.

Физическое лицо, которое может быть идентифицировано, – физическое лицо, которое может быть прямо или косвенно определено, в частности, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Данная формулировка Закона предусматривает отнесение к персональным данным информации о лице, которое может быть:

прямо определено;

косвенно определено.

Физическое лицо, которое может быть прямо определено, – это лицо, личность которого можно установить на основании имеющейся информации без использования дополнительных сведений. Иными словами, на основании данной информации мы можем узнать ФИО соответствующего лица.

Например, заведующий кафедрой криминалистики юридического факультета БГУ, менеджер ООО ”Астра“ и номер его телефона, одинокий пенсионер, проживающий по адресу: ул. Никифорова, д. 18, кв. 47, лучший бомбардир футбольного клуба ”Минск“ в 2020–2021 гг. и др.

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

Так, поскольку в большинстве случаев имя и фамилия не являются уникальными, то для определения конкретного лица может потребоваться получение дополнительной информации, например, даты и места рождения, информации о месте работы, учебы, месте жительства. Схожим образом знания места работы (например, юрисконсульт такой-то организации) в ряде случаев недостаточно для идентификации лица, если соответствующих работников в организации несколько, и может потребоваться дополнительная информация (например, имя).

Когда мы говорим о возможности получения дополнительной информации, речь идет о легальной возможности, а не о незаконных ”пробивах“ по базам или других ”серых“ схемах. В качестве примеров информации, к которой может получить доступ заинтересованное лицо, можно отметить:

информацию, находящуюся в публичных реестрах или ресурсах (единый государственный регистр юридических лиц и индивидуальных предпринимателей, реестр движимого имущества, обремененного залогом, и др.);

информацию, содержащуюся в сети Интернет в открытом доступе (страницы социальных сетей, сайты организаций и др.);

информацию, распространяемую государственными органами и организациями (например, статистические данные);

информацию, которая доступна конкретному пользователю, имеющему доступ к соответствующим данным (данные переписки, предшествующий опыт общения и др.).

При этом для признания сведений персональными реальная идентификация человека не требуется. Достаточно наличия соответствующей возможности.

Закон предусматривает ряд идентификаторов, которые позволяют прямо или косвенно определить лицо:

ФИО;

дата рождения;

идентификационный номер;

один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Так, например, к признакам, характерным для физической идентичности, могут относиться пол, рост, вес, цвет волос, состояние здоровья (например, высокий мужчина с длинными темными волосами из нашей учебной группы). Об экономической идентичности может свидетельствовать владение транспортным средством, объектами недвижимости, уровень заработной платы, номер кредитной карточки и др.). Социальная идентичность может характеризоваться посредством ссылок на вероисповедание, национальность, политические взгляды, социальные связи, высказывания и комментарии, сексуальную ориентацию.

Это не полный перечень соответствующих идентификаторов. Можно выделить и иные сведения, которые используются для прямого или косвенного определения лица, например:

номер телефона, почтовый адрес, адрес электронной почты;

номер паспорта и дата его выдачи;

история посещения сайтов, поисковые запросы;

IP-адрес, идентификатор файла cookie и др.

Оценка того, достаточно ли тех или иных сведений для прямого или косвенного определения лица осуществляется лишь в отношении конкретной ситуации и только применительно к конкретному оператору. Информация, которая позволяет идентифицировать человека в одном контексте, может не идентифицировать человека в другом случае. Так, например, имя и фамилия Михаил Ковалев являются весьма распространенным. Таких данных вполне достаточно для идентификации лица в небольшом коллективе, например, классе или даже в школе, но явно недостаточно для идентификации лица среди населения города или страны.

На то, можно ли идентифицировать человека с помощью конкретной информации, в значительной степени влияет, кто владеет этой информацией и имеет к ней доступ. Когда информация размещается публично, доступ к ней может получить любое лицо. Соответственно, это может затруднить определение того, к какой дополнительной информации люди могут иметь доступ и какие у них могут быть мотивы для идентификации человека.

Для примера рассмотрим вопрос об отнесении к персональным данным адреса электронной почты субъекта и номера его мобильного телефона.

Адреса электронной почты может быть достаточно, чтобы идентифицировать кого-то, когда в электронном адресе отражаются данные о лице (ФИО, дата рождения, место работы и др.) (например, Kovalev12.10.1983@cpd.by). В этом случае обработка такой информации является обработкой персональных данных.

В других ситуациях информация лишь теоретически может быть связана с лицом и субъект может не обладать реальными законными возможностями получения информации с целью идентификации лица. В таком случае данные не признаются персональными. Например, info@cpd.by, 1237@gmail.com.

Что касается номера мобильного телефона, то данная информация имеет специфику по сравнению с иными персональными данными, обусловленную возможностью связаться непосредственно с субъектом независимо от его желания. Данная возможность может использоваться не только для выяснения личности такого лица, но и в иных целях (оказания влияния на принятие решений, например, участвовать в голосовании и голосовать определенным образом, а также рассылки рекламных или иных нежелательных сообщений). Это может причинять беспокойство, вызывать раздражение, недовольство попытками завладеть вниманием человека. Кроме того, неправомерное использование номера мобильного телефона может нарушить интересы третьих лиц, например, семьи субъекта.

В этой связи, если обработка номера телефона может иметь воздействие на лицо, причинять ему беспокойство и др., то такую обработку следует рассматривать как обработку персональных данных. Это позволяет делать внешние коммуникации ожидаемыми и предсказуемыми.

Подводя итог, можно отметить, что универсального перечня сведений, которые должны признаваться персональными данными, нет и, наверно, не может быть. Как следствие, вопрос об отнесении сведений к персональным данным должен рассматриваться в каждом конкретном случае с учетом всех обстоятельств.

Статья 2. Предмет регулирования настоящего Закона

Комментарий к статье 2

1. Законом предусматривается, что его действие будет распространяться на обработку персональных данных, осуществляемую операторами:

с использованием средств автоматизации. Термин ”средства автоматизации“ в Законе не раскрывается. Ориентиром может выступать его определение в отдельных подзаконных актах. Например, Инструкцией о порядке технической эксплуатации средств телекоммуникации в органах внутренних дел, утвержденной приказом Министерства внутренних дел Республики Беларусь от 17 сентября 2012 г. № 333, предусмотрено, что средства автоматизации – совокупность технических и программных средств, предназначенных для сбора, ввода, обработки, хранения, отображения, регистрации и документирования информации, а также для обмена данными в информационных сетях и системах.

Фактически обработкой с использованием средств автоматизации будут признаваться любые действия с персональными данными, осуществляемые в электронной форме.

Разновидностью обработки с использованием средств автоматизации являются и ситуации, когда только часть операций по обработке персональных данных осуществлялась с использованием средств автоматизации (средства автоматизации применяются на одном из этапов). Например, распечатанные списки неплательщиков жилищно-коммунальных услуг размещаются на доске объявлений возле подъезда, информация об участниках судебного разбирательства вывешивается в здании суда. В подобных случаях следует исходить из того, что вывешенная информация будет являться результатом обработки с использованием средств автоматизации (компьютера и др.) и, следовательно, на такие отношения должен распространяться Закон;

без использования таких средств, если при этом обеспечивается поиск персональных данных и (или) доступ к таким персональным данным по определенным критериям (картотеки, списки, базы данных, журналы и др.).

Действие Закона не ограничивается сферой использования средств автоматизации. Закон распространяется также и на обработку персональных данных без их использования, но только если при этом персональные данные систематизированы и обеспечивается их поиск и (или) доступ к таким данным по определенным критериям.

Возможность поиска и доступа к персональным данным по четким критериям (алгоритмам) приводит к тому, что обработка персональных

данных на бумажных носителях по своей сути мало чем отличается от аналогичной обработки с использованием средств автоматизации (оперативность поиска, простота и легкость доступа, возможность добавления или исключения позиций и др.). Это и обуславливает распространение на такую обработку действия Закона.

Примерами систематизации персональных данных без использования средств автоматизации могут быть:

ведение журнала посетителей на вахте (в журнале отражается время прихода и ухода, ФИО посетителя и данные подразделения, которое он посещает) – поиск информации и доступ к ней осуществляется на основе хронологического критерия (время посещения);

хранение трудовых книжек в отделе кадров (расставлены по подразделениям, а внутри подразделений – по ФИО) – поиск данных и доступ к ним реализуется по двум критериям;

хранение медицинских карточек пациентов в поликлинике (размещены по участкам (адресам) и ФИО) – поиск данных осуществляется по двум критериям.

2. Закон не распространяется на отношения, касающиеся обработки персональных данных:

физическими лицами в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью.

Разговаривая по телефону, обмениваясь смс, общаясь в социальных сетях, мы постоянно используем персональные данные, как свои собственные, так и иных лиц (друзей, знакомых, родственников). По сути, межличностное общение невозможно без обмена личной информацией (обсуждение планов, новостей, привычек, тех или иных событий и др.), что составляет существенную часть наших взаимоотношений с другими людьми.

Рассматриваемое изъятие из сферы действия Закона – попытка избежать тотального признания всех граждан операторами. По сути, данная оговорка является отражением здравого смысла с тем, чтобы предписания Закона не становились искусственным препятствием для реализации устоявшихся социальных моделей поведения, где неписанные нормы поведения выступают более эффективным регулятором.

Термин ”личное, семейное, домашнее и иное подобное использование, не связанное с профессиональной или предпринимательской деятельностью“ не имеет определения в Законе. Не имеет он четкой дефиниции и в иных актах законодательства, несмотря на неоднократное использование в ГК и других законодательных актах.

Закон устанавливает определенные ориентиры для понимания того, что должно оцениваться как ”личное, семейное, домашнее и иное подобное использование“. Так, если обработка персональных данных связана с предпринимательской деятельностью, то такая обработка не может подпадать под рассматриваемую оговорку. При этом неважно, зарегистрировано ли лицо в качестве индивидуального предпринимателя или нет, а также допускается ли законодательством осуществление определенных видов деятельности (услуг агроэкотуризма, ремесленной деятельности и др.) без необходимости иметь статус индивидуального предпринимателя.

Также не подпадают под данное изъятие и действия работника в рамках своих должностных обязанностей (проверка потенциальных кандидатов в социальных сетях и др.), поскольку такая обработка будет связана с профессиональной деятельностью лица. В большинстве случаев как обработку, связанную с профессиональной или предпринимательской деятельностью, следует рассматривать и деятельность так называемых ”блогеров“, особенно при условии использования ими соответствующего интернет-ресурса для показа рекламы и др.

Показательными случаями применения рассматриваемого изъятия могут быть ситуации совместных съемок, последующего обмена фотографиями между друзьями, родственниками, знакомыми, просмотр таких фотографий, общение в чатах, социальных сетях, мессенджерах, систематизация контактов в мобильном телефоне.

Дискуссионным на практике является вопрос о допустимости применения рассматриваемого изъятия в случае распространения персональных данных третьих лиц в социальных сетях.

С одной стороны, личное, семейное, домашнее и иное подобное использование персональных данных предполагает контроль (понимание) круга лиц, которые имеют доступ к персональным данным. Если же персональные данные, например совместные фотографии, становятся доступными для неопределенного круга лиц, когда участники закрытой группы не могут контролировать доступ посторонних к такой информации, то, на первый взгляд, говорить о применимости данного изъятия не приходится.

Однако подобный вариант будет идти вразрез со сложившимися моделями социального общения и возлагать на граждан чрезмерные обременения, которые вытекают из статуса оператора. Сложно представить себе получение одним гражданином согласия от другого гражданина в соответствии с требованиями ст. 5 Закона на размещение совместного фото. Также не совсем ясно, чем принципиально будут отличаться закрытые социальные группы, включающие сотни человек,

от распространения персональных данных, когда с ними ознакомилось всего несколько субъектов.

С учетом изложенного размещение персональных данных в открытом доступе в социальных сетях, если это не связано с предпринимательской или профессиональной деятельностью, может рассматриваться как подпадающее под комментируемую норму. Помимо прочего данный подход дает четкий критерий определения сферы действия Закона, что существенно повышает прозрачность и предсказуемость правового регулирования.

Вместе с тем это вовсе не означает, что граждане свободны в сборе и распространении персональных данных о других лицах.

Согласно ст. 18 Закона ”Об информации, информатизации и защите информации“ сбор, обработка, хранение, предоставление, распространение информации о частной жизни физического лица, а также пользование ею и обработка персональных данных осуществляются с согласия данного физического лица, если иное не установлено законодательными актами. Эта норма применяется независимо от того, подпадают ли те или иные случаи под сферу действия законодательства о персональных данных.

При этом, вне сферы действия Закона при получении согласия нет необходимости соблюдать положения ст. 5 Закона о форме и содержании согласия на обработку персональных данных. Факт наличия или отсутствия согласия оценивается исходя из особенностей конкретной ситуации (согласие может носить устный характер, о согласии может свидетельствовать поведение лица, не возражающего против съемки, переписка в социальных сетях, обмен e-mail и др.).

В случае, если названные предписания не выполняются, то субъект несет ответственность в соответствии с положениями ст. 23.7 КоАП. Данная статья также применяется независимо от того, распространяется ли на физическое лицо действие Закона или нет;

отнесенных в установленном порядке к государственным секретам.

Закон также не применяется к обработке персональных данных, отнесенных в установленном порядке к государственным секретам. Это, в частности, означает, что соответствующие органы, обрабатывающие персональные данные, не связаны ограничениями, установленными Законом (сроки хранения, неизбыточность данных, прозрачность обработки и др.), а субъекты персональных данных в отношении обрабатываемых данных не наделяются предусмотренными Законом правами (правом на получение информации, касающейся обработки персональных данных, и др.).

В этом случае обработка персональных данных осуществляется в порядке, установленном Законом Республики Беларусь от 19 июля 2010 г. № 170-З ”О государственных секретах“ и принятыми в его развитие иными актами законодательства.

Статья 3. Правовое регулирование отношений в сфере обработки персональных данных

Комментарий к статье 3

1. В соответствии с п. 1 комментируемой статьи отношения в сфере обработки персональных данных регулируются законодательством о персональных данных, а также международными договорами Республики Беларусь.

В свою очередь п. 2 комментируемой статьи определяет, что законодательство о персональных данных состоит из Закона и иных актов законодательства.

Структуру законодательства о персональных данных в самом общем виде можно представить следующим образом:

1) Конституция Республики Беларусь.

Согласно ст. 28 Конституции государство создает условия для защиты персональных данных и безопасности личности и общества при их использовании.

2) Законодательные акты общего характера, регулирующие персональные данные:

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

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

3) Законодательные акты, регулирующие обработку персональных данных, входящих в состав охраняемой законом тайны:

Банковский кодекс Республики Беларусь (ст. 121 ”Банковская тайна“);

Закон ”О здравоохранении“ (ст. 46) и др.

4) Иные законодательные акты, регулирующие вопросы, связанные с обработкой персональных данных:

4.1) комплексно регулирующие порядок функционирования отдельных информационных ресурсов, содержащих персональные данные:

Закон Республики Беларусь ”О регистре населения“;

Закон ”О единой государственной системе регистрации и учета правонарушений“;

Закон Республики Беларусь от 10 ноября 2008 г. № 441-З ”О кредитных историях“ и др.;

4.2) регулирующие отдельные аспекты обработки персональных данных. Как правило, такие акты содержат указание на возможность тех или иных организаций (преимущественно государственных органов и государственных организаций) осуществлять обработку персональных данных без получения согласия граждан.

В целом, в качестве акта законодательства о персональных данных может рассматриваться любой нормативный правовой акт, в той или иной степени регулирующий действия с персональными данными, независимо от использования в самом акте данного термина, а также от отраслевой принадлежности самого акта.

При этом Указ Президента Республики Беларусь от 4 января 1999 г. № 1 ”Об утверждении Единого правового классификатора Республики Беларусь“ относит законодательство о персональных данных и их защите (10.03.08.05) к блоку законодательства об информации, информатизации и защите информации.

2. Согласно п. 3 комментируемой статьи в случае, если законодательным актом, устанавливающим правовой режим охраняемой законом тайны, предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, применяются положения этого законодательного акта.

Согласно ст. 17 Закона ”Об информации, информатизации и защите информации“ персональные данные и информация, составляющая коммерческую, профессиональную, банковскую и иную охраняемую законом тайну относятся к самостоятельным видам информации, распространение и (или) предоставление которой ограничено. Тем не менее, довольно часто одни и те же сведения будут соответствовать признакам персональных данных и одновременно рассматриваться как сведения, составляющие охраняемую законом тайну.

Например, сведения о состоянии здоровья, обрабатываемые учреждением здравоохранения, подпадают под признаки персональных данных и в то же время являются врачебной тайной. Происходит удвоение правового режима защиты данных, что может привести к сложностям на практике в связи с отличающимися требованиями различных нормативных правовых актов.

В этом контексте рассматриваемая норма Закона выступает своеобразным инструментом разрешения возможных коллизий и определения применимого правового режима.

Важно отметить, что указанные положения не исключают применения положений Закона в сфере охраняемой законом тайны, а лишь указывают на приоритет регулирования, когда одни и те же вопросы по-разному регламентированы Законом и законодательным актом, устанавливающим порядок обработки персональных данных в составе охраняемой законом тайны.

Взаимодействие рассматриваемых правовых режимов можно представить в следующем виде:

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

Например, Закон ”О здравоохранении“ не предусматривает права пациента на получение информации о предоставлении его персональных данных третьим лицам. В такой ситуации будут применяться положения ст. 12 Закона;

когда законодательным актом, устанавливающим правовой режим охраняемой законом тайны, и принятыми в его развитие актами предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, – применяются положения этого законодательного акта.

Особенности обработки персональных данных имеют место в том случае, когда Закон и законодательный акт, устанавливающий правовой режим охраняемой законом тайны, а также принятые в его развитие акты по-разному регулируют один и тот же вопрос.

Это, например, могут быть:

различный круг оснований для обработки персональных данных;

различный круг органов и организаций, которые имеют право на получение персональных данных;

различные подходы к объему персональных данных, необходимых для достижения определенной цели;

различные требования к форме и содержанию согласия на обработку персональных данных;

различные подходы к срокам хранения персональных данных.

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

Беларусь), подлежат применению нормы данного постановления, а не положения ст. 5 Закона.

3. Пункт 4 комментируемой статьи предусматривает приоритет международных договоров над Законом по вопросу обработки персональных данных.

Вопросы обработки персональных данных отражаются в целом ряде международных договоров Республики Беларусь, например:

Соглашение между Правительством Республики Беларусь и Правительством Республики Армения о реадмиссии (заключено в г. Минске 8 октября 2021 г.);

Соглашение между Правительством Республики Беларусь и Правительством Арабской Республики Египет о сотрудничестве и взаимной помощи в таможенных делах (заключено в г. Каире 19 февраля 2020 г.);

Соглашение между Республикой Беларусь и Российской Федерацией о повышении эффективности взаимодействия в борьбе с преступностью (заключено в г. Бресте 15 сентября 2014 г.).

Во многих случаях такие договоры содержат правила, отличные от Закона (круг оснований, порядок защиты данных и др.), применение которых и будет основываться на норме рассматриваемого пункта.

Кроме того, в большинстве случаев подобные международные договоры предусматривают необходимость обмена персональными данными между государственными органами, что приводит к трансграничной передаче персональных данных. В этой связи комментируемая норма находит свое отражение и в ст. 9 Закона при описании оснований для трансграничной передачи персональных данных. Так, в качестве самостоятельного основания для трансграничной передачи указано на необходимость исполнения международных договоров Республики Беларусь.

ГЛАВА 2
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Статья 4. Общие требования к обработке персональных данных

Комментарий к статье 4

В комментируемой статье закрепляются общие требования к обработке персональных данных:

законность;

соразмерность и справедливость;

наличие правового основания;

ограничение цели;

запрет избыточности;

прозрачность;

ограничение хранения;

достоверность.

Перечисленные требования к обработке персональных данных являются ”каркасом“ законодательства о персональных данных, в концентрированном виде выражая сущность государственной политики в этом вопросе. Любая норма Закона или иного акта законодательства о персональных данных является развитием одного из этих требований, которые в ряде случаев переплетаются, взаимно дополняя и усиливая друг друга.

Указанные требования сформулированы довольно общим образом и подлежат применению всеми операторами (уполномоченными лицами) вне зависимости от сферы и специфики их деятельности.

Они могут выступать как в виде общих положений, которые конкретизируются в определенной норме Закона, так и быть нормами прямого действия, нарушение которых с учетом обстоятельств конкретной ситуации может влечь различные меры ответственности.

1. Самым общим требованием к обработке персональных данных является необходимость осуществлять обработку таких данных в соответствии с Законом и иными актами законодательства (**законность**).

По своей сути требование законности в силу предписаний ч. 3 ст. 7 Конституции существует в любой сфере и является общеправовым принципом. Тем не менее в рассматриваемой сфере данное требование имеет собственное содержание.

Прежде всего законность обработки предполагает выполнение оператором (уполномоченным лицом) всех обязанностей, которые на него возлагаются Законом.

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

2. В соответствии с п. 2 комментируемой статьи обработка должна быть соразмерна заявленным целям и обеспечивать на всех этапах обработки справедливое соотношение интересов всех заинтересованных лиц.

Фактически тут закрепляются два самостоятельных требования – **соразмерность** и **справедливость**.

В самом упрощенном виде обработку можно признать соразмерной, когда цель обработки ”стоит“ использованных для ее достижения персональных данных и без их обработки (иными методами) данная цель достигнута не будет или ее достижение будет серьезно затруднено.

Довольно распространенной на практике является ситуация, когда для достижения вполне легальной цели могут использоваться персональные данные, в то время как цель может или должна быть достигнута иным образом. В этой связи, например, сканирование радужной оболочки глаз при входе в организацию (при отсутствии специфических обстоятельств, требующих от организации применения повышенных мер безопасности) для целей учета прихода и ухода с работы сложно признать соразмерной мерой, поскольку данная цель может быть достигнута иными способами (с помощью карточки, наличия охранника и др.).

В свою очередь, справедливость означает учет интересов всех заинтересованных лиц при обработке персональных данных.

Данное требование отражает необходимость обеспечения баланса между интересами операторов и субъектов персональных данных. Любой перекос и абсолютизация интересов одной из сторон могут привести к негативным последствиям. Так, возложение непропорциональных или чрезмерных обязанностей на операторов может привести к превышению издержек по защите данных над возможными выгодами и, как следствие, уклонению от выполнения таких обязанностей. И наоборот, игнорирование прав субъектов персональных данных и чрезмерная свобода действий операторов может обусловить

превращение конституционного права на защиту персональных данных в чисто декларативное.

Справедливость обработки также означает недопустимость злоупотребления сложившейся ситуацией (монопольным положением оператора, отсутствием у субъекта возможности ознакомиться с информацией и др.). В любом случае вопрос справедливости обработки является предметом оценки конкретной ситуации. При этом обработка может рассматриваться как несправедливая независимо от формального наличия правового основания обработки персональных данных.

3. Пункт 3 комментируемой статьи закрепляет необходимость **наличия правового основания** для обработки персональных данных.

Обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами.

Таким образом, в качестве общего правила обработки указывается на необходимость получения согласия субъекта персональных данных. Иные основания рассматриваются лишь как возможные исключения из него.

Этот подход, являясь отражением предписаний ч. 1 ст. 2 Конституции, подчеркивает принадлежность персональных данных субъекту персональных данных и его главенствующую роль в контексте обработки, недопустимость отторжения личных данных от гражданина. На данный вывод не влияет и тот факт, что в современном мире преобладающая масса бизнес-процессов, связанных с обработкой персональных данных, осуществляется без согласия лица.

Одновременно рассматриваемым пунктом предусматривается, что в случае обработки персональных данных без согласия субъекта персональных данных цели обработки персональных данных должны устанавливаться Законом и иными законодательными актами. Эта норма основывается на положениях ст. 23 Конституции и призвана исключить возможность ”произвольного“ нормотворчества на подзаконном уровне и создание каждым органом под себя удобных правовых оснований для обработки персональных данных.

Наиболее распространенные цели обработки персональных данных без согласия соответствующего субъекта закреплены в ст.ст. 6, 8 Закона. При этом указанные статьи не предусматривают исчерпывающего перечня целей для обработки персональных данных, в связи с чем подобные положения могут содержаться и в иных законодательных актах.

4. Обработка должна ограничиваться достижением конкретных, заранее заявленных законных целей (**ограничение цели**).

Указанное требование содержит ряд характеристик цели обработки персональных данных для признания ее соответствующей Закону:

конкретность. Конкретность цели является отправной точкой для последующего анализа вопроса о объеме данных, необходимых для ее достижения, а также основой для понимания субъектом персональных данных сути их обработки. Кроме того, конкретность цели является элементом защиты от так называемой ”функциональной ползучести“[14], когда изложенная весьма общим образом цель ”подгоняется“ под текущие потребности оператора.

В этой связи не допускается указание абстрактных или общих целей, которые не определяют пределов обработки и не позволяют субъекту персональных данных понять, для чего будут обрабатываться его персональные данные.

В частности, не соответствуют критерию конкретности такие формулировки, как: ”совершенствование деятельности организации“; ”разработка новых услуг“; ”достижение общественно значимых целей“, ”реализация устава“ и т.п.[15];

заявленность цели до момента начала обработки. Цель обработки должна быть определена до ее начала. Это обеспечивает предсказуемость обработки для субъекта персональных данных, давая возможность при необходимости принять меры по защите своих прав. Иными словами, оператор не может подбирать цель постфактум, после начала и, тем более, окончания обработки.

На практике механизм заявления цели (информирования о цели) зависит от правового основания обработки данных. При их обработке на основании согласия цель обработки указывается при предоставлении информации субъекту в соответствии с п. 5 ст. 5 Закона. При обработке персональных данных без согласия цели обработки указываются в документах, определяющих политику оператора в отношении обработки персональных данных;

законность. Законность цели является конкретизацией общего требования законности обработки персональных данных. Ее смысл в недопустимости обработки персональных данных для осуществления противозаконной деятельности (например, осуществления мошеннических действий, преследования лица и др.). В такой ситуации обработка должна рассматриваться как незаконная и влечь соответствующие меры ответственности.

Закон содержит весьма важное для правоприменения положение о недопустимости обработки персональных данных, не совместимой с первоначально заявленными целями их обработки. Эта норма призвана

---

[14] Англ. ‘function creep’.

[15] Больше примеров содержится в Рекомендациях по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных, размещенных на официальном интернет-сайте Центра.

дать ответ на вопрос о возможности обработки персональных данных, полученных для одной цели, в иных целях. Ключевым моментом здесь является правильное понимание сути обработки, совместимой с первоначально заявленными целями.

Для решения данного вопроса следует учитывать положения ч. 2 комментируемого пункта, где предусматривается, что в случае необходимости изменения первоначально заявленных целей обработки персональных данных оператор обязан получить согласие субъекта персональных данных на обработку его персональных данных в соответствии с измененными целями обработки персональных данных при отсутствии иных оснований для такой обработки, предусмотренных Законом и иными законодательными актами.

Таким образом, следует отличать измененные цели от совместимых целей. Измененная цель – новая цель, которая не охватывается первоначальной, не вытекает из нее. В свою очередь совместимая цель по своей сути будет представлять конкретизацию (уточнение) первоначальной цели. В этой связи не должна рассматриваться как новая цель ее новая формулировка, не меняющая существа обработки, либо цель, конкретизирующая первоначальную.

Так, например, если первоначальная цель была заявлена как ”заключение и исполнение договора“, то цель – ”отправка напоминаний о необходимости оплаты“ может обоснованно рассматриваться как конкретизация первоначальной цели.

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

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

В рассматриваемых нормах сформулировано требование **запрета избыточности** обрабатываемых данных. Ее мерилом выступает заявленная цель обработки, с которой соотносят перечень персональных данных, используемых для ее достижения.

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

Разновидностями данного нарушения могут быть ситуации, когда:

персональные данные не соответствуют заявленным целям. В таких ситуациях обрабатываемые персональные данные никак не влияют на достижение заявленной цели. Например, обработка сведений о родственниках кандидата на работу, когда это не предусмотрено законодательством, никак не влияет на оценку профессиональных качеств такого лица;

персональные данные избыточны по отношению к заявленной цели. В этом случае обрабатываемые данные связаны с конечной целью, но она может быть достигнута либо с использованием меньшего набора данных, либо с использованием менее чувствительных их категорий, либо могут использоваться обезличенные данные вместо обычных персональных данных.

Так, если оператору нужно контактировать лишь с отдельными лицами (сообщать о наличии задолженности), то получение для этих целей полной базы, где наряду с информацией об указанных лицах будут содержатся данные о других лицах, является нарушением данного требования.

Важно учитывать, что по смыслу Закона обработка персональных данных, указанных в нормативном правовом акте (когда на оператора возложена обязанность их обрабатывать), не может рассматриваться как избыточная обработка или обработка, не соответствующая цели. Изменение объема обрабатываемых данных в такой ситуации должно осуществляться посредством корректировки соответствующего нормативного правового акта.

6. Обработка персональных данных должна носить прозрачный характер. С этой целью субъекту персональных данных в случаях, предусмотренных Законом, предоставляется соответствующая информация, касающаяся обработки его персональных данных (**прозрачность**).

Сложность современных информационных отношений, множество участников различных бизнес-процессов, широкое использование трансграничной передачи данных, применение новейших технологий обработки данных (большие данные, искусственный интеллект и др.) серьезно осложняют для субъекта персональных данных понимание сути обработки данных, а также того, как и кем они в итоге используются. Вместе с тем без уяснения сути обработки субъект просто не в состоянии эффективно пользоваться своими правами, в том числе, при необходимости, возражать против соответствующей обработки.

В этом контексте прозрачность обработки персональных данных имеет критически важное значение для обеспечения применения Закона

и создания возможности для субъектов персональных данных в реализации и отстаивании своих прав.

Требование прозрачности обработки не ограничивается лишь моментом сбора персональных данных от субъекта, но распространяется на весь цикл их обработки. Прозрачность обработки персональных данных обеспечивается:

на стадии сбора (получения) – при получении данных либо от самого субъекта, либо от третьих лиц;

во время иных действий по обработке – при коммуникации с субъектом персональных данных, например, по вопросу реализации его прав, либо в специфических ситуациях, например, при установлении факта утечки персональных данных.

Обеспечение прозрачности обработки персональных данных осуществляется посредством предоставления субъекту персональных данных и иным лицам информации о такой обработке. Эта информация предоставляется:

при получении согласия (п. 5 ст. 5 Закона определяет объем информации, которая в обязательном порядке предоставляется субъекту);

в рамках размещения документов, определяющих политику оператора в отношении обработки персональных данных;

при взаимодействии с субъектом персональных данных при реализации его прав;

при информировании субъекта персональных данных в случае утечки персональных данных и др.

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

Необходимо также избегать излишнего цитирования актов законодательства, использования большого числа специальных терминов, подробного описания технических аспектов обработки персональных данных. Для обеспечения большей наглядности могут использоваться схемы, таблицы и др.

Форма представления информации может меняться в зависимости от целевой аудитории (несовершеннолетние, пенсионеры и др.).

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

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

Однако это не означает, что оператор регулярно должен обращаться к субъекту или в другие организации для актуализации имеющейся информации.

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

Следует учитывать, что в ряде случаев обновление персональных данных невозможно в принципе. Так, если речь идет о зарегистрированной сделке, то данные сохраняются в том виде, в котором они были на момент ее регистрации, независимо от последующего изменения, например, паспортных данных сторон.

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

Срок хранения персональных данных определяется оператором и отражается в политике. При его определении следует исходить из следующего:

если *срок хранения определен в законодательном акте (акте законодательства, принятом в развитие законодательного акта)*, то данные могут храниться в течение этого срока. Такое хранение не может рассматриваться как нарушение Закона. В данном случае происходит своеобразная трансформация правового основания обработки (например, вместо исполнения договора правовым основанием становится необходимость выполнения обязанностей, предусмотренных законодательным актом). Среди актов, которые устанавливают сроки хранения отдельных категорий персональных данных, можно назвать:

постановление Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 ”О перечне типовых документов“. В нем содержится более 1 тыс. наименований различных документов,

в том числе содержащих персональные данные, с указанием сроков их хранения;

иные акты законодательства, устанавливающие сроки хранения отдельных категорий персональных данных. Так, например, согласно пункту 7 Положения о порядке предварительной идентификации пользователей интернет-ресурса, сетевого издания, утвержденного постановлением Совета Министров Республики Беларусь от 23 ноября 2018 г. № 850, владелец интернет-ресурса на время действия пользовательского соглашения, а также в течение года с даты его расторжения обеспечивает хранение на физически размещенных на территории Республики Беларусь серверах:

полученных при предварительной идентификации пользователя сведений, указанных в подпункте 1.3 пункта 1 статьи 30^1 Закона Республики Беларусь «О средствах массовой информации»;

сведений о размещении и (или) изменении пользователем на интернет-ресурсе информационных сообщений и (или) материалов, дате и времени их размещения и (или) изменения;

сведений о сетевом (IP) адресе устройства пользователя, присвоенном при регистрации пользователя на интернет-ресурсе, внесении изменений в регистрационные данные пользователя;

иных сведений, полученных владельцем интернет-ресурса при идентификации пользователя;

если срок хранения не определен в акте законодательства, то он определяется самим оператором. Ориентиром выступает рассматриваемая норма Закона, а именно – возможность хранить данные не дольше, чем это необходимо для достижения цели обработки.

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

Данный подход корреспондируется с положениями абзаца седьмого ст. 16 Закона, которыми на оператора возлагается обязанность прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами.

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

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

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

комбинация различных критериев (1 год с момента последнего использования карточки программы лояльности).

Не соответствует требованиям прозрачности подход, при котором срок обработки персональных данных, полученных на основании согласия, определяется как ”до отзыва согласия“. С учетом количества согласий, которые предоставляет субъект ежегодно, это означает возложение на самого субъекта бремени учета всех выданных согласий.

Следует отметить, что ряд операторов полагают, что данная норма не предусматривает необходимости удаления персональных данных, а лишь требует хранить их в форме, не позволяющей идентифицировать лицо. В этой связи существует мнение о допустимости после достижения цели обработки хранить персональные данные в обезличенном виде. Иными словами, достаточно лишь разделить идентифицирующую и иную информацию и хранить их раздельно.

Подобная позиция не основана на Законе. Раздельное хранение идентифицирующих и иных данных не исключает идентификацию субъекта и, соответственно, является обработкой персональных данных, которая должна иметь соответствующее правовое основание.

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

Статья 5. Согласие субъекта персональных данных

Комментарий к статье 5

1. Согласие субъекта персональных данных является самостоятельным правовым основанием обработки персональных данных, отражающим принадлежность таких данных конкретному лицу и его возможность распоряжаться ими по своему усмотрению.

Предполагается, что взрослый человек, обладая всей необходимой информацией, способен адекватно оценить риски и принять осознанное решение о распоряжении своими персональными данными. Право субъекта персональных данных на дачу согласия на обработку своих данных предоставляет ему возможность контролировать процессы обработки данных о нем и определять, где, когда, кому, для каких целей и в каком объеме предоставлять подобную информацию.

Термин ”согласие“ широко применяется в различных актах законодательства, но далеко не всегда речь идет о согласии в понимании

законодательства о персональных данных. В этой связи согласие на обработку персональных данных следует отличать от согласия на осуществление в отношении лица или его имущества какого-либо действия (письменное согласие на перевод работника, согласие родителей на выезд ребенка за границу, согласие на совершение сделок по отчуждению имущества подопечного и т.п.).

Важно отметить, что хотя согласие и является базовым правовым основанием для обработки, его наличие не является универсальным или обязательным условием для обработки персональных данных. Обработка персональных данных осуществляется без согласия субъекта персональных данных в случаях, предусмотренных ст.ст. 6 и 8 Закона. В этой связи получение согласия при наличии иных оснований рассматривается как избыточная обработка персональных данных. Одним из критериев, свидетельствующих о неправомерности обработки персональных данных на основании согласия, может являться, в частности, тот факт, что отзыв согласия не допускается или не влечет прекращения обработки персональных данных.

Закон определяет критерии, которым должно соответствовать согласие: свободное, однозначное, информированное. Только при их соблюдении согласие на обработку персональных данных может быть признано юридически действительным.

Согласие является свободным, когда субъект самостоятельно, исходя из своего внутреннего убеждения, выражает свою волю в отношении обработки персональных данных. Данное требование предполагает недопустимость понуждения субъекта к даче такого согласия под угрозой наступления неблагоприятных для него последствий.

При оценке того, является ли согласие свободным, следует исходить из того, обладает ли субъект персональных данных реальным выбором давать свое согласие либо его согласие является вынужденным, например, в силу связанности согласия с достижением иной, желаемой для него цели.

Пример.

Заказ и доставка товара в интернет-магазине не может быть реализована, пока субъект не даст согласие на использование адреса электронной почты для осуществления рекламной рассылки. В данной ситуации обработка персональных данных в целях получения рекламных сообщений не является необходимой для заключения договора розничной купли-продажи. Подобная обработка будет рассматриваться как нарушение Закона.

Согласие не будет являться также свободным и в случае, когда одно согласие получается для достижения нескольких самостоятельных целей (например, для осуществления рекламной рассылки, а также для передачи данных организациям-партнерам).

В случае объективной потребности в получении согласия на достижение подобных целей, оператору следует обращаться к субъекту персональных данных за получением отдельного согласия на каждую из таких целей (принцип ”одна цель – одно согласие“). При этом субъект персональных данных вправе давать свое согласие исключительно на те цели, которые посчитает нужными. Для реализации требований к свободному согласию оператору необходимо предоставить субъекту персональных данных право выбора конкретных целей обработки персональных данных, с которыми он согласен, а также указать категории персональных данных, обрабатываемые применительно к каждой цели.

Цели обработки персональных данных в таких случаях могут, например, разделяться на соответствующие ”чек-боксы“, в которых субъект персональных данных может выразить свое согласие путем проставления отметки (галочки).

Согласие не может рассматриваться как свободное при очевидной диспропорции возможностей оператора и субъекта персональных данных. В этой связи за редкими исключениями не рассматривается как свободное согласие между нанимателем и работником (кандидатом на работу).

Согласие является однозначным, когда дается путем совершения четкого намеренного действия. Соответствующая информация должна быть воспринята субъектом персональных данных и отражать его действительные намерения. Факт дачи согласия не должен быть предметом допущений, а должен следовать из конкретных действий субъекта, свидетельствующих об этом. Молчание или бездействие субъекта персональных данных, даже если такое поведение в соответствии с изданными оператором документами, определяющими политику в отношении обработки персональных данных, будет признаваться согласием, не будет удовлетворять критерию однозначности согласия.

В этой связи не соответствуют критерию однозначности, например, следующие модели получения согласия:

”оставаясь на линии, Вы тем самым даете согласие на обработку персональных данных“;

”продолжая пользоваться сайтом, Вы даете согласие на обработку персональных данных“.

Согласие должно быть информированным. Даче согласия должно предшествовать предоставление субъекту всей необходимой и достоверной информации о целях обработки, об обрабатываемых данных, операторе и иных лицах, которые будут осуществлять обработку персональных данных, сроке обработки и другой необходимой

информации. Предоставляемая оператором информация должна позволять субъекту получить ответы на вопросы: кто, зачем, какие данные, каким образом и в течение какого срока будет обрабатывать.

Таким образом, чтобы согласие было информированным, оператору необходимо до получения согласия соблюсти обязанность по предоставлению субъекту персональных данных информации, содержащейся в п. 5 ст. 5 Закона, простым и ясным языком разъяснить субъекту персональных данных его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия или отказа в даче такого согласия.

Данная информация должна быть предоставлена в той же форме, что и форма получения согласия.

Пример.

Так, размещение данной информации на корпоративном сайте в глобальной компьютерной сети Интернет не будет являться надлежащей формой предоставления такой информации, если согласие получается в письменной форме. Не будет являться "надлежащим" информированием и получение согласия путем ознакомления с политикой обработки персональных данных, содержащей описание нескольких бизнес-процессов. В последнем случае оператор фактически перекладывает на субъекта бремя поиска соответствующего бизнес-процесса и выделение необходимой информации в тексте политики. Кроме того, политика обработки персональных данных может периодически меняться, что фактически приводило бы к одностороннему изменению содержания полученного согласия.

2. При определении способа получения согласия следует иметь в виду, что согласно п. 7 ст. 5 Закона обязанность доказывания получения свободного, однозначного, информированного согласия субъекта персональных данных возлагается на оператора.

Согласно п. 2 ст. 5 Закона согласие субъекта персональных данных может быть получено в письменной форме, в виде электронного документа или в иной электронной форме.

По общему правилу, согласие на обработку персональных данных может быть дано в любой форме, позволяющей подтвердить факт его получения, если только конкретная форма дачи согласия прямо не предусмотрена в законодательстве (*см. комментарий к п. 4 ст. 5 Закона*).

Получение согласия в письменной форме представляет собой собственноручно подписанный субъектом персональных данных документ, независимо от того, набран ли он на компьютере или написан от руки, который подтверждает добровольное решение гражданина передать оператору свою личную информацию для определенных целей. Как получение согласия в письменной форме следует рассматривать и случаи, когда законодателем прямо установлено, что согласие физического лица считается совершенным в письменной форме.

Пример.

Так, в соответствии с ч. 3 подп. 1.11 п. 1 Указа Президента Республики Беларусь от 18 апреля 2019 г. № 148 ”О цифровых банковских технологиях“ для целей деятельности пользователей межбанковской системы идентификации при наличии условий, предусмотренных данной нормой, документы, информация, включая согласие на сбор, обработку, хранение, предоставление и использование персональных данных и иной информации о клиентах, их представителях, в том числе хранящихся в системе идентификации, считаются совершенными (предоставленными) в письменной форме.

Что касается механизма получения оператором согласия в письменной форме, то оно может быть получено как по почте, так и в присутствии работника оператора.

Часто задаваемым является вопрос о допустимости включения норм о согласии в текст договора с субъектом персональных данных. Конкретных норм, которые бы предусматривали оформление согласия путем составления отдельного документа или запрещали включение соответствующих положений в текст договора, Закон не содержит.

Вместе с тем следует исходить из того, что договор и согласие являются самостоятельными правовыми основаниями обработки персональных данных, которые не должны смешиваться и подменять друг друга. При этом к согласию Законом установлен ряд требований, исполнение которых представляется затруднительным, при включении согласия на обработку персональных данных для достижения целей, не связанных с предметом договора, в текст договора. Помимо серьезной ”перегрузки“ договора это приведет к тому, что при корректировке согласия потребуется внесение изменений в сам договор, что не всегда целесообразно.

Более того, включение в текст договора согласия на обработку персональных данных может приводить к конфликтным ситуациям и затруднительности обоснования оператором свободного характера полученного согласия. В этой связи более предпочтительным будет оформление согласия на обработку персональных данных и предоставление необходимой информации, связанной с обработкой, в отдельном документе.

Унифицированной формы для оформления согласия законодательно не предусмотрено. В качестве ориентира можно использовать образец согласия на обработку персональных данных, размещенный на официальном интернет-сайте Центра.

Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной цифровой подписью.

3. Пунктом 3 ст. 5 Закона предусмотрено, что в иной электронной форме согласие субъекта персональных данных может быть получено посредством:

указания (выбора) субъектом персональных данных определенной информации (кода) после получения СМС-сообщения, сообщения на адрес электронной почты;

проставления субъектом персональных данных соответствующей отметки на интернет-ресурсе;

других способов, позволяющих установить факт получения согласия субъекта персональных данных.

В современных условиях возможности получения согласия субъекта персональных данных не ограничиваются только лишь традиционной письменной формой либо формой электронного документа. С учетом того, что многие виды деятельности могут осуществляться онлайн и не предполагать физического взаимодействия оператора и субъекта персональных данных, законодатель предоставляет возможность получать согласие субъекта персональных данных и иными способами.

Распространенным примером получения согласия в иной электронной форме является проставление субъектом персональных данных соответствующей отметки на интернет-ресурсе, разрешающей обработку персональных данных этого субъекта. Однако само по себе проставление отметки на сайте не может легитимировать соответствующую обработку, если согласие не будет являться свободным, информированным и однозначным.

Перечень способов, позволяющих получать согласие в иной электронной форме, является открытым, что позволяет оператору как использовать перечисленные в Законе способы получения согласия, так и создает возможности для использования потенциально новых форм взаимодействия субъектов в условиях цифровой трансформации государства и общества.

В этой связи оператор (уполномоченное лицо в интересах оператора) может разработать собственный алгоритм получения согласия в иной электронной форме, главное, чтобы при этом были обеспечены требования к согласию, предусмотренные п. 1 ст. 5 Закона.

4. В отдельных случаях, для определенных правоотношений необходимость получения согласия только в письменной форме или в виде электронного документа может быть предусмотрена в законодательных актах.

Так, например, требования в отношении оформления согласия на предоставление сведений о правонарушениях установлены Законом ”О единой государственной системе регистрации и учета

правонарушений“ и принятым в его развитие постановлением Совета Министров Республики Беларусь от 20 июля 2007 г. № 909 ”О функционировании единой государственной системы регистрации и учета правонарушений“ (п.п. 124–126 Положения о порядке функционирования единой государственной системы регистрации и учета правонарушений, утвержденного этим постановлением). При этом в приложении 20 к данному Положению приведена форма такого согласия.

В соответствии с внесенными в Закон ”О регистре населения“ изменениями с 1 января 2023 г. при предоставлении персональных данных по электронному запросу согласие физического лица может быть получено только в виде электронного документа, а по письменному запросу – только в письменной форме в соответствии с требованиями законодательства о персональных данных.

5. В п. 5 ст. 5 Закона содержатся положения, определяющие объем предоставляемой информации и требования к ее изложению, для признания согласия информированным. При этом ч. 2 данного пункта предусмотрено, что информация должна быть предоставлена оператором субъекту персональных данных в письменной либо электронной форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой ему информации.

В этой связи, а также с учетом принципа прозрачности (например, исключения необходимости поиска такой информации по разделам политики) информация, предоставляемая оператором до получения согласия субъекта персональных данных, должна содержаться отдельно от иной информации, например, политики оператора в отношении обработки персональных данных, условий пользования сайтом и т.д.

Для того, чтобы согласие соответствовало критерию информированности, оператор должен ознакомить субъекта персональных данных со следующей информацией:

наименование (фамилия, собственное имя, отчество (если таковое имеется)) и место нахождения (адрес места жительства (места пребывания)) оператора, получающего согласие субъекта персональных данных;

цели обработки персональных данных. Не допускается получать общее согласие на достижение всех целей. Если оператор заинтересован в получении согласия на несколько самостоятельных целей обработки, то он может сделать это в одном документе, но обязан получать отдельное согласие на каждую цель (например, на передачу персональных данных конкретной организации, на получение рекламной рассылки). При этом субъекту должна быть предоставлена возможность согласиться с одной целью и не соглашаться с другой (другими).

Цели должны носить конкретный характер, что позволяет определить перечень персональных данных, достаточный для их достижения. В этой связи указание абстрактных, чрезмерно укрупненных целей, не дающих возможности уяснить механизм обработки персональных данных, будет препятствовать признанию согласия информированным (например, улучшение деятельности организации, реализация законных прав оператора, реализация устава и др.)[16];

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных. Указываются конкретные персональные данные, которые необходимы и достаточны для реализации цели обработки персональных данных. Недопустимо указание персональных данных ”с запасом“. Оператору следует по возможности минимизировать объем персональных данных, руководствуясь принципом недопущения избыточности обработки;

срок, на который дается согласие субъекта персональных данных. В качестве срока обработки персональных данных может быть указана дата или конкретный период времени либо критерии, используемые для определения срока обработки.

Срок согласия должен быть конкретным, доступным для восприятия и понятным для субъекта персональных данных. Срок согласия может быть выражен конкретными датой, периодом времени либо критериями, используемыми для определения таких сроков, например:

конкретная дата (например, до 31 декабря 2023 г.);

период (например, 1 год с даты получения согласия, истечение срока программы лояльности);

комбинированный (например, в течение 1 года (месяца) с даты совершения последней покупки, авторизации на сайте и т.п.).

Не допускается использование при определении сроков согласия таких формулировок, как ”до отзыва согласия субъектом персональных данных“, ”сроки устанавливаются законодательством“ и т.п., поскольку они не соответствуют требованиям прозрачности обработки персональных данных.

Не рекомендуется определять срок действия согласия свыше 3 лет, поскольку в связи со значительным количеством оставляемых согласий гражданину будет затруднительно контролировать обработку своих персональных данных.

Если срок согласия различается для каждой цели,

[16] Более подробная информация о допустимых (недопустимых) целях обработки содержится в Рекомендациях по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных, размещенных на официальном интернет-сайте Центра.

то его необходимо обозначить для каждой цели отдельно;

информацию об уполномоченных лицах в случае, если обработка персональных данных будет осуществляться такими лицами. Указываются конкретные уполномоченные лица и место их нахождения, а в случае затруднительности такого указания (например, наличие значительного количества уполномоченных лиц и их постоянное изменение) – конкретные категории таких лиц (например, организации, оказывающие оператору услуги по системному администрированию локальной сети; организации, осуществляющие доставку покупателю купленных у оператора товаров; организации, оказывающие оператору услуги по ведению бухгалтерского, кадрового учета) и место их нахождения (страна нахождения).

Не допускается указание слишком общих категорий (например, ”лица, с которыми оператор имеет договорные отношения“), а также открытого перечня таких лиц (”и иные лица“);

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

конкретные действия, совершаемые с персональными данными, поручаемые уполномоченному лицу (например, сбор персональных данных для заключения договора с определением перечня необходимых персональных данных; внесение сведений в информационный ресурс; хранение персональных данных с указанием сроков и условий хранения; их актуализация путем сопоставления с дополнительной информацией и т.п.);

информация об использовании обезличивания персональных данных в целях повышения их защищенности (при использовании обезличивания);

условия, при которых возможно предоставление персональных данных третьим лицам или их распространение (если предполагается их предоставление или распространение);

при наличии трансграничной передачи персональных данных – государства, в которые будет осуществляться передача. В случае передачи в страны, где не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, необходимо отразить возможные риски такой передачи (абзац второй п. 1 ст. 9 Закона);

иную информацию, необходимую для обеспечения прозрачности процесса обработки персональных данных. Например, правовые, организационные и технические меры для защиты персональных данных субъектов, применяемые оператором, если эта информация может оказать влияние на принятие решения субъектом персональных данных.

До получения согласия субъекта персональных данных оператор обязан простым и ясным языком разъяснить субъекту персональных данных его права, связанные с обработкой персональных данных, механизм реализации таких прав, а также последствия дачи согласия субъекта персональных данных или отказа в даче такого согласия. Эта информация должна быть предоставлена оператором субъекту персональных данных в письменной либо электронной форме, соответствующей форме выражения его согласия, отдельно от иной предоставляемой ему информации.

Обязанность включать данную информацию в текст согласия законодательством не установлена. В этой связи в тексте допускается указание на то, что субъект ознакомился с соответствующей информацией.

Для целей обеспечения информированного согласия не является надлежащим:

предоставление необходимой информации путем отсылки для самостоятельного ознакомления к сайту оператора при получении согласия на обработку персональных данных в письменной форме;

размещение необходимой информации, например на информационных стендах организации;

предоставление необходимой информации путем ознакомления с политикой оператора в отношении обработки персональных данных, содержащей описание нескольких бизнес-процессов, при получении согласия в иной электронной форме.

6. В п. 6 ст. 5 Закона предусмотрено, что субъект персональных данных при даче согласия оператору указывает свои фамилию, имя, отчество (если таковое имеется), дату рождения, идентификационный номер, а в случае отсутствия такого номера – номер документа, удостоверяющего его личность, за исключением случая, предусмотренного ч. 2 данного пункта.

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

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

Пример.

Если для регистрации личного кабинета на сайте и получения рекламной рассылки достаточно указать ФИО и адрес электронной почты, то указание идентификационного номера при получении согласия не требуется. Для целей рассмотрения резюме, регистрации в интернет-магазине указание паспортных данных и (или) идентификационного номера также является избыточным.

Пункт 6 ст. 5 Закона не называет способы указания соответствующих сведений субъектом персональных данных. Требование о собственноручном заполнении согласия субъектом персональных данных, в том числе сведений о себе, в Законе также отсутствует.

В этой связи устное сообщение персональных данных с целью дальнейшей подготовки текста согласия и его дальнейшего подписания субъектом персональных данных не противоречит нормам Закона. Работник оператора в таких случаях может вносить персональные данные субъекта в текст согласия для дальнейшего подписания субъектом персональных данных. Указанные операции следует рассматривать как элемент единого действия – получения согласия.

7. Следует учитывать, что согласно п. 7 ст. 5 Закона обязанность доказывания получения согласия субъекта персональных данных возлагается на оператора. Поэтому получение согласия субъекта персональных данных следует организовать таким образом, чтобы оператор в любой момент мог подтвердить данный факт.

Механизм подтверждения получения согласия субъекта персональных данных определяется оператором самостоятельно.

Пример.

Такое подтверждение может быть осуществлено с помощью технической информации, содержащейся в базе данных оператора. Так, в случае получения согласия субъекта персональных данных в электронной форме оператор должен сохранить соответствующую запись об этом. При этом нет необходимости записывать содержание всех сеансов связи с субъектом персональных данных.

В случае получения согласия субъекта персональных данных в письменной форме или форме электронного документа оператору следует организовать и вести учет полученных согласий. Важно отметить, что у оператора нет обязанности хранить все полученные согласия централизованно, в одном месте. В этой связи не является нарушением Закона, например, хранение согласий соответствующим подразделением, ответственным за реализацию конкретных бизнес-процессов.

Закон допускает получение одного согласия в отношении нескольких операторов, если они осуществляют совместную обработку персональных данных, то есть совместно определяют способы и цели обработки (”сооператорство“).

8. Предоставление согласия на обработку персональных данных со стороны их субъекта носит *добровольный характер*, и он имеет право отказаться от дачи такого согласия. Данная возможность отражает принадлежность персональных данных конкретному гражданину и его возможность по собственному усмотрению распоряжаться такими данными *(об отзыве согласия см. комментарий к ст. 10 Закона)*.

9. В случае признания субъекта персональных данных недееспособным или ограниченно дееспособным, а также до достижения им возраста шестнадцати лет, за исключением вступления в брак до достижения возраста шестнадцати лет, согласие на обработку его персональных данных дает один из его законных представителей.

Что касается возможности получить согласие субъекта персональных данных на обработку его персональных данных через представителя на основании доверенности, то данный подход не противоречит требованиям Закона.

При этом в случае дачи согласия вместо субъекта персональных данных (представительства), такие лица наделяются и правами субъекта персональных данных, предусмотренными Законом, в целях их реализации.

Статья 6. Обработка персональных данных без согласия субъекта персональных данных

Комментарий к статье 6

По общему правилу, закрепленному в п. 3 ст. 4 Закона, обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами.

Таким образом, Закон определяет согласие как базовое основание для обработки персональных данных. В то же время оно является одним из наиболее ”хрупких“ правовых оснований для обработки персональных данных как с точки зрения сложности получения согласия в силу предъявляемых к нему требований, так и с учетом возможности его отзыва в любое время.

Важно отметить, что согласие не является универсальным или обязательным условием для обработки персональных данных. В ряде случаев обработка персональных данных в принципе не может и не должна основываться на воле субъекта персональных данных.

В этой связи Законом установлены случаи (основания), когда согласие такого субъекта на обработку его персональных данных не требуется.

При этом следует учитывать, что все правовые основания, включая согласие, имеют равную силу.

Если обработка персональных данных может осуществляться на одном из оснований, не требующих согласия, то его получение влечет избыточную обработку персональных данных.

В комментируемой статье приведены основания для обработки так называемых ”обычных“ персональных данных, не относящихся к специальным персональным данным, порядок обработки которых установлен ст. 8 Закона.

Всего в комментируемой статье содержится двадцать таких оснований. Однако, несмотря на видимую множественность, все они могут быть сведены к следующим основаниям:

оформление и реализация трудовых (служебных) отношений;

заключение и исполнение договора;

обработка персональных данных, указанных в документе, адресованном оператору;

защита жизни, здоровья или иных жизненно важных интересов человека;

обработка распространенных ранее персональных данных;

обработка обезличенных персональных данных для научных или иных исследовательских целей;

выполнение обязанностей (реализация полномочий), предусмотренных законодательными актами.

Дело в том, что большинство перечисленных в рассматриваемой статье оснований (абзацы второй – седьмой, девятый – двенадцатый, четырнадцатый и двадцать первый) являются частными случаями обработки персональных данных, необходимой для выполнения обязанностей (реализации полномочий), предусмотренных законодательными актами. Выделение таких оснований в качестве самостоятельных объясняется стремлением заинтересованных организаций упростить правоприменение и облегчить ”узнавание“ как операторами, так и гражданами наиболее распространенных случаев обработки персональных данных без согласия в конкретных сферах деятельности.

Комментируемая статья предусматривает следующие случаи (основания), когда согласие субъекта персональных данных на обработку персональных данных не требуется:

для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности.

Порядок ведения административного и уголовного процессов установлен соответственно ПИКоАП и УПК.

В соответствии с п. 10 ч. 1 ст. 1.10 КоАП, ст.ст. 3.1 и 3.30 ПИКоАП ведение административного процесса осуществляется судом и уполномоченными на то органами и организациями (органами внутренних дел, административными комиссиями и др.). К органам, ведущим уголовный процесс, относятся органы уголовного преследования (органы дознания, следователи, прокуроры) и суд (ст. 6 УПК).

При совершении процессуальных действий, предусмотренных ПИКоАП и УПК, соответствующие органы и организации вправе осуществлять обработку персональных данных.

Так, например, в соответствии со ст. 3.29 ПИКоАП должностные лица органов, ведущих административный процесс, применяют профилактические меры воздействия, составляют протоколы, рассматривают дела об административных правонарушениях, налагают предусмотренные КоАП административные взыскания. Указанные действия неразрывно связаны с обработкой персональных данных, для которой на основании рассматриваемого абзаца второго ст. 6 Закона получать согласие субъекта персональных данных не требуется.

В свою очередь оперативно-розыскная деятельность регулируется Законом Республики Беларусь от 15.07.2015 307-З ”Об оперативно-розыскной деятельности“.

Оперативно-розыскную деятельность осуществляют:

органы внутренних дел;

органы государственной безопасности;

органы пограничной службы;

Служба безопасности Президента Республики Беларусь;

Оперативно-аналитический центр при Президенте Республики Беларусь;

органы финансовых расследований Комитета государственного контроля;

таможенные органы;

разведывательные службы Вооруженных Сил Республики Беларусь.

Органы, осуществляющие оперативно-розыскную деятельность, при выполнении задач оперативно-розыскной деятельности, в частности, имеют право:

создавать и (или) использовать базы данных (учеты), информационные системы, средства негласного получения (фиксации) информации и иные средства в соответствии с указанным Законом и иными актами законодательства;

получать безвозмездно сведения из баз данных (учетов), информационных систем путем удаленного доступа

и (или) на материальных носителях информации от организаций, которые являются собственниками этих баз данных (учетов), информационных систем, в случаях, установленных законодательными актами, и порядке, определенном законодательством;

собирать, обрабатывать, хранить и изучать сведения и документы, необходимые для выполнения задач оперативно-розыскной деятельности;

получать от граждан на безвозмездной или возмездной основе сведения, необходимые для выполнения задач оперативно-розыскной деятельности;

направлять в организации письменные запросы о внесении в базы данных (учеты), информационные системы, собственниками которых являются эти организации, изменений, необходимых для выполнения задач оперативно-розыскной деятельности;

для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов.

Данное основание охватывает фактически два случая обработки персональных данных:

осуществление правосудия;

исполнительное производство.

Законодательными актами предусмотрено, что правосудие осуществляется только судом.

Обязанности (полномочия) суда (судей) при осуществлении правосудия установлены, в частности Кодексом Республики Беларусь о судоустройстве и статусе судей, ПИКоАП, УПК, Хозяйственным процессуальным кодексом Республики Беларусь, ГПК и рядом иных законодательных актов.

Например, абзацем четвертым ч. 2 ст. 71 Кодекса Республики Беларусь о судоустройстве и статусе судей предусмотрено, что для осуществления правосудия судья имеет право запрашивать и получать в установленном порядке на безвозмездной основе сведения из информационных систем государственных органов и иных организаций и иметь доступ, в том числе удаленный, к таким информационным системам, содержащим персональные данные, запрашивать и получать в установленном порядке на безвозмездной основе от государственных органов и иных организаций без письменного согласия граждан сведения из информационных систем, содержащих персональные данные, по письменному запросу или на основании соглашения о предоставлении персональных данных, заключенного Верховным Судом Республики Беларусь с собственником (владельцем) информационного ресурса (системы).

Обработка персональных данных при реализации перечисленных полномочий и в иных подобных случаях осуществляется без согласия субъекта персональных данных на основании абзаца третьего ст. 6 Закона.

Необходимо отметить, что при осуществлении правосудия персональные данные обрабатываются не только судом, но и участниками судебного процесса, в том числе истцом и ответчиком. Так, в частности, ст. 56 ГПК предусмотрено право заинтересованных в исходе дела лиц подавать заявления, знакомиться с материалами дела, делать выписки из них, снимать копии представленных документов, заявлять отводы, представлять доказательства, участвовать в исследовании доказательств, задавать вопросы другим участникам судопроизводства по делу, заявлять ходатайства, давать устные и письменные объяснения суду, представлять свои доводы и соображения, возражать против ходатайств, доводов и соображений других лиц, обжаловать (опротестовывать) судебные постановления, а также совершать иные процессуальные действия, предусмотренные ГПК.

Обработка персональных данных такими лицами осуществляется на основании абзаца двадцатого рассматриваемой статьи – для выполнения полномочий, предусмотренных законодательными актами.

Пример.

В Национальном центре защиты персональных данных рассматривалась жалоба субъекта персональных данных на незаконное получение информации о его предыдущей работе ответчиком по его исковому заявлению о взыскании заработной платы и расторжении трудового договора по требованию работника.

При рассмотрении жалобы установлено, что информация о предыдущей трудовой деятельности получена судом в рамках истребования доказательств в ходе рассмотрения гражданского дела по иску заявителя. Данные сведения хранились в материалах дела и были получены ответчиком без согласия истца в ходе ознакомления с материалами дела, то есть при реализации им полномочий, предусмотренных законодательным актом – ГПК.

Обработка персональных данных без согласия субъекта персональных данных также осуществляется *для исполнения судебных постановлений и иных исполнительных документов*.

Перечень исполнительных документов содержится в ст. 10 Закона ”Об исполнительном производстве“, согласно которой наряду с судебными постановлениями к ним, в частности, относятся:

постановления органа, ведущего административный процесс, в части имущественных взысканий по делам об административных правонарушениях;

исполнительные надписи нотариусов, дипломатических агентов дипломатических представительств Республики Беларусь и консульских должностных лиц консульских учреждений Республики Беларусь о взыскании денежных сумм (задолженности);

постановления прокуроров о выселении в административном порядке;

удостоверения комиссий по трудовым спорам;

решения налоговых органов о взыскании налогов, сборов (пошлин), а также иных обязательных платежей в республиканский и местные бюджеты, контроль за правильностью исчисления, своевременностью и полнотой уплаты которых возложен на налоговые органы, и др.

В соответствии со ст. 6 Закона ”Об исполнительном производстве“ исполнение исполнительных документов возлагается на главное управление принудительного исполнения Министерства юстиции и территориальные органы принудительного исполнения, а непосредственное осуществление функций по исполнению исполнительных документов – на судебных исполнителей. В случаях, предусмотренных актами законодательства, функции по непосредственному исполнению исполнительных документов могут возлагаться на иных работников соответствующих органов принудительного исполнения, кроме лиц, осуществляющих обеспечение деятельности и техническое обслуживание этих органов, на которых при исполнении ими исполнительных документов также распространяется законодательство об исполнительном производстве.

Статьей 63 Закона ”Об исполнительном производстве“ определены полномочия судебного исполнителя при исполнении исполнительных документов. В частности, он имеет право:

получать по находящимся в его производстве исполнительным документам от граждан, в том числе индивидуальных предпринимателей, должностных лиц государственных органов и иных организаций на безвозмездной основе необходимые материалы и (или) документы, информацию (за исключением первичных статистических данных), включая информацию, содержащую банковскую и (или) иную охраняемую законом тайну, с соблюдением требований, установленных законодательными актами;

получать по находящимся в его производстве исполнительным документам на безвозмездной основе без письменного согласия физических лиц сведения из информационных ресурсов и систем, содержащих персональные данные, а также иметь доступ, включая удаленный, к информационным ресурсам и системам, содержащим такие данные, по письменному запросу или на основании соглашения о предоставлении персональных данных государственными органами

и (или) иными организациями, в том числе с использованием общегосударственной автоматизированной информационной системы;

использовать технические средства, осуществляющие звуко- и видеозапись, кино- и фотосъемку.

Обработка персональных данных при реализации судебными исполнителями перечисленных и иных полномочий и обязанностей, предусмотренных Законом ”Об исполнительном производстве“ и принятыми в его развитие иными нормативными правовыми актами, осуществляется без согласия субъекта персональных данных на основании абзаца третьего комментируемой статьи.

Данное основание применимо и иными операторами, которые вовлечены в процесс исполнительного производства и на которых возложена обязанность по совершению определенных действий, связанных с исполнением исполнительного документа, или по воздержанию от совершения определенных действий (банками и (или) небанковскими кредитно-финансовыми организациями, организациями по государственной регистрации недвижимого имущества, прав на него и сделок с ним, третьими лицами, собственниками имущества (учредителями, участниками) должника – юридического лица и др.);

в целях осуществления контроля (надзора) в соответствии с законодательными актами.

Основным комплексным законодательным актом, регулирующим вопросы осуществления контроля (надзора), является Указ № 510, которым предусмотрено два вида контроля – государственный и общественный.

Поскольку в приведенном основании обработки персональных данных не уточняется, о каких видах контроля идет речь, оно применимо для целей как государственного, так и общественного контроля.

Государственный контроль (надзор) осуществляется в формах выборочных проверок, внеплановых проверок, мероприятий технического (технологического, поверочного) характера, а также мер профилактического и предупредительного характера.

Указом № 510 утвержден перечень контролирующих (надзорных) органов, уполномоченных проводить проверки в рамках государственного контроля, и сфер их контрольной (надзорной) деятельности, а также определены права и обязанности данных органов при осуществлении этой деятельности.

Так, например, п. 4 Положения о порядке организации и проведения проверок, утвержденного Указом № 510, предусмотрено, что контролирующие (надзорные) органы и проверяющие в пределах своей компетенции вправе, в частности:

в рамках вопросов, подлежащих проверке, требовать и получать от проверяемого субъекта, участников контрольного обмера необходимые для проверки документы (их копии), в том числе в электронном виде, иную информацию, касающуюся его деятельности и имущества;

получать доступ в пределах своей компетенции к базам и банкам данных проверяемого субъекта с учетом требований законодательства об информации, информатизации и защите информации;

при проведении проверки использовать технические средства, в том числе аппаратуру, осуществляющую звуко- и видеозапись, кино- и фотосъемку, ксерокопирование, устройства для сканирования документов, идентификаторы скрытых изображений, для контроля (надзора) за соблюдением законодательства, сбора и фиксации доказательств, подтверждающих факты правонарушений.

Общественный контроль осуществляется профессиональными союзами, их организационными структурами, объединениями таких союзов и их организационными структурами (п. 5 Указа № 510). Случаи и порядок осуществления этого вида контроля установлены Указом Президента Республики Беларусь от 6 мая 2010 г. № 240 ”Об осуществлении общественного контроля профессиональными союзами“, который наделяет профессиональные союзы правами, аналогичными перечисленным выше.

Важно учитывать, что наличие у контролирующих (надзорных) органов и профсоюзов соответствующих прав (полномочий), позволяющих осуществлять обработку персональных данных без согласия субъектов персональных данных, не освобождает их от обязанности соблюдать общие требования к обработке персональных данных, предусмотренные ст. 4 Закона, в том числе требования о соответствии содержания и объема обрабатываемых персональных данных заявленным целям их обработки и исключении избыточной обработки персональных данных.

Данное требование корреспондирует с закрепленной в абзаце шестом п. 6 Положения о порядке организации и проведения проверок обязанностью контролирующих (надзорных) органов и проверяющих требовать у проверяемых субъектов только те сведения и документы, которые относятся к вопросам, подлежащим проверке, и которые субъект обязан иметь (вести, составлять) в соответствии с законодательными актами.

Применение данного основания (весьма обширного по своему содержанию) также не снимает с организаций, предоставляющих персональные данные, обязанностей по соблюдению требований ст. 4 Закона, в том числе по исключению чрезмерной обработки

персональных данных, разновидностью которой является их предоставление, и по информированию субъекта персональных данных о том, какие персональные данные и кому предоставлялись. В этой связи оператор, предоставляющий контролирующим органам информацию, при наличии сомнений может запрашивать дополнительную информацию на предмет соблюдения положений ст. 4 Закона, в частности, уточнения правовых оснований, целей и, соответственно, объема информации, необходимой для их достижения;

при реализации норм законодательства в области национальной безопасности, о борьбе с коррупцией, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения.

Данное основание охватывает ряд случаев, в которых обработка персональных данных осуществляется в связи с реализацией государственными органами и иными организациями публично значимых функций. В одних законодательных актах предусматривается конкретный перечень обрабатываемых персональных данных (например, круг сведений, подлежащих установлению при идентификации клиентов – физических лиц, осуществляющих финансовые операции), в то время как в других – перечень таких данных в самом акте не закрепляется и вытекает из сути осуществляемых действий.

Для большинства людей рассматриваемые виды деятельности характеризуются высокой степенью закрытости, широкой распространенностью принудительных мер, сложностью оценки соразмерности применяемых мер, что во многом вытекает из задач, которые стоят перед соответствующими структурами.

Отражением этого факта являются предусмотренные Законом применительно к указанным сферам изъятия из права на получение информации, касающейся обработки персональных данных, и права на получение информации о предоставлении персональных данных третьим лицам.

Тем не менее, подобные особенности не означают выведения всей деятельности из-под сферы законодательства о персональных данных. Названные структуры обязаны соблюдать положения Закона об общих требованиях к обработке персональных данных (ст. 4 Закона), необходимости реализации мер по их защите (ст. 17 Закона) и несут ответственность за допущенные нарушения;

при реализации норм законодательства о выборах, референдуме, об отзыве депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, депутата местного Совета депутатов.

Сбор подписей, подача деклараций кандидатами, изготовление информационных материалов о кандидатах, регистрация инициативных групп и многие другие процессы, предусмотренные Избирательным кодексом Республики Беларусь, неизменно сопровождаются обработкой персональных данных.

Независимо от того, кто их обрабатывает, такая обработка, если она вытекает из норм законодательства о выборах, референдуме, об отзыве депутата Палаты представителей, члена Совета Республики Национального собрания Республики Беларусь, депутата местного Совета депутатов, будет осуществляться без согласия субъектов персональных данных.

Особенностью обработки персональных данных при реализации этого законодательства является необходимость обеспечения, с одной стороны, прозрачности избирательного процесса, а с другой – тайны голосования избирателей. Так, избиратели должны понимать, за кого они голосуют, что обуславливает необходимость распространения информации о кандидатах. В то же время информация о том, кто и за кого голосовал, является тайной и в этой связи должны быть исключены любые действия, связанные с ее нарушением;

для ведения индивидуального (персонифицированного) учета сведений о застрахованных лицах для целей государственного социального страхования, в том числе профессионального пенсионного страхования.

Данное основание применяется органами Фонда социальной защиты населения Министерства труда и социальной защиты Республики Беларусь (далее – Фонд), на который Указом Президента Республики Беларусь от 16 января 2009 г. № 40 возложены функции организации и ведения индивидуального (персонифицированного) учета в системе государственного социального страхования сведений о физических лицах, на которых распространяется государственное социальное страхование (абзац пятый п. 8 Положения о Фонде социальной защиты населения Министерства труда и социальной защиты Республики Беларусь, утвержденного названным Указом).

При ведении индивидуального (персонифицированного) учета органы Фонда обрабатывают огромный массив персональных данных. Их перечень отражается на индивидуальном лицевом счете застрахованного лица и определен ст. 6 Закона Республики Беларусь от 6 января 1999 г. № 230-З ”Об индивидуальном (персонифицированном) учете в системе государственного социального страхования“ (далее – Закон ”Об индивидуальном (персонифицированном) учете в системе государственного социального страхования“). Обработка этих персональных данных органами Фонда

осуществляется без согласия субъектов персональных данных на основании рассматриваемой нормы Закона.

Следует также учитывать, что источниками персональных данных, необходимых для ведения индивидуального (персонифицированного) учета, являются плательщики взносов на государственное социальное страхование (далее – плательщики взносов) – работодатели, Белорусское республиканское унитарное страховое предприятие ”Белгосстрах“, физические лица, самостоятельно уплачивающие обязательные страховые взносы, организации, в которых обеспечивались денежным довольствием военнослужащие срочной военной службы.

Права и обязанности плательщиков взносов определены ст. 10 Закона ”Об индивидуальном (персонифицированном) учете в системе государственного социального страхования“. Так, например, они обязаны:

представлять в установленном порядке в органы, осуществляющие персонифицированный учет, достоверные сведения, необходимые для ведения персонифицированного учета;

представлять по требованию застрахованного лица сведения о нем, переданные в эти органы.

Обработка персональных данных субъектов персональных данных плательщиками взносов при реализации ими своих прав и обязанностей осуществляется на основании абзаца двадцатого ст. 6 Закона;

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

В связи с неравным статусом сторон в рамках трудовых отношений согласие работников на обработку их персональных данных нанимателем, как правило, не может носить свободного характера и, соответственно, выступать правовым основанием для обработки. В большинстве случаев такая обработка осуществляется в силу требований законодательства.

Данное основание охватывает два случая обработки персональных данных:

при оформлении трудовых (служебных) отношений;

в процессе трудовой (служебной) деятельности.

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

Данное основание также не используется, когда обработка персональных данных работника осуществляется в период трудовой

(служебной) деятельности, но не связана непосредственно с трудовой функцией работника (например, при организации добровольного медицинского страхования, если это не предусмотрено коллективным договором или коллективный договор в организации отсутствует).

Важным условием применения абзаца восьмого комментируемой статьи является закрепление необходимости обработки определенных персональных данных в законодательстве. При этом в силу многообразия процессов, в которых используются персональные данные работников, не всегда возможно в акте законодательства детально прописать все компоненты и случаи обработки.

В этой связи данное условие имеет достаточно широкое применение. К таким случаям относятся как ситуации, когда обработка персональных данных и круг обрабатываемых персональных данных работников прямо предусматриваются в нормативных правовых актах, так и ситуации, когда в акте законодательства данная информация напрямую не указана, но необходимость такой обработки прямо вытекает из предписаний этого акта, возлагающего на нанимателя определенные обязанности или предоставляющего ему определенные полномочия.

Например, при приеме на работу работник заполняет ряд документов, в том числе личный листок по учету кадров, форма которого установлена приложением 2 к Инструкции о порядке формирования, ведения и хранения личных дел работников, утвержденной постановлением Комитета по архивам и делопроизводству при Совете Министров Республики Беларусь от 26 марта 2004 г. № 2. В этой связи объем персональных данных предопределен содержанием установленной формы.

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

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

и определяется в каждой конкретной ситуации, исходя из существа гарантии.

Во всех указанных и подобных ситуациях правовым основанием для обработки персональных данных работников будет являться абзац восьмой ст. 6 Закона.

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

Вопрос о допустимости обработки на данном основании персональных данных третьих лиц, например, членов семьи работника, лиц, дающих рекомендации и т.п. заслуживает отдельного внимания. Если такая обработка напрямую предусмотрена законодательством (например, заполнение личного листка по учету кадров, личной карточки воинского учета по установленной форме) или обусловлена необходимостью выполнения возложенных на нанимателя законодательством обязанностей (например, при предоставлении социального отпуска при рождении ребенка, компенсаций в связи с переездом на работу в другую местность и т.п.), она осуществляется без согласия указанных лиц на основании рассматриваемого абзаца ст. 6 Закона. Иными словами, работник может предоставлять нанимателю сведения о родственниках без получения их согласия.

Если обработка персональных данных близких родственников (членов семьи) работника законодательством не предусмотрена, то требуется иное правовое основание (например, согласие), а также обеспечение соответствия обработки таких данных требованиям ст. 4 Закона (прежде всего, соразмерность обработки и запрет избыточности)[17];

для осуществления нотариальной деятельности.

В соответствии с п. 1 ст. 3 Закона Республики Беларусь от 18 июля 2004 г. № 305-З ”О нотариате и нотариальной деятельности“ (далее – Закон о нотариате) под нотариальной деятельностью понимаются

[17] В целях определения единообразных подходов к обработке нанимателями персональных данных работников, а также соискателей на трудоустройство Национальным центром защиты персональных данных разработаны Рекомендации об обработке персональных данных в связи с трудовой (служебной) деятельностью, в которых отражены как общие подходы к обработке персональных данных в сфере трудовых отношений, так и конкретные примеры случаев такой обработки. Рекомендации размещены на официальном интернет-сайте Центра.

совершение от имени Республики Беларусь нотариусами, уполномоченными должностными лицами, должностными лицами загранучреждений нотариальных действий, предусмотренных данным законом и иными законодательными актами, международными договорами Республики Беларусь, а также оказание нотариусами услуг правового и технического характера.

Таким образом, наряду с нотариусами обработку персональных данных на данном основании при осуществлении нотариальной деятельности могут осуществлять уполномоченные должностные лица местных исполнительных и распорядительных органов, а также загранучреждений.

Полномочия нотариусов определены в ст. 24 Закона о нотариате. Так, например, в соответствии с п. 1 данной статьи нотариусы вправе:

истребовать и получать от государственных органов, иных организаций, индивидуальных предпринимателей и нотариусов, в том числе из государственных информационных ресурсов (систем) в установленном законодательными актами порядке, сведения и (или) документы, необходимые для осуществления нотариальной деятельности;

составлять проекты сделок, доверенностей, согласий, отказов, заявлений и иных нотариальных документов;

изготавливать копии документов и выписки из них и др.

Пунктом 1 ст. 25 Закона о нотариате на нотариусов возложен ряд обязанностей, в том числе:

проверять действительность представляемых гражданами и юридическими лицами для совершения нотариальных действий сведений и (или) документов посредством получения информации из информационных ресурсов (систем) государственных органов и иных организаций, к которым нотариус имеет доступ в соответствии с законодательством и (или) на основании соглашений, заключенных Белорусской нотариальной палатой с собственниками (владельцами) информационных ресурсов (систем);

вносить в единую электронную систему учета нотариальных действий и наследственных дел сведения в порядке, установленном Советом Министров Республики Беларусь.

Важно отметить, что в соответствии с п. 2 ст. 19 Закона о нотариате внесение сведений в единую электронную систему учета нотариальных действий и наследственных дел, сбор, систематизация, хранение, изменение, использование таких сведений нотариусами, а также уполномоченными должностными лицами местных исполнительных и распорядительных органов и должностными лицами загранучреждений осуществляются без согласия физических

или юридических лиц, от имени, на имя, по поручению либо в отношении которых совершается (совершено) нотариальное действие или подаются (поданы) заявления, указанные в п. 2 ст. 81 названного Закона, либо иных лиц, участвующих (участвовавших) в совершении нотариального действия, и не являются разглашением нотариальной тайны.

Таким образом, истребование персональных данных из соответствующих информационных ресурсов (систем) государственных органов и иных организаций для проверки действительности представляемых нотариусу сведений и (или) документов, в том числе удостоверяющих личность, и их последующее внесение в единую электронную систему учета нотариальных действий и наследственных дел осуществляется без согласия субъекта персональных данных;

при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь.

Порядок рассмотрения перечисленных вопросов, обязанности, полномочия и порядок взаимодействия участвующих в этом государственных органов регламентированы соответственно Законом Республики Беларусь от 1 августа 2002 г. № 136-З ”О гражданстве Республики Беларусь“ и Законом Республики Беларусь от 23 июня 2008 г. № 354-З ”О предоставлении иностранным гражданам и лицам без гражданства статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь“, а также принятыми в их развитие иными нормативными правовыми актами.

Согласно ст. 28 Закона Республики Беларусь ”О гражданстве Республики Беларусь“ решения по вопросам гражданства Республики Беларусь принимаются Президентом Республики Беларусь, органами внутренних дел, органами дипломатической службы.

На указанные органы возложен ряд полномочий, требующих обработки персональных данных, например по приему заявлений по вопросам гражданства Республики Беларусь, проверке фактов и документов, представленных в обоснование таких заявлений.

Указом Президента Республики Беларусь от 17 ноября 1994 г. № 209 утверждено Положение о порядке рассмотрения вопросов, связанных с гражданством Республики Беларусь, которым определен порядок приема, оформления и рассмотрения заявлений по вопросам гражданства Республики Беларусь, взаимодействия государственных органов при рассмотрении заявлений, принятия, исполнения и отмены решений по этим вопросам.

В частности, данное Положение предусматривает предварительное (до внесения на рассмотрение Президента Республики Беларусь) рассмотрение заявлений о приеме в гражданство Республики Беларусь, выходе из гражданства Республики Беларусь вместе с материалами дел по ним Комиссией по вопросам гражданства при Президенте Республики Беларусь, которая в том числе наделена правом запрашивать дополнительные документы и (или) материалы у соответствующих государственных органов, иных организаций, которые обязаны представить их в установленный Комиссией срок.

Положением о порядке рассмотрения вопросов, связанных с гражданством Республики Беларусь также определены формы заявлений и перечни необходимых документов и (или) материалов, являющихся основанием для приобретения и прекращения гражданства Республики Беларусь.

Инструкцией о порядке организации работы по предоставлению статуса беженца, дополнительной защиты и убежища в Республике Беларусь, утвержденной постановлением Министерства внутренних дел Республики Беларусь от 22 июня 2017 г. № 173, предусмотрено, например, заполнение анкеты иностранного гражданина или лица без гражданства, ходатайствующего о предоставлении статуса беженца, дополнительной защиты или убежища в Республике Беларусь по форме согласно приложению 4 к данной Инструкции.

Необходимо отметить, что в формах заявлений, анкет, а также в документах и материалах, требуемых для рассмотрения вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь, содержатся как ”обычные“ персональные данные (фамилия, собственное имя, отчество, число, месяц, год и место рождения, семейное положение и состав семьи, сведения о близких родственниках с указанием их места жительства, трудовая деятельность, образование и т.п.), так и специальные персональные данные (о вероисповедании, национальности, политической или общественной деятельности, привлечении к административной или уголовной ответственности, результаты обязательной государственной дактилоскопической регистрации и обязательного медицинского освидетельствования и т.п.). В этой связи в большинстве случаев обработка персональных данных при рассмотрении вопросов, связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь, будет осуществляться одновременно на двух правовых основаниях, предусмотренных абзацем десятым ст. 6 и абзацем девятым п. 2 ст. 8 Закона;

в целях назначения и выплаты пенсий, ежемесячного денежного содержания отдельным категориям государственных служащих, пособий.

В первоначальной редакции данное основание охватывало лишь цели назначения и выплаты пенсий и пособий. Законом Республики Беларусь от 1 июня 2022 г. № 175-З "О государственной службе" (далее – Закон "О государственной службе") оно дополнено еще одной целью – назначение и выплата ежемесячного денежного содержания отдельным категориям государственных служащих, что вполне логично, поскольку ежемесячное содержание также является одним из видов социального обеспечения, альтернативным пенсии.

Поскольку в приведенном основании не уточняется, о каких видах пенсий и пособий идет речь, оно применимо при обработке персональных данных государственными органами и иными организациями, осуществляющими назначение и выплату любых пенсий и пособий, предусмотренных законодательством, например:

органами по труду, занятости и социальной защите – при назначении и выплате пенсий в соответствии с Законом Республики Беларусь от 17 апреля 1992 г. № 1596-XII "О пенсионном обеспечении", а также ежемесячного денежного содержания в соответствии с Положением о порядке назначения и выплаты ежемесячного денежного содержания отдельным категориям государственных служащих, утвержденным Указом Президента Республики Беларусь от 30 ноября 2006 г. № 705. В отдельных случаях вопрос о назначении трудовых и социальных пенсий решается комиссией по назначению пенсий, образуемой районным (городским) исполнительным и распорядительным органом, которая будет осуществлять обработку персональных данных также на указанном основании;

органами Фонда – при назначении и выплате досрочных профессиональных пенсий в соответствии с Законом Республики Беларусь от 5 января 2008 г. № 322-З "О профессиональном пенсионном страховании";

пенсионными органами Министерства обороны, Министерства внутренних дел, Министерства по чрезвычайным ситуациям и Комитета государственной безопасности – при назначении и выплате пенсий и пособий в соответствии с Законом Республики Беларусь от 17 декабря 1992 г. № 2050-XII "О пенсионном обеспечении военнослужащих, лиц начальствующего и рядового состава органов внутренних дел, Следственного комитета, Государственного комитета судебных экспертиз, органов и подразделений по чрезвычайным ситуациям и органов финансовых расследований";

Комиссией по установлению пенсий за особые заслуги при Совете Министров Республики Беларусь, Министерством труда и социальной защиты – при установлении пенсий за особые заслуги перед Республикой Беларусь в соответствии с Положением о пенсиях за особые заслуги перед Республикой Беларусь, утвержденным постановлением Совета Министров Республики Беларусь от 30 марта 1993 г. № 185;

государственными органами и иными организациями, назначающими и выплачивающими государственные пособия по государственному социальному страхованию (пособия по беременности и родам, пособия, связанные с рождением ребенка, уходом за ребенком в возрасте до трех лет, пособия по временной нетрудоспособности, безработице, на погребение и т.п.), а также иные виды пособий (пособия по уходу за инвалидом I группы либо лицом, достигшим 80-летнего возраста, единовременного пособия в случае смерти государственного гражданского служащего и т.п.).

В упомянутых случаях обработка персональных данных государственными органами и иными организациями при реализации ими обязанностей (полномочий) для целей назначения и выплаты соответствующих пенсий и пособий будет осуществляться без согласия субъектов персональных данных.

В отдельных ситуациях рассматриваемые полномочия конкретизируются в законодательстве.

Так, например, в соответствии со ст. 14 Закона Республики Беларусь от 15 июня 2006 г. № 125-З ”О занятости населения Республики Беларусь“ органы государственной службы занятости населения на безвозмездной основе запрашивают и получают из информационных ресурсов (систем) персональные данные, в том числе специальные персональные данные, необходимые для назначения и осуществления им социальных выплат, к которым в том числе относится пособие по безработице.

Согласно ст. 9 Закона Республики Беларусь ”О пенсионном обеспечении“ органы, осуществляющие пенсионное обеспечение, на безвозмездной основе запрашивают и получают из информационных ресурсов (систем) персональные данные, в том числе специальные персональные данные, необходимые для назначения и выплаты пенсий, без согласия физических лиц.

Кроме того, ст. 5 Закона Республики Беларусь от 29 декабря 2012 г. № 7-З ”О государственных пособиях семьям, воспитывающим детей“ предусмотрено, что государственные органы, иные организации, назначающие и выплачивающие государственные пособия, для целей назначения и выплаты, а также для проверки представленных гражданами документов и (или) сведений имеют право, в частности,

самостоятельно запрашивать и получать без письменного согласия граждан у государственных органов, иных организаций любых организационно-правовых форм документы и (или) сведения, не включенные в перечни документов и (или) сведений, представляемых гражданами для назначения государственных пособий, в том числе содержащие персональные данные граждан, если такие документы и (или) сведения относятся к запрашиваемым документам и (или) сведениям, которые устанавливаются Советом Министров Республики Беларусь.

При этом необходимо учитывать, что при наличии специального правового основания для обработки персональных данных, включая специальные персональные данные, в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством, обработка персональных данных работников нанимателями для целей назначения и выплаты им пособий, предусмотренных законодательством (например, пособия по временной нетрудоспособности, по беременности и родам, по уходу за ребенком в возрасте до трех лет и т.п.), будет осуществляться на основании абзаца восьмого ст. 6 и абзаца третьего п. 2 ст. 8 Закона.

Следует отметить, что, как правило, выплата пенсий и пособий, назначаемых органами по труду, занятости и социальной защите, органами, осуществляющими пенсионное обеспечение военнослужащих и приравненных к ним лиц, органами Фонда, осуществляется по выбору получателя через банки и (или) объекты почтовой связи, организации, осуществляющие деятельность по доставке пенсий и пособий. Такой порядок выплаты закрепляется в соответствующем законодательном акте или принятом в его развитие ином нормативном правовом акте. Данные организации будут осуществлять обработку персональных данных для целей осуществления этих выплат на основании абзаца двадцатого комментируемой статьи;

для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации;

Определения терминов ”государственные статистические наблюдения“ и ”официальная статистическая информация“ содержатся в Законе Республики Беларусь от 28 ноября 2004 г. № 345-З ”О государственной статистике“ (далее – Закон ”О государственной статистике“).

Так, государственные статистические наблюдения – это сбор первичных статистических данных, осуществляемый органами государственной статистики или государственными организациями, уполномоченными на ведение государственной статистики, в целях формирования официальной статистической информации.

Официальная статистическая информация – информация об экономическом, демографическом, социальном положении и о состоянии окружающей среды в Республике Беларусь, сформированная путем обработки первичных статистических и (или) административных данных в соответствии с официальной статистической методологией.

С учетом приведенных определений рассматриваемое основание применимо только органами государственной статистики или иными государственными организациями, уполномоченными на ее ведение, и исключительно для целей государственной статистики.

Согласно ст. 17 Закона ”О государственной статистике“ органы государственной статистики ведут государственную статистику по формам централизованных государственных статистических наблюдений и указаниям по их заполнению и (или) с использованием административных данных, а также в соответствии с методиками по формированию и расчету статистических показателей и инструкциями по организации и проведению государственных статистических наблюдений, утверждаемыми республиканским органом государственного управления в области государственной статистики, и (или) в соответствии с международными стандартами и рекомендациями в области статистики.

При этом под административными данными понимается документированная информация (за исключением первичных статистических данных), полученная государственными органами и иными организациями в связи с осуществлением государственно-властных полномочий, административных процедур, контрольных (надзорных) и других функций, возложенных на них нормативными правовыми актами, и используемая для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации.

В соответствии со ст. 18 Закона ”О государственной статистике“ государственные статистические наблюдения проводятся по формам централизованных и нецентрализованных государственных статистических наблюдений, к которым относятся государственная статистическая отчетность, анкета, вопросник, переписной лист и иные формы государственных статистических наблюдений.

Обработка персональных данных, содержащихся в административных данных, а также в формах централизованных государственных статистических наблюдений, осуществляется органами государственной статистики и государственными организациями, уполномоченными на ведение государственной статистики, без согласия субъектов персональных данных.

Разновидностью такой обработки персональных данных является перепись населения, осуществляемая в соответствии с Законом ”О переписи населения“. Указанным Законом определены обязанности и полномочия государственных органов, осуществляющих подготовку и проведение переписи населения, обработка персональных данных для реализации которых осуществляется без согласия субъектов персональных данных.

Так, например, в соответствии со ст. 9 Закона ”О переписи населения“ указанные органы в пределах своей компетенции имеют право:

собирать, обрабатывать, хранить персональные данные респондентов без их письменного согласия с соблюдением требований законодательства Республики Беларусь о защите информации, распространение и (или) предоставление которой ограничено;

получать безвозмездно без письменного согласия респондентов от государственных органов и иных организаций в рамках программы переписи населения сведения из информационных ресурсов (систем), содержащих персональные данные, по письменному запросу или на основании соглашения о предоставлении персональных данных, заключенного с собственником (владельцем) информационного ресурса (системы).

Статья 11 Закона ”О переписи населения“ закрепляет основные права и обязанности переписного персонала. В частности, лица, входящие в состав переписного персонала:

имеют право получать в порядке, установленном этим Законом, персональные данные от респондентов согласно форме переписного листа, а также получать такие данные от государственных органов и иных организаций без письменного согласия респондентов;

обязаны при проведении опроса строго придерживаться перечня вопросов, содержащихся в переписном листе, и точно передавать их содержание.

В свою очередь, формы переписного листа утверждены постановлением Национального статистического комитета Республики Беларусь от 10 октября 2018 г. № 99 ”Об утверждении форм переписного листа и иной переписной документации“;

в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных.

Указанное правовое основание может быть применено при одновременном соблюдении следующих условий:

обработка персональных данных осуществляется в научных или иных исследовательских целях;

персональные данные обезличены *(об обезличивании см. комментарий к ст. 1 Закона)*.

По сути, рассматриваемое основание является способом найти баланс между необходимостью развития новых технологий (большие данные, искусственный интеллект и др.), требующих обработки массивов персональных данных для создания новых сервисов и др., и требованиями законодательства о персональных данных.

Под научными целями понимаются цели, отвечающие критериям научной деятельности в соответствии с Законом Республики Беларусь от 21 октября 1996 г. № 708-XIII "О научной деятельности", определяющим ее как творческую деятельность, направленную на получение новых знаний о природе, человеке, обществе, искусственно созданных объектах и на использование научных знаний для разработки новых способов их применения.

Пример.

Оператор электросвязи передает персональные данные в обезличенном виде (номера телефонов абонентов, отобранных по обозначенным критериям (пол, возраст и др.) организациям, которые аккредитованы согласно постановлению Совета Министров Республики Беларусь от 8 ноября 2005 г. № 1240 "О некоторых вопросах проведения опросов общественного мнения, относящихся к республиканским референдумам, выборам и общественно-политической ситуации в стране, и об опубликовании их результатов в средствах массовой информации", для проведения исследований и опросов общественного мнения.

Определение термина "исследовательские цели" в законодательстве отсутствует, однако с учетом случаев его применения в нормативных правовых актах такой термин должен иметь довольно широкое трактование. Вместе с тем это основание не может применяться при обработке обезличенных персональных данных, направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и (или) его продвижение на рынке;

при осуществлении учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением и возмещения расходов на электроэнергию, платы за другие услуги и возмещения налогов, а также при предоставлении льгот и взыскании задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением и возмещению расходов на электроэнергию.

Данное основание применяется организациями, в полномочия которых входит осуществление соответствующих действий по учету, расчету и начислению платы за жилищно-коммунальные услуги, платы за пользование жилым помещением (например, расчетно-справочные центры), в том числе организации, на которые возложены функции по начислению безналичных жилищных субсидий и взысканию

задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением, возмещению расходов на электроэнергию (например, энергоснабжающие организации).

В соответствии с п. 36 ст. 1 Жилищного кодекса Республики Беларусь к организациям, осуществляющим учет, расчет и начисление платы за жилищно-коммунальные услуги и платы за пользование жилым помещением, относятся организации, оказывающие жилищно-коммунальные услуги и (или) осуществляющие функции учета, расчета и начисления платы за жилищно-коммунальные услуги, платы за пользование жилым помещением, возмещения расходов организаций, осуществляющих эксплуатацию жилищного фонда и (или) предоставляющих жилищно-коммунальные услуги, на электроэнергию, потребляемую на освещение вспомогательных помещений и работу оборудования в многоквартирных жилых домах, а также функции по начислению безналичных жилищных субсидий и взысканию задолженности по плате за жилищно-коммунальные услуги, плате за пользование жилым помещением, возмещению расходов на электроэнергию.

Согласно подп. 1.1 п. 1 Указа Президента Республики Беларусь от 31 декабря 2015 г. № 535 ”О предоставлении жилищно-коммунальных услуг“ начисление платы за жилищно-коммунальные услуги и платы за пользование жилыми помещениями в жилых домах товариществ собственников либо организаций застройщиков осуществляется с использованием единой общереспубликанской информационной системы по учету, расчету и начислению платы за жилищно-коммунальные услуги и платы за пользование жилым помещением (АИС ”Расчет-ЖКУ“), в том числе через уполномоченные местными исполнительными и распорядительными органами организации, осуществляющие учет, расчет и начисление платы за жилищно-коммунальные услуги и платы за пользование жилым помещением.

Абзац четырнадцатый комментируемой статьи не распространяется на организации, которые предоставляют сведения в АИС ”Расчет-ЖКУ“.

Основной механизм по информированию начисляющих организаций предусмотрен в постановлении Совета Министров Республики Беларусь от 12 июня 2014 г. № 571 ”О порядке расчетов и внесения платы за жилищно-коммунальные услуги и платы за пользование жилыми помещениями государственного жилищного фонда, а также возмещения расходов на электроэнергию“, принятом в соответствии с ч. 2 подп. 1.4 п. 1 Указа Президента Республики Беларусь от 5 декабря 2013 г. № 550 ”О некоторых вопросах регулирования тарифов (цен) на жилищно-коммунальные услуги и внесении изменений и дополнений в некоторые указы Президента

Республики Беларусь“ и ч. 4 п. 9 ст. 31 Жилищного кодекса Республики Беларусь.

Обработка персональных данных организациями, обязанными в соответствии с указанными нормативными правовыми актами или иными законодательными актами предоставлять сведения в АИС ”Расчет-ЖКУ“, осуществляется без согласия субъектов персональных данных на основании абзаца двадцатого ст. 6 Закона (обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами);

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

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

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

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

Пример.

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

оператор осуществляет обработку тех персональных данных физического лица, которые указаны в договоре либо получены в процессе его заключения (исполнения);

оператор осуществляет обработку персональных данных физического лица только для целей совершения действий, установленных договором, то есть, когда обработка персональных данных является необходимой для оказания услуг, выполнения работ, совершения действий в отношении конкретного физического лица, и без обработки таких данных выполнение обязательств по договору невозможно или существенно затруднено.

Пример.

Между оператором и субъектом персональных данных заключен договор купли-продажи, по которому оператор обязан осуществить доставку товаров. Для этой цели оператор может обрабатывать имя, фамилию, адрес места жительства и (или) номер телефона субъекта персональных данных.

Рассматриваемое основание применяется как в случае обработки персональных данных на основании заключенного договора, так и в случае обработки персональных данных субъекта персональных данных на стадии заключения договора. При этом на возможность применения данного основания не влияет тот факт, что в итоге договор с субъектом персональных данных может быть не заключен.

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

оставление заявки на сайте с контактными данными гражданина для связи и уточнения условий оказания услуг, продажи товаров, обсуждения стоимости и др.;

принятие условий пользовательского соглашения на сайте (публичного договора между владельцем интернет-ресурса и пользователем), например, посредством регистрации учетной записи на интернет-ресурсе.

Как обработку для целей исполнения договора следует расценивать ситуации:

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

осуществление гарантийного и постгарантийного обслуживания;

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

Не могут рассматриваться в качестве обработки для целей исполнения договора способы обработки, не являющиеся необходимыми для исполнения договора.

Пример.

Обработка оператором персональных данных субъекта персональных данных с целью направления ему информации рекламного характера на основании абзаца пятнадцатого ст. 6 Закона недопустима.

В случае неисполнения одной из сторон условий договора другая сторона может осуществлять обработку персональных данных в целях защиты своих прав, например составления искового заявления в суд. Правовым основанием в данном случае будет выступать абзац двадцатый ст. 6 Закона (реализация полномочий, предоставленных законодательным актом).

Следует также учитывать, что с 1 января 2023 г. Законом Республики Беларусь от 14 октября 2022 г. № 213-З "О лицензировании" (ст. 231) ограничено проведение юридическими лицами, оказывающими юридические услуги, досудебной работы по взысканию задолженности с должников, являющихся физическими лицами. В этой связи рассматриваемое основание (исполнение договора) не может быть использовано для передачи персональных данных юридическим лицам для проведения досудебной работы по взысканию задолженности с физических лиц.

Для обработки персональных данных физического лица в целях, не связанных с заключением (исполнением) договора, требуется согласие физического лица или иное правовое основание, предусмотренное законодательными актами;

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

Такое основание может быть применено, если:

документ адресован оператору;

документ подписан субъектом персональных данных (собственноручно либо с использованием электронной цифровой подписи или иных технических средств, компьютерных программ, информационных систем или информационных сетей, если такой способ подписания позволяет достоверно установить, что документ подписан субъектом персональных данных);

обработке подлежат те персональные данные, которые указаны в документе;

обработка осуществляется для целей, указанных в документе.

Примером обработки персональных данных на данном основании является подача работниками заявлений на оказание материальной помощи, частичное возмещение стоимости путевок в санаторно-

курортные и оздоровительные учреждения, компенсацию стоимости подписки, абонементов и т.п.

Следует отметить, что указанное основание не применяется в случаях, когда в организацию поступает документ, подписанный субъектом персональных данных, но необходимость направления такого документа (заявления) вытекает из законодательных актов и (или) форма такого документа устанавливается законодательством. Кроме того, оно не применяется, если форма заявления и круг указываемых в нем персональных данных определяются оператором, иначе это даст возможность операторам ”обходить“ требования Закона;

в целях осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации, организации, осуществляющей издательскую деятельность, направленных на защиту общественного интереса, представляющего собой потребность общества в обнаружении и раскрытии информации об угрозах национальной безопасности, общественному порядку, здоровью населения и окружающей среде, информации, влияющей на выполнение своих обязанностей государственными должностными лицами, занимающими ответственное положение, общественными деятелями, за исключением случаев, предусмотренных гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса.

Данное основание может быть использовано в деятельности журналиста, средства массовой информации, а также организации, осуществляющей издательскую деятельность, и предназначено для установления баланса между правом на защиту персональных данных и правом на свободу журналисткой деятельности в части поиска информации. Обработка персональных данных этими лицами допускается без согласия субъектов персональных данных в случаях, когда имеется превалирование общественных интересов над личными правами.

Пунктом 7 ст. 1 Закона Республики Беларусь от 17 июля 2008 г. № 427-З ”О средствах массовой информации“ (далее – Закон ”О средствах массовой информации“) определено, что журналист средства массовой информации – это физическое лицо, занимающееся сбором, редактированием и созданием (подготовкой) информационных сообщений и (или) материалов для юридического лица, на которое возложены функции редакции средства массовой информации, связанное с этим юридическим лицом трудовыми либо другими договорными отношениями.

В этой связи рассматриваемое основание неприменимо для так называемых блогеров независимо от того, какое количество подписчиков у них имеется, а также для информационных ресурсов, не зарегистрированных в качестве сетевого издания.

Данное основание является развитием предписаний ст. 40 Закона ”О средствах массовой информации“, конкретизируя условия ее применения. Оно раскрывает используемый в указанной статье термин ”общественный интерес“, понимая под ним потребность общества в обнаружении и раскрытии информации об угрозах национальной безопасности, общественному порядку, здоровью населения и окружающей среде, информации, влияющей на выполнение своих обязанностей государственными должностными лицами, занимающими ответственное положение, общественными деятелями, за исключением случаев, предусмотренных гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса.

В этой связи такое основание не применяется в случаях, когда обработка персональных данных не обусловлена защитой общественного интереса, например при осуществлении фото- и видеосъемок на праздниках, юбилеях, при обычных интервью и т.п. В подобных ситуациях обработка персональных данных должна осуществляться на ином правовом основании (например, на основании абзаца двадцатого ст. 6 Закона).

Так, согласно подп. 4.7 п. 4 ст. 34 Закона ”О средствах массовой информации“ журналист средства массовой информации обязан получать согласие физических лиц на проведение аудио- и видеозаписи, кино- и фотосъемок, за исключением их проведения в местах, открытых для массового посещения, на массовых мероприятиях.

Данное основание также не применяется к случаям обработки персональных данных, предусмотренным гражданским процессуальным, хозяйственным процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса.

Порядок осуществления лицами, присутствующими в открытом судебном заседании, фотосъемки и ведения видеозаписи в ходе судебного разбирательства дела закреплен во всех процессуальных кодексах, согласно которым осуществление фото-, киносъемки и видеозаписи допускается с разрешения суда (председательствующего) с учетом мнения юридически заинтересованных в исходе дела лиц, участвующих в деле (ч. 4 ст. 271 ГПК), лиц, участвующих в судебном заседании (ч. 6 ст. 176 Хозяйственного процессуального кодекса Республики

Беларусь), при наличии согласия сторон (ч. 6 ст. 287 УПК) или лиц, участвующих в рассмотрении дела об административном правонарушении (ч. 6 ст. 6.12 ПИКоАП).

Пунктом 6 постановления Пленума Верховного Суда Республики Беларусь от 20 декабря 2013 г. № 11 "Об обеспечении гласности при осуществлении правосудия и о распространении информации о деятельности судов" разъясняется, что лица, не являющиеся участниками судебного процесса, журналисты средств массовой информации обращаются к суду с соответствующей просьбой (заявлением). Наличие такого ходатайства (просьбы), а также мнение сторон отражаются в протоколе судебного заседания;

для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Аналогичное правовое основание обработки персональных данных без согласия субъекта персональных данных предусмотрено в международных актах, в том числе в Конвенции о защите физических лиц при автоматизированной обработке персональных данных, в GDPR, в Федеральном законе Российской Федерации от 27 июля 2006 г. № 152-ФЗ "О персональных данных".

Данное основание имеет устоявшуюся узкую трактовку и применяется в очень редких ситуациях, когда имеется прямая угроза жизни, например при оказании неотложной медицинской помощи (когда лицо не в состоянии выразить согласие по причине болезненного, бессознательного состояния и т.п.), в гуманитарных целях (контроль эпидемий и их распространения и т.п.) или в чрезвычайных ситуациях гуманитарного характера (техногенные или природные катастрофы, стихийное бедствие и т.п.), в иных исключительных ситуациях.

Для его применения необходимо одновременное соблюдение двух условий:

обработка персональных данных необходима для целей защиты жизни, здоровья или иных жизненно важных интересов либо самого субъекта персональных данных, либо иных лиц;

получение согласия субъекта персональных данных на обработку персональных данных невозможно.

Примеры.

1. Субъект персональных данных поступает в тяжелом состоянии в больницу и не может дать согласие на обработку персональных данных. Работники больницы в целях защиты его жизни вправе осуществить обработку его медицинских и иных данных.

2. Человеку требуется экстренная операция, для проведения которой необходимы отдельные сведения из медицинских документов его родителей.

Вместе с тем работники больницы по объективным причинам не могут связаться с ними и получить согласие на обработку их персональных данных.

3. В подъезде жилого дома в целях обеспечения сохранности имущества по решению более половины собственников квартир установлена камера видеонаблюдения. Обработка персональных данных субъектов персональных данных, чье видеоизображение попало в объектив камеры, не может осуществляться на основании рассматриваемой нормы, поскольку собственники остальных квартир, которые не выражали согласия или не принимали участие в опросе, и другие субъекты персональных данных не лишены юридической возможности дать согласие на обработку их персональных данных.

В случаях когда возможность получения согласия субъекта персональных данных на обработку персональных данных имеется (как в последнем примере), абзац восемнадцатый ст. 6 Закона не может быть применен;

в отношении распространенных ранее персональных данных до момента заявления субъектом персональных данных требований о прекращении обработки распространенных персональных данных, а также об их удалении при отсутствии иных оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами.

Указанное основание является развитием положений абзаца седьмого ст. 1 Закона и применяется при обработке общедоступных персональных данных, которые ранее были распространены, вне зависимости от того, кто конкретно распространил персональные данные.

Важно учитывать, что рассматриваемое основание может быть применено только в отношении общедоступных персональных данных, которые ранее были распространены на законных основаниях (самим субъектом, с его согласия или в соответствии с требованиями законодательных актов), и не легитимирует обработку персональных данных, распространенных в результате совершения преступления или иного правонарушения. При этом оценка законности распространения общедоступных персональных данных с учетом риск-ориентированного подхода является обязанностью оператора, применяющего данное правовое основание для обработки. При наличии сомнений оператор может принимать дополнительные меры для уточнения факта законности распространения персональных данных.

Если субъект персональных данных заявил требование о прекращении обработки распространенных персональных данных, а также об их удалении, их обработка должна быть прекращена, если у оператора не имеется иных оснований для обработки персональных данных, предусмотренных Законом или иными законодательными актами.

Заявление о прекращении обработки распространенных персональных данных должно быть подано оператору в порядке, установленном ст. 14 Закона;

в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами.

Обработку персональных данных по данному основанию могут осуществлять как государственные органы для выполнения своих задач и функций, так и иные организации при выполнении возложенных на них обязанностей (полномочий).

Пример.

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

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

Пример.

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

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

Рассматриваемое основание как основание более общего порядка применяется при отсутствии конкретизирующего его основания в данной

статье. В этой связи, если обработка персональных данных подпадает под иное основание, предусмотренное комментируемой статьей применительно к конкретной сфере деятельности, то оно не применяется;

в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка персональных данных без согласия субъекта персональных данных.

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

Примерами таких законодательных актов являются:

Закон Республики Беларусь от 28 октября 2008 г. № 433-З ”Об основах административных процедур“, п. 2 ст. 20 которого предусматривает, что сбор, обработка, хранение, использование персональных данных граждан при осуществлении административных процедур осуществляются без их письменного согласия с соблюдением требований, определенных законодательными актами, по защите информации, распространение и (или) предоставление которой ограничено;

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

В ряде случаях подобные нормы уточняют перечень персональных данных, круг органов, которые должны их предоставлять, конкретные способы запроса информации, сроки (периодичность) предоставления запрашиваемых данных, закрепляют безвозмездный характер получения данных и т.п.

Так, п. 7 Указа Президента Республики Беларусь от 16 декабря 2019 г.№ 460 ”Об общегосударственной автоматизированной информационной системе“ предусматривает, что владельцы (операторы) государственных информационных ресурсов (систем) обязаны предоставлять оператору ОАИС на безвозмездной основе информацию, содержащуюся в таких информационных ресурсах (системах), в том числе персональные данные без согласия физических лиц, сведения, содержащие коммерческую, профессиональную, банковскую и иную охраняемую законом тайну, которая необходима для эффективного оказания электронных услуг, осуществления административных процедур в электронной форме, а также обеспечения создания и функционирования личных электронных кабинетов на базе единого портала электронных услуг. При этом обработка персональных данных осуществляется без согласия физических лиц:

оператором ОАИС посредством ОАИС и иных информационных ресурсов (систем);

владельцами и (или) операторами государственных информационных ресурсов (систем) посредством ОАИС.

Статья 7. Обработка персональных данных по поручению оператора

Комментарий к статье 7

1. Комментируемая статья регулирует статус уполномоченного лица, осуществляющего обработку персональных данных по поручению оператора.

Такое лицо, равно как и оператор, обязано соблюдать требования к обработке персональных данных, предусмотренные Законом и иными актами законодательства.

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

Если уполномоченное лицо полагает, что поручения оператора по обработке персональных данных не соответствуют требованиям законодательства, оно должно незамедлительно уведомить об этом оператора.

2. Исходя из определения уполномоченного лица, содержащегося в абзаце шестнадцатом ст. 1 Закона, взаимоотношения оператора и уполномоченного лица могут опосредоваться:

актом законодательства.

Пример.

В соответствии с постановлением Министерства образования Республики Беларусь от 16 апреля 2019 г. № 36 "О порядке формирования и ведения единой базы данных обучающихся в учреждениях образования Республики Беларусь" база данных обучающихся является государственным информационным ресурсом, владельцем которого является Министерство образования, а оператором – учреждение "Главный информационно-аналитический центр Министерства образования Республики Беларусь";

решением государственного органа, являющегося оператором.

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

договором между оператором и уполномоченным лицом.

Это могут быть самостоятельный договор или отдельные положения в заключенном для достижения какой-либо цели договоре, так как обычно обработка персональных данных является

сопутствующей деятельностью по отношению к предмету взаимоотношений оператора и уполномоченного лица.

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

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

цели обработки персональных данных;

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

обязанности по соблюдению конфиденциальности персональных данных;

меры по обеспечению защиты персональных данных в соответствии со ст. 17 Закона.

В случае если решение государственного органа, являющегося оператором, о поручении обработки персональных данных подчиненным (входящим в состав) государственным органам (организациям) дополнительно опосредуется заключением договора, то требования, предусмотренные п. 1 ст. 7 Закона, достаточно предусмотреть в данном договоре.

Цели обработки персональных данных уполномоченным лицом должны соответствовать целям, заявленным в документе, определяющем политику оператора в отношении обработки персональных данных, и не должны быть абстрактными или общими.

При определении перечня действий, которые будут совершаться с персональными данными, целесообразно указать конкретные действия, совершаемые с персональными данными (например, сбор персональных данных для заключения договора с определением перечня необходимых персональных данных; внесение сведений в информационный ресурс; хранение персональных данных с указанием сроков и условий хранения; их актуализация путем сопоставления с дополнительной информацией и т.п.).

В договоре также целесообразно предусмотреть:

условия о возможности привлечения уполномоченным лицом иных лиц для обработки персональных данных или о запрете таких действий;

механизм участия уполномоченного лица в выполнении оператором обязанностей перед субъектами персональных данных;

обязанность уполномоченного лица прекратить по окончании договора обработку соответствующих персональных данных и передать такие данные оператору либо удалить (блокировать) их. При этом в силу требований абзаца седьмого п. 1 ст. 16 Закона такая обязанность должна

распространяться в том числе на случаи, когда уполномоченное лицо находится за пределами Республики Беларусь[18].

3. Пунктом 2 комментируемой статьи закрепляется, что уполномоченное лицо не обязано получать согласие субъекта персональных данных. Если для обработки персональных данных по поручению оператора необходимо получение согласия субъекта персональных данных, такое согласие получает оператор.

Такой подход обусловлен тем, что именно оператор принимает решение об обработке персональных данных и определяет ключевые параметры их обработки. Исходя из этого, оператор должен определить основание для обработки персональных данных и обеспечить его наличие. Соответствующие обязанности оператора закреплены в ст. 16 Закона.

Вместе с тем отсутствие у уполномоченного лица обязанности получать согласие субъекта персональных данных не исключает возможности его получения уполномоченным лицом по поручению оператора.

4. Пункт 3 комментируемой статьи устанавливает распределение ответственности между оператором и уполномоченным лицом.

Закон в равной степени возлагает на операторов и уполномоченных лиц ответственность за непринятие правовых, организационных и 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.

Таким образом, независимо от статуса (оператор или уполномоченное лицо) такие лица, в случае совершения ими действий, не соответствующих законодательству, будут нести предусмотренную законодательными актами ответственность, в частности, по ст. 23.7 КоАП.

Вместе с тем, поскольку ключевые параметры обработки персональных данных определяет оператор, именно он обязан обеспечивать права субъектов персональных данных и несет ответственность перед субъектом персональных данных как за свои действия, так и за действия уполномоченного лица в случае, если поручает обработку персональных данных уполномоченному лицу.

---

[18] Подробнее см. стандартные положения для включения в договор между оператором и уполномоченным лицом согласно приложению к Рекомендациям о взаимоотношениях операторов и уполномоченных лиц при обработке персональных данных, размещенным на официальном интернет-сайте Центра.

Если субъекту персональных данных причинен вред, в том числе моральный, действиями оператора или уполномоченного лица, то исходя из комментируемой нормы, этот субъект должен обратиться с иском к оператору. Оператор, в свою очередь, будет требовать привлечения уполномоченного лица к ответственности за нарушение условий договора.

В этой связи операторам следует тщательно подходить к выбору уполномоченного лица и привлекать к обработке персональных данных только тех уполномоченных лиц, которые предоставляют достаточные гарантии принятия ими соответствующих правовых, организационных и технических мер для обеспечения обработки персональных данных в соответствии с требованиями Закона.

Статья 8. Обработка специальных персональных данных

Комментарий к статье 8

1. В комментируемой статье закрепляются основания для обработки специальных персональных данных. Перечень этих оснований отличается от перечня оснований для обработки ”обычных“ персональных данных. Для обработки специальных персональных данных предусматривается меньшее количество оснований, что выглядит логичным с учетом более ”чувствительного“ характера этих данных для субъекта.

Для большей наглядности ниже сопоставлены в табличном виде ключевые основания для обработки персональных данных, предусмотренные в ст.ст. 6 и 8 Закона.

Основания обработки по ст. 6	**Основания обработки по ст. 8**
согласие	согласие
при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности	при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности
получение персональных данных на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором	
в научных или иных исследовательских целях при условии обязательного обезличивания персональных данных	

Основания обработки по ст. 6	Основания обработки по ст. 8
при обработке персональных данных, когда они указаны в документе, адресованном оператору и подписанном субъектом персональных данных, в соответствии с содержанием такого документа	
для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно	для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно
в отношении распространенных ранее персональных данных	если специальные персональные данные сделаны общедоступными персональными данными самим субъектом персональных данных
обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами	обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами

Сравнительный анализ указанных оснований показывает, что законодатель ограничивает основания для использования специальных персональных данных в гражданском обороте. По сути, они могут использоваться либо на основании согласия, либо в силу требований законодательства (обработка в связи с трудовой деятельностью также осуществляется в случаях, определенных законодательством). Такой подход направлен на предоставление субъекту персональных данных большего контроля за обработкой информации о нем.

По общему правилу, обработка специальных персональных данных без согласия субъекта персональных данных запрещается. Закон не предусматривает особых требований к согласию на обработку специальных персональных данных по сравнению с ”обычными“ данными.

Справочно:

Для сравнения: в Российской Федерации требуется письменная форма согласия на обработку специальных персональных данных, в рамках GDPR обработка особых категорий персональных данных допускается, если субъект дал прямое согласие на их обработку (подп. а п. 2 ст. 9 GDPR).

В этой связи согласие может быть получено в любой форме согласно ст. 5 Закона. Тем не менее, использование оператором именно письменной формы согласия может рассматриваться как один из элементов реализации оператором в рамках п. 3 ст. 8 Закона комплекса

мер по предупреждению рисков, которые могут возникнуть при обработке специальных персональных данных.

Правило о допустимости обработки специальных персональных данных на основании согласия не является абсолютным. Исключения из этого правила предусмотрены в п. 2 комментируемой статьи.

Некоторые из таких оснований-исключений повторяют основания ст. 6, другие несколько отличаются по своим формулировкам. Имеют место также случаи, когда основание включено в ст. 8, но отсутствует в ст. 6. Последние ситуации можно объяснить тем, что в первоначальных версиях законопроекта перечень оснований обработки специальных персональных данных носил закрытый характер и, соответственно, возможность их обработки для выполнения обязанностей (полномочий), предусмотренных законодательными актами, не допускалась. В этой связи заинтересованные органы стремились максимально указать все возможные основания в ст. 8, что после закрепления отсылочной нормы о возможности обработки специальных персональных данных в соответствии с законодательными актами сделало содержание такой статьи в определенной степени дублирующим.

Справочно:

Так, например, ст. 6 Закона не предусмотрено такое основание как осуществление административных процедур. Это обусловлено наличием специальной нормы в п. 2 ст. 20 Закона Республики Беларусь от 28 октября 2008 г. № 433-З "Об основах административных процедур". В этой связи применительно к "обычным" персональным данным основанием обработки персональных данных будет выступать абзац двадцать первый ст. 6 Закона. В свою очередь, при наличии аналогичного основания в ст. 8 Закона обработка специальных персональных данных для целей осуществления административных процедур будет осуществляться по иному основанию (абзац тринадцатый п. 2 ст. 8 Закона).

2. Пункт 2 комментируемой статьи закрепляет перечень исключений из правила о необходимости получения согласия на обработку специальных персональных данных. Согласие субъекта персональных данных на такую обработку не требуется в следующих случаях:

если специальные персональные данные сделаны общедоступными персональными данными самим субъектом персональных данных.

В соответствии со ст. 1 Закон выделяется два вида общедоступных персональных данных:

распространенные самим субъектом персональных данных или с его согласия;

распространенные в соответствии с требованиями законодательных актов.

С учетом изложенного, если специальные персональные данные распространяются самим субъектом персональных данных, то правовым

основанием обработки будет выступать абзац второй рассматриваемого пункта комментируемой статьи. Если же специальные персональные данные распространяются в соответствии с требованиями законодательных актов, то они будут обрабатываться в соответствии с абзацем семнадцатым названного пункта (обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами).

Примерами самостоятельного распространения специальных персональных данных может быть размещение информации о состоянии здоровья, политических позициях (взглядах), участии в деятельности профсоюзов, национальной принадлежности на странице в социальной сети и др. Важно отметить, что если субъектом персональных данных не были сделаны соответствующие настройки приватности и доступ к личной информации разрешен для неограниченного круга лиц, то, по общему правилу, презюмируется, что субъект сделал такие данные общедоступными;

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

Такое основание по своему содержанию во многом аналогично основанию, предусмотренному в ст. 6 *(см. подробнее комментарий к указанной статье)*.

Обработка специальных персональных данных при оформлении трудовых (служебных) отношений должна основываться на положениях актов законодательства. Например, форма личного листка по учету кадров, утвержденная постановлением Комитета по архивам и делопроизводству при Совете Министров Республики Беларусь от 26 марта 2004 г. № 2, предусматривает указание информации об участии работника в деятельности профсоюзов.

Тем не менее, на практике нередко встречаются довольно широкие трактовки рассматриваемого основания, которые не соответствуют требованиям Закона.

Так, например, все чаще имеют место ситуации, когда наниматели пытаются использовать данное основание для оправдания применения биометрической идентификации работников в целях контроля своевременности прихода на работу и ухода с работы. Подобный подход, хотя и может быть оправдан в отдельных ситуациях (в связи с работой на особо опасных объектах и др.), в большинстве случаев не соответствует требованию соразмерности и создает дополнительные риски для прав субъектов персональных данных;

в целях назначения и выплаты пенсий, ежемесячного денежного содержания отдельным категориям государственных служащих.

Данное основание отсутствовало в первоначально принятом варианте Закона и появилось после принятия Закона ”О государственной службе“. С учетом открытого круга оснований для обработки специальных персональных данных в ст. 8 его включение, как и ряд иных положений Закона, обеспечивающих конкретизацию уже имеющихся правовых оснований, обусловлено желанием упростить правоприменение, а не наличием правового пробела.

Назначение и выплата пенсий требуют обработки широкого круга персональных данных, в том числе в ряде случаев специальных персональных данных, например, сведений о состоянии здоровья при назначении пенсии по инвалидности.

Обработка специальных персональных данных осуществляется и при назначении ежемесячного содержания отдельным категориям государственных служащих. Так, например, ежемесячное денежное содержание не назначается (не выплачивается) лицам, совершившим в период прохождения государственной службы тяжкое или особо тяжкое преступление против интересов службы либо тяжкое или особо тяжкое преступление, сопряженное с использованием должностным лицом своих служебных полномочий. В этой связи требуется обработка информации о привлечении к уголовной ответственности лиц, претендующих на назначение ежемесячного денежного содержания;

при обработке общественными объединениями, политическими партиями, профессиональными союзами, религиозными организациями персональных данных их учредителей (членов) для достижения уставных целей при условии, что эти данные не подлежат распространению без согласия субъекта персональных данных.

Наличие этого основания связано с отнесением к специальным персональным данным информации, касающейся политических взглядов, членства в профессиональных союзах, религиозных или других убеждений. Рассматриваемое основание дает возможность обработки специальных персональных данных для достижения уставных целей соответствующих организаций (для ведения списков членов, учета уплаты взносов, если они предусмотрены, информирования о проводимых мероприятиях и др.). Тем не менее, оно не может выступать юридической основой для распространения персональных данных, например, посредством размещения их в сети Интернет.

Это основание также не подходит для обработки персональных данных в целях регистрации общественных организаций или представления списков таких членов контролирующим органам, когда это предусмотрено законодательством. Например, согласно Закону Республики Беларусь от 5 октября 1994 г. № 3266-XII ”О политических партиях“ политическая партия, союз ежегодно до 1 марта представляют

в Министерство юстиции списки членов выборных органов политической партии, союза, в которых указаны фамилия, собственное имя, отчество, дата рождения, гражданство, место жительства и номер домашнего телефона, место работы (учебы) и номер рабочего телефона, должность в этих выборных органах и дата избрания каждого из членов с приложением соответствующих протоколов. В этом случае правовым основанием для обработки соответствующих персональных данных будет абзац семнадцатый п. 2 ст. 8 Закона;

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.

Согласно абзацу двадцать девятому ч. 1 ст. 1 Закона ”О здравоохранении“ работниками здравоохранения признаются лица, занимающие в установленном законодательством порядке должности медицинских, фармацевтических работников, а также иные лица, работающие в области здравоохранения.

Действующее законодательство и практика его применения исходит из того, что к иным лицам, работающим в области здравоохранения, следует относить не только непосредственно медицинский персонал, но и иных лиц (бухгалтер, юрисконсульт и др.), получивших доступ к медицинским данным в связи с необходимостью организации процесса оказания медицинской помощи.

Организация оказания медицинской помощи не ограничивается лишь действиями по получению анализов, постановке диагноза, назначению лечения и др. В этой связи, например, обработка специальных персональных данных пациентов при оформлении актов выполненных работ, заполнении иных документов, связанных с медицинской помощью, относится к организации ее оказания и будет подпадать под рассматриваемое исключение.

Правильное понимание данного основания невозможно также без учета положений законодательства о здравоохранении, поскольку согласно п. 3 ст. 3 Закона в случае, если законодательным актом, устанавливающим правовой режим охраняемой законом тайны, предусматриваются особенности обработки персональных данных, входящих в состав охраняемой законом тайны, применяются положения этого законодательного акта.

Так, в частности, в соответствии с ч. 13 ст. 44 Закона ”О здравоохранении“ при формировании электронной медицинской карты пациента, информационных систем, информационных ресурсов,

баз (банков) данных, реестров (регистров) в здравоохранении согласие, отзыв согласия на внесение и обработку персональных данных пациента или лиц, указанных в ч. 2 ст. 18 этого Закона, информации, составляющей врачебную тайну, отказ от их внесения и обработки оформляются на бумажном носителе или иным способом, не запрещенным законодательством, по формам и в порядке, устанавливаемым Министерством здравоохранения.

Названная бланкетная норма реализована в Инструкции о формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных, информации, составляющей врачебную тайну, отказа от их внесения и обработки и порядке информирования о праве на отказ от внесения информации, составляющей врачебную тайну, в централизованную информационную систему здравоохранения, утвержденной постановлением Министерства здравоохранения Республики Беларусь от 7 июня 2021 г. № 74, хотя тут и имеется определенное расхождение относительно категорий информационных ресурсов (систем).

Этой Инструкцией предусматривается, что:

перед внесением персональных данных, информации, составляющей врачебную тайну, в электронную медицинскую карту пациента, информационную систему должно быть получено письменное согласие пациента или лиц, указанных в ч. 2 ст. 18 Закона ”О здравоохранении“, на внесение и обработку персональных данных пациента, информации, составляющей врачебную тайну;

согласие дается однократно при первичном посещении государственной организации здравоохранения;

отказ пациента или лиц, указанных в ч. 2 ст. 18 Закона ”О здравоохранении“, от внесения и обработки персональных данных пациента, информации, составляющей врачебную тайну, при формировании электронной медицинской карты пациента, информационной системы, оформляется по форме согласно приложению к постановлению, которым утверждена Инструкция;

владелец (оператор) информационной системы с момента оформления отказа от внесения и обработки персональных данных пациента, информации, составляющей врачебную тайну, вправе продолжить хранение и обработку обезличенных данных (информации) пациента в порядке, установленном законодательными актами.

С учетом изложенного можно сделать следующие выводы:

при оказании медицинской помощи (внесении информации в бумажную карточку в соответствии с установленной формой, проведении анализов, постановке диагноза и др.), а также при иных действиях, связанных с организацией оказания медицинской помощи

(заключении и исполнении договоров оказания медицинских услуг, оформлении актов выполненных работ, заполнении иных документов и др.), получение согласия не требуется;

при формировании электронной медицинской карты пациента, внесении персональных данных в информационные системы, информационные ресурсы, базы (банки) данных, реестры (регистры) в системе здравоохранения требуется получение согласия. При этом, если указанные действия осуществлялись до вступления в силу ч. 13 ст. 44 Закона "О здравоохранении" и пациент не требует прекращения обработки его данных о состоянии здоровья в соответствующих ресурсах, такая обработка может продолжаться;

если пациент не дает согласия на внесение персональных данных в электронную медицинскую карту пациента, информационную систему и др., то обработка его персональных данных должна вестись на бумажных носителях;

отказ в оказании медицинской помощи в связи с отказом в даче указанного согласия не допускается;

для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов, совершения исполнительной надписи, оформления наследственных прав.

Данное основание фактически является объединением двух самостоятельных оснований, предусмотренных в абзацах третьем и девятом ст. 6 Закона (*см. комментарий к ст. 6 Закона*). При этом в отношении обработки специальных персональных данных в сфере нотариальной деятельности указывается лишь на совершение исполнительной надписи и оформление наследственных прав.

Следует также учитывать, что рассматриваемое основание является частным случаем обработки, предусмотренной абзацем семнадцатым комментируемого пункта, и его появление обусловлено традиционным обособлением сферы правосудия и связанных с ней сфер в нормативных правовых актах;

для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности.

Данное основание аналогично основанию, предусмотренному абзацем вторым ст. 6 (*см. комментарий к ст. 6*);

в случаях, предусмотренных уголовно-исполнительным законодательством, законодательством в области национальной безопасности, об обороне, о борьбе с коррупцией, о борьбе с терроризмом и противодействии экстремизму, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения, о Государственной границе Республики

Беларусь, о гражданстве, о порядке выезда из Республики Беларусь и въезда в Республику Беларусь, о статусе беженца, дополнительной защите, убежище и временной защите в Республике Беларусь.

Основания, указанные в абзаце девятом рассматриваемого пункта, предусматривают широкий круг случаев, когда обработка специальных персональных данных осуществляется в связи с реализацией государственными органами (организациями) публично значимых функций.

В ряде законодательных актов предусматривается конкретный набор обрабатываемых персональных данных (например, круг сведений, подлежащих установлению при идентификации физических лиц, осуществляющих финансовые операции), в то время как в других – круг таких данных определяется в каждом конкретном случае.

Как и во многих других ситуациях, обработка специальных персональных данных, как правило, сопровождается обработкой ”обычных“ данных. В этой связи юридическое основание для обработки всего объема персональных данных будет представлять собой совокупность норм как предусмотренных в ст. 6, так и включенных в ст. 8 Закона.

Следует также отметить предусмотренные Законом применительно ко многим из сфер, перечисленных в рассматриваемом абзаце, изъятия из права на получение информации, касающейся обработки персональных данных, и права на получение информации о предоставлении персональных данных третьим лицам;

в целях обеспечения функционирования единой государственной системы регистрации и учета правонарушений.

Закон ”О единой государственной системе регистрации и учета правонарушений“ предусматривает порядок регистрации правонарушений органами уголовного преследования, органами, ведущими административный процесс, и судами, а также порядок учета правонарушений и предоставления сведений о правонарушениях органами внутренних дел. В единый государственный банк данных о правонарушениях включаются сведения о совершенных преступлениях и иных правонарушениях, которые относятся к категории специальных персональных данных.

В соответствии со ст. 7 Закона ”О единой государственной системе регистрации и учета правонарушений“ государственные органы и иные государственные организации в целях функционирования единой государственной системы регистрации и учета правонарушений обеспечивают контроль за деятельностью органов уголовного преследования и органов, ведущих административный процесс, по регистрации правонарушений, передаче ими сведений

о правонарушениях в органы внутренних дел, а также по сохранности и защите сведений о правонарушениях.

Таким образом, указанное основание применимо как непосредственно органами внутренних дел, которые ведут единый государственный банк данных о правонарушениях, так и теми органами (организациями), которые в соответствии с названным Законом вносят соответствующие сведения в указанный банк данных;

в целях ведения криминалистических учетов.

В соответствии со ст. 45 Закона Республики Беларусь от 18 декабря 2019 г. № 281-З ”О судебно-экспертной деятельности“ криминалистические учеты – это массивы (базы, банки) данных, содержащие в обобщенном, систематизированном виде объекты (их копии, изображения, информацию о них), в том числе судебных экспертиз, используемые для выполнения судами, органами уголовного преследования, органами, ведущими административный процесс, а также органами, обеспечивающими национальную безопасность Республики Беларусь, возложенных на них задач.

Криминалистические учеты могут содержать различную информацию, в том числе и специальные персональные данные (данные о состоянии здоровья, биометрические персональные данные и др.), которые будут использоваться в процессе экспертиз в рамках уголовного, гражданского процессов и др.

Можно отметить, что ст. 45 Закона Республики Беларусь ”О судебно-экспертной деятельности“ предусматривает, что криминалистические учеты могут содержать персональные данные, обработка которых в целях ведения криминалистических учетов осуществляется без согласия физических лиц. В этой связи, принимая во внимание положения абзаца восемнадцатого комментируемого пункта (когда законодательными актами прямо предусмотрена обработка специальных персональных данных без согласия лица), включение соответствующего основания в качестве самостоятельного является в определенной степени излишним;

для организации и проведения государственных статистических наблюдений, формирования официальной статистической информации.

Данное основание аналогично основанию, предусмотренному в ст. 6. Закона *(подробнее см. комментарий к абзацу двенадцатому ст. 6 Закона)*;

для осуществления административных процедур.

Перечни документов и сведений, которые представляются для осуществления административных процедур в отношении граждан, утверждены Указом Президента Республики Беларусь от 26 апреля 2010 г. № 200 ”Об административных процедурах, осуществляемых

государственными органами и иными организациями по заявлениям граждан“ и могут содержать в том числе и специальные персональные данные. Например, заключение врачебно-консультационной комиссии государственной организации здравоохранения о наличии заболеваний, при которых граждане не могут пользоваться лифтом (подп. 1.11^1 п. 1 перечня административных процедур, осуществляемых государственными органами и иными организациями по заявлениям граждан, утвержденного данным Указом).

Кроме того, специальные персональные данные также могут содержаться в документах и сведениях, запрашиваемых организациями при осуществлении административных процедур.

Примером могут быть сведения о наличии не снятой или не погашенной в установленном порядке судимости за совершение умышленных тяжких или особо тяжких преступлений против человека (п. 51 перечня документов и (или) сведений, самостоятельно запрашиваемых местными исполнительными и распорядительными органами при осуществлении административных процедур по заявлениям граждан, утвержденного постановлением Совета Министров Республики Беларусь от 18 сентября 2020 г. № 541 ”О документах, запрашиваемых при осуществлении административных процедур“);

в связи с реализацией международных договоров Республики Беларусь о реадмиссии.

Реадмиссия представляет собой передачу компетентными органами государства запрашивающей Стороны и прием компетентными органами государства запрашиваемой Стороны в порядке, на условиях и в целях, предусмотренных соответствующим Соглашением, лиц, въехавших или находящихся на территории государства запрашивающей Стороны в нарушение законодательства этого государства по вопросам въезда, выезда и пребывания иностранных граждан и лиц без гражданства.

На сегодняшний день Беларусь имеет действующие соглашения о реадмиссии с рядом государств (Украина, Армения, Российская Федерация, Турция, Казахстан, Грузия).

В подобных соглашениях предусматривается, что компетентный орган государства запрашиваемой Стороны принимает по запросу компетентного органа государства запрашивающей Стороны лиц, которые въехали или находятся на территории государства запрашивающей Стороны с нарушением законодательства этого государства по вопросам въезда, выезда и пребывания иностранных граждан и лиц без гражданства, если установлено, что они являются гражданами государства запрашиваемой Стороны либо утратили его гражданство после въезда на территорию государства

запрашивающей Стороны и не приобрели гражданство другого государства.

Для реализации таких соглашений устанавливаются перечни документов, на основании которых подтверждается или может предполагаться наличие гражданства у соответствующего лица. В этих документах могут содержаться в том числе и специальные персональные данные, например, биометрические данные в документе, удостоверяющем личность;

для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Данное основание аналогично основанию, предусмотренному в ст. 6 Закона *(см. подробнее комментарий к абзацу восемнадцатому ст. 6 Закона)*;

в случаях, когда обработка специальных персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами.

Данное основание появилось в законопроекте на последних стадиях и его включение в значительной степени ”ослабило“ ограничительный характер предписаний об основаниях обработки специальных персональных данных, а также в значительной степени нивелировало различия в правовом режиме ”обычных“ и специальных персональных данных.

Справочно:

Для сравнения в Российской Федерации обработка специальных персональных данных без согласия лица допускается по основаниям, исчерпывающим образом предусмотренным в ст. 10 Федерального закона от 27 июля 2006 г. № 152-ФЗ ”О персональных данных“.

Подобное решение отечественного законодателя отчасти можно объяснить новизной регулируемого института и опасениями ”потерять“ определенные процессы, требующие использования специальных персональных данных, что, как следствие, может создать неоправданные препятствия для выполнения различными органами своих функций. Следует признать, что подобные опасения небеспочвенны. В той же Российской Федерации перечень оснований для обработки специальных персональных данных за время, прошедшее с момента первоначального принятия закона, увеличился вдвое.

В целом, обработка специальных персональных данных для выполнения обязанностей (полномочий), предусмотренных законодательными актами, – довольно распространенная ситуация. В ряде законодательных актов прямо предусматривается необходимость обработки определенных специальных персональных данных.

Так, например, ст. 27[1] Закона Республики Беларусь от 19 ноября 1993 г. № 2570-XII ”О правах ребенка“ предусматривает, что не имеют права заниматься педагогической деятельностью, педагогической деятельностью в сфере физической культуры и спорта, занимать должности служащих, связанные с выполнением воспитательных функций, другие должности служащих, профессии рабочих, связанные с постоянной работой с детьми, физические лица, в отношении которых вступил в законную силу обвинительный приговор суда за совершение преступлений, предусмотренных ст.ст. 139, 145–147, 154, ч.ч. 2 и 3 ст. 165, главой 20, ст. 172, ч. 2 ст. 173, ст.ст. 181, 182, 187, 342[1], 343 и 343[1] УК, вне зависимости от снятия или погашения судимости либо прекращено уголовное преследование за совершение указанных преступлений по основаниям, предусмотренным п. 3 или 4 ч. 1 ст. 29 УПК.

Схожим образом согласно Закону ”О государственной службе“ гражданин не может быть принят на гражданскую службу в случае наличия не погашенной или не снятой в установленном порядке судимости, если иное не установлено законодательными актами, закрепляющими правовой статус отдельных категорий гражданских служащих.

В таких ситуациях запрос и получение соответствующих сведений при приеме лица на работу не требует получения согласия гражданина и основывается на положениях рассматриваемого абзаца.

В других ситуациях возможность обработки специальных персональных данных без согласия лица в законодательном акте прямо не оговаривается, но может вытекать из обязанностей (полномочий), предусматриваемых таким актом.

Такая ситуация возникает, например, при поступлении в организацию обращения, содержащего специальные персональные данные. Закон Республики Беларусь от 18 июля 2011 г. № 300-З ”Об обращениях граждан и юридических лиц“ возлагает на организации обязанность принимать меры для полного, объективного, всестороннего и своевременного рассмотрения обращений. В этой ситуации организация, получившая такое обращение, в процессе его рассмотрения обрабатывает такие данные, в том числе хранит их, для выполнения обязанностей, предусмотренных Законом ”Об обращениях граждан и юридических лиц“ и принятыми в его развитие иными актами законодательства;

в случаях, когда Законом и иными законодательными актами прямо предусматривается обработка специальных персональных данных без согласия субъекта персональных данных.

Это основание является частным случаем предыдущего основания с той разницей, что в законодательном акте прямо предусматривается возможность обработки специальных персональных данных без согласия гражданина.

Как пример, можно указать Закон ”О единой государственной системе регистрации и учета правонарушений“, предусматривающий в ст. 12, кому и для каких целей предоставляются без согласия физических сведения о совершенных ими правонарушениях.

3. Согласно п. 3 комментируемой статьи обработка специальных персональных данных допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке таких персональных данных для прав и свобод субъектов персональных данных.

Специальные персональные данные представляют собой весьма ”чувствительную“ категорию для граждан, и обработка таких данных потенциально несет повышенный риск для них, что обуславливает необходимость принятия усиленных мер защиты.

Меры по предупреждению рисков для прав субъектов персональных данных определяет оператор с учетом конкретных обстоятельств обработки. К таким мерам, в частности, могут быть отнесены:

при обработке персональных данных на основании согласия – получение согласия в письменной форме, что повысит уверенность в том, что данные предоставлены самим субъектом;

предоставление доступа к таким данным ограниченному кругу лиц;

минимизация сроков хранения специальных персональных данных;

применение методов обезличивания при обработке специальных персональных данных;

исключение практики трансграничной передачи таких данных, передачи данных уполномоченным лицам и др.

Статья 9. Трансграничная передача персональных данных

Комментарий к статье 9

О понятии трансграничной передачи см. подробнее комментарий к ст. 1 Закона.

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

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

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

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

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

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

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

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

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

Для ”легитимации“ согласия как основания для трансграничной передачи необходимо одновременное выполнение двух условий:

соответствие такого согласия требованиям ст. 5 Закона;

дополнительное информирование субъекта о рисках, возникающих в связи с отсутствием надлежащего уровня защиты персональных данных в стране, куда такие данные передаются.

Практическая реализация данного требования предполагает либо получение отдельного согласия на трансграничную передачу, либо добавление соответствующей информации в общее согласие, получаемое в соответствии со ст. 5 Закона.

Что касается возможных рисков, то они определяются оператором применительно к конкретной стране и условиям передачи. Среди потенциальных рисков могут быть названы отсутствие (ограниченность) законодательства о персональных данных, фактическая неприменяемость такого законодательства на практике, отсутствие уполномоченного органа по защите прав субъектов персональных данных, отсутствие или ограниченность прав субъектов персональных данных, неопределенность оснований для обработки персональных данных, возможность широкого доступа к таким данным органов безопасности, отсутствие мер ответственности за нарушения в сфере обработки персональных данных, отсутствие обязательных требований о технической и криптографической защите информационных систем (ресурсов), содержащих персональные данные, и др.;

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

В данном случае передача данных должна вытекать из предмета договора, например, когда заключен договор на организацию отдыха с туристическим агентством и в рамках реализации такого договора оно передает данные клиента в зарубежный отель для бронирования. В этой ситуации дополнительного указания (закрепления) в договоре на возможность трансграничной передачи персональных данных не требуется.

При этом сама передача данных может быть опосредована договорными отношениями между организациями (в нашем случае между туристическим агентством и отелем), в рамках которых определяются в том числе объем и формат передаваемых данных.

Трансграничная передача персональных данных только на основании договора между юридическими лицами при отсутствии договора с субъектом персональных данных, в рамках которого требуется передать соответствующие данные, не будет согласовываться с требованиями Закона;

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

Причина появления данного изъятия обусловлена тем, что государством по различным причинам признается нецелесообразным ”закрывать“ определенные данные. Если они могут стать доступны

любому лицу (в ряде случаев за плату), то теряют смысл и любые ограничения для трансграничной передачи персональных данных.

В качестве примера можно привести ситуации с доступом к персональным данным, содержащимся в ряде государственных информационных ресурсов (единый государственный регистр юридических лиц и индивидуальных предпринимателей и др.);

такая передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Рассматриваемое основание по своему содержанию аналогично положениям абзаца восемнадцатого ст. 6 Закона *(см. соответствующий комментарий)*;

обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь.

Данное исключение с учетом положений п. 4 ст. 3 Закона формально является излишним. Логику подобного "двойного" исключения можно объяснить широкой распространенностью трансграничной передачи персональных данных в рамках соответствующих договоров и желанием исключить возможные споры среди практических работников.

Для применения рассматриваемого основания не требуется, чтобы в международном договоре прямо указывалось на возможность именно трансграничной передачи данных. Достаточно, чтобы необходимость передачи данных вытекала из положений соответствующего договора. Так, например, в договоре может содержаться указание на перечень данных, которыми стороны обмениваются, органы, которые имеют право получать такие данные, и др.;

такая передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения в соответствии с законодательством.

Законом Республики Беларусь от 30 июня 2014 г. № 165-З "О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения" предусматриваются случаи взаимодействия с зарубежными и международными организациями, в том числе предусматривающие необходимость представления персональных данных участников финансовых операций.

Так, в частности, орган финансового мониторинга может представлять в компетентные органы иностранных государств по их запросу или по собственной инициативе соответствующую информацию (в том числе содержащую банковскую или иную охраняемую законом тайну) при условии, что ее представление не причиняет вреда национальной безопасности Республики Беларусь и эта информация не будет использована без предварительного согласия органа финансового мониторинга;

получено соответствующее разрешение Национального центра защиты персональных данных.

Порядок получения разрешения определен приказом директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 14 ”О трансграничной передаче персональных данных“ (далее – приказ № 14).

Анализ данного приказа позволяет выделить два вида разрешений на трансграничную передачу персональных данных:

индивидуальные разрешения, выдаваемые на основании заявления. Порядок выдачи таких разрешений определен в Положении о порядке выдачи разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, утвержденном названным приказом № 14.

Для получения индивидуального разрешения заявитель лично или через своих представителей подает в Национальный центр защиты персональных данных в письменном виде или в виде электронного документа заявление и прилагает к нему проект договора, которым оформляется трансграничная передача персональных данных, согласованный заявителем и получателем персональных данных, на дату, предшествующую дате подачи заявления, либо иной документ, в соответствии с которым предполагается осуществлять передачу персональных данных.

Заявитель может представить и иные документы, подтверждающие гарантии соблюдения прав субъектов персональных данных в иностранном государстве.

К заявлению, подаваемому представителем заявителя, прилагается документ, подтверждающий его полномочия (доверенность, решение суда, иные документы), – для письменного заявления, электронная копия документа, подтверждающего его полномочия, – для заявления, подаваемого в виде электронного документа.

Заявление рассматривается в течение тридцати дней со дня регистрации.

В ходе рассмотрения заявления и прилагаемых к нему документов изучается информация об уровне защиты прав субъектов персональных данных на территории иностранного государства.

Разрешение выдается при условии обеспечения защиты прав субъектов персональных данных на уровне не ниже, чем это предусмотрено законодательством Республики Беларусь.

Национальный центр защиты персональных данных отказывает в выдаче разрешения:

в случаях ликвидации (прекращения деятельности), смерти заявителя, получателя персональных данных;

если заявитель обрабатывает персональные данные в нарушение требований Закона;

если представленные заявителем документы и (или) сведения не позволяют сделать вывод о надлежащей защите прав субъектов персональных данных, в том числе, когда правовые, организационные и технические меры, принимаемые получателем персональных данных, не являются достаточными для обеспечения защиты прав субъектов персональных данных на уровне не ниже, чем это предусмотрено законодательством Республики Беларусь;

общие разрешения, предусмотренные подп. 1^1 п. 1 приказа № 14. Для использования данного типа разрешения не требуется подача заявления и рассмотрение конкретной, индивидуальной ситуации. Осуществлять трансграничную передачу персональных данных на этом основании может любой оператор (уполномоченное лицо), который подпадает под соответствующие критерии.

Согласно подп. 1^1 п. 1 приказа № 14 разрешается трансграничная передача персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных:

при размещении государственными органами, государственными организациями, а также хозяйственными обществами, в отношении которых Республика Беларусь либо административно-территориальная единица, обладая акциями (долями в уставных фондах), может определять решения, принимаемые этими хозяйственными обществами, информации о своей деятельности в глобальной компьютерной сети Интернет;

в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами.

ГЛАВА 3
ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ И ОБЯЗАННОСТИ ОПЕРАТОРА

Статья 10. Право на отзыв согласия субъекта персональных данных

Комментарий к статье 10

1. Отзыв согласия – одно из прав субъекта персональных данных, означающее прекращение права оператора обрабатывать персональные данные, если у него нет иных правовых оснований для обработки. Следовательно, при получении заявления об отзыве согласия следует проверить наличие иных оснований для обработки персональных данных, предусмотренных ст. 6 или п. 2 ст. 8 Закона. Бремя доказывания наличия таких оснований возлагается на самого оператора.

Отзыв согласия возможен только в том случае, если обработка персональных данных осуществлялась на основании согласия. Если обработка осуществлялась на иных правовых основаниях, но при этом имели место нарушения, то защита прав субъектов персональных данных осуществляется посредством реализации права на прекращение обработки персональных данных.

Законодатель не связывает отзыв согласия на обработку персональных данных с наличием каких-либо условий или наступлением определенных событий. В этой связи субъект персональных данных может в любой момент без объяснения причин отозвать данное им согласие.

При наличии нескольких целей обработки персональных данных на этапе получения согласия оператор должен предоставить субъекту возможность выразить согласие в отношении каждой из заявленных целей обработки (*см. комментарий к ст. 5 Закона*). Соответственно субъект может в любой момент отозвать свое согласие на обработку персональных данных в отношении одной или нескольких целей. При этом в отношении оставшихся целей такая обработка должна продолжаться.

Пунктом 1 ст. 10 Закона установлены способы подачи заявления об отзыве согласия:

в форме, посредством которой получено согласие. Так, если согласие получено посредством иной электронной формы, например, посредством указания субъектом кода, после получения СМС-сообщения, то оператор обязан обеспечить возможность отзыва согласия аналогичным способом;

в письменной форме либо в виде электронного документа в соответствии со ст. 14 Закона. В отличие от предыдущего, данный вариант является универсальным и не зависит от способа получения оператором согласия субъекта персональных данных.

2. В связи с отзывом согласия у оператора возникает корреспондирующая этому праву обязанность прекратить обработку персональных данных, осуществить их удаление (блокирование) и уведомить об этом субъекта, если отсутствуют иные основания для таких действий с персональными данными, предусмотренные Законом и иными законодательными актами.

Законодателем для реализации права на отзыв согласия предусмотрен пятнадцатидневный срок, в течение которого оператор должен проверить наличие иных оснований для обработки персональных данных, удостовериться в их отсутствии, прекратить обработку персональных данных, осуществить их удаление и уведомить об этом субъекта персональных данных.

При этом если обработка персональных данных осуществляется уполномоченным лицом, оператор должен обеспечить прекращение обработки персональных данных, а также их удаление уполномоченным лицом, что вытекает из положений ст. 16 Закона.

Стоит также учитывать, что при отсутствии технической возможности удаления персональных данных оператор обязан принять меры по недопущению дальнейшей обработки персональных данных, включая их блокирование, и уведомить об этом субъекта персональных данных в тот же срок *(о блокировании см. комментарий к ст. 1 Закона)*.

3. Согласно пункту 3 комментируемой статьи окончание действия договора, в соответствии с которым осуществлялась обработка персональных данных, или его расторжение влекут последствия, указанные в пункте 2 данной статьи, если иное не предусмотрено этим договором или актами законодательства.

Следует учитывать, что сам по себе факт окончания договора далеко не во всех случаях свидетельствует о необходимости прекращения обработки и удаления персональных данных. Необходимость обеспечения гарантийного и послегарантийного обслуживания, защиты прав одной из сторон при неисполнении другой стороной условий договора и другие предусмотренные законодательством случаи, обусловливают обработку персональных данных и после окончания срока такого договора.

Кроме того, распространенным исключением являются и случаи, когда хранение договора в пределах установленного срока вытекает из требований законодательства, в частности, постановления Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140

”О перечне типовых документов“. В этой связи, если хранение документов, содержащих персональные данные, обусловлено необходимостью соблюдения требований указанных нормативных правовых актов, прекращение обработки и удаление персональных данных не осуществляется. Правовым основанием для продолжения такой обработки будет выступать абзац двадцатый ст. 6 Закона.

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

При этом законодателем предусмотрено, что печатные издания, аудио- либо видеозаписи программ, радио-, телепрограммы, кинохроникальные программы, иная информационная продукция, содержащие персональные данные, выпущенные до момента отзыва согласия субъекта персональных данных, не подлежат изъятию из гражданского оборота. Таким образом, изымать и уничтожать уже напечатанные, опубликованные материалы не требуется.

Однако здесь необходимо учитывать такой аспект, что если согласие субъекта персональных данных дано на обработку его персональных данных, например, для изготовления рекламного буклета, брошюрок, календариков с использованием изображения субъекта персональных данных, то если изготовление такой продукции подразумевалось поэтапно, в несколько тиражей, часть из которых уже была изготовлена, то в случае отзыва согласия субъекта персональных данных на такую обработку, она должна быть прекращена в отношении еще не изготовленных тиражей.

Статья 11. Право на получение информации, касающейся обработки персональных данных, и изменение персональных данных

Комментарий к статье 11

1. Пункт 1 комментируемой статьи Закона закрепляет право на получение информации, касающейся обработки своих персональных данных. Наличие данного права является неотъемлемым условием эффективного контроля за соблюдением оператором законодательства о персональных данных и недопущением нарушения им прав и свобод субъекта персональных данных.

Перечень предоставляемой информации носит открытый характер и должен содержать:

наименование (фамилию, собственное имя, отчество (если таковое имеется)) и место нахождения (адрес места жительства (места пребывания)) оператора;

подтверждение факта обработки персональных данных оператором (уполномоченным лицом);

его персональные данные и источник их получения;

правовые основания и цели обработки персональных данных;

срок, на который дано согласие;

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

иную информацию, предусмотренную законодательством.

На практике возникают вопросы относительно объема персональных данных, который необходимо указать в ответе на заявление о получении информации. К таковым относятся как те персональные данные, которые предоставил непосредственно субъект персональных данных, так и данные, полученные оператором от иных лиц, из открытых источников или данные, созданные оператором (уполномоченным лицом) в процессе обработки.

По общему правилу, в ответе на заявление о получении информации, касающейся обработки персональных данных, необходимо указывать конкретные данные, а не их описание или обобщающие характеристики (например, ”данные о доходах“). Исключением являются случаи обработки оператором большого массива однотипных данных или технической невозможности указания всех обрабатываемых данных. В таких ситуациях допустимо обозначить общее описание отдельных категорий персональных данных.

Ответ на заявление о получении информации, касающейся обработки персональных данных, помимо определенного объема непосредственно персональных данных, должен содержать указание на правовое основание и цель обработки персональных данных.

Следует также учитывать особенность, связанную с обработкой персональных данных уполномоченными лицами. Если в политике в отношении обработки персональных данных допустимо указать категории уполномоченных лиц, то в ответе на заявление о получении информации необходимо указывать конкретных уполномоченных лиц, которым оператор поручил обработку персональных данных.

Отметим, что предоставляемая оператором информация должна касаться персональных данных только того субъекта, который обратился к нему с соответствующим заявлением, даже если обработка осуществляется на основании документа, содержащего персональные

данные нескольких субъектов (например, в случае договора со множественностью лиц на одной стороне).

В целом, информация должна быть предоставлена в доступной форме, то есть изложена понятным для лиц, не обладающих специальными познаниями в этой сфере, языком, исключающим использование сложных языковых конструкций, абстрактный или двусмысленный характер текста.

2. Пункт 2 комментируемой статьи Закона определяет условия реализации права на получение информации.

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

Необходимая информация предоставляется субъекту персональных данных бесплатно, при этом последний не должен обосновывать свой интерес к запрашиваемой информации.

Исключения, касающиеся сроков и необходимости платы за соответствующие запросы, могут быть предусмотрены законодательными актами.

Например, физическое лицо вправе получить справку (выписку) из регистра населения в отношении своих персональных данных бесплатно один раз в пределах календарного года, второй и последующий разы предоставление данных осуществляется на платной основе. Предоставление справки (выписки) из регистра осуществляется не позднее пяти календарных дней со дня подачи в регистрирующую службу соответствующего заявления, но этот срок может быть продлен до пятнадцати календарных дней (п. 7 ст. 26, п.п. 1 и 2 ст. 27 Закона ”О регистре населения“).

Выписка из единого государственного банка данных о правонарушениях предоставляется на платной основе физическому лицу (за исключением лица, являющегося потерпевшим по уголовному делу либо делу об административном правонарушении, в отношении сведений о правонарушениях по этим делам) в течение пятнадцати дней со дня подачи заявления (ч. 7 ст. 15 Закона ”О единой государственной системе регистрации и учета правонарушений“).

3. Пункт 3 комментируемой статьи Закона определяет перечень случаев, когда информация, касающаяся обработки своих персональных данных, не предоставляется.

В частности, такая информация не предоставляется, если персональные данные могут быть получены любым лицом посредством:

направления запроса в порядке, установленном законодательством. Такой порядок предусмотрен, например, для выписки из Единого

государственного регистра юридических лиц и индивидуальных предпринимателей (п. 19 постановления Совета Министров Республики Беларусь от 23 февраля 2009 г. № 229 ”О Едином государственном регистре юридических лиц и индивидуальных предпринимателей“);

доступа к информационному ресурсу (системе) в глобальной компьютерной сети Интернет (например, интернет-ресурсы, предлагающие услуги продажи тех или иных предметов частными лицами с указанием данных продавцов (имя, телефон)).

Ряд ограничений для получения информации, касающейся персональных данных, установлен с целью защиты публичных интересов (если обработка персональных данных осуществляется в соответствии с законодательством в области национальной безопасности, о борьбе с коррупцией, об оперативно-розыскной деятельности и т.д.) либо для исключения возложения на операторов чрезмерного бремени по администрированию связанных с подготовкой ответов процессов.

Перечень исключений не носит закрытого характера. В этой связи законодательными актами могут быть предусмотрены дополнительные исключения.

4. Пункт 4 комментируемой статьи Закона посвящен реализации права на изменение персональных данных.

Субъект персональных данных вправе обратиться к оператору с целью изменения своих персональных данных в случаях, когда оператор обрабатывает неполные, устаревшие или неточные данные. Нередко это может быть следствием получения информации в соответствии с п. 1 комментируемой статьи.

Как правило, субъект персональных данных реализует данное право, если у него отсутствует возможность изменить персональные данные самостоятельно (например, в личном кабинете пользователя на сайте) или когда точность таких данных имеет принципиальное значение для реализации прав и законных интересов субъекта.

Законодательством о персональных данных не предусмотрена общая обязанность субъекта персональных данных уведомлять об изменении его персональных данных оператора. Однако соответствующие обязанности могут быть закреплены законодательными актами, регулирующими отношения по отдельным вопросам.

Так, следует учитывать предусмотренную ч. 2 п. 2 ст. 18 ГК обязанность гражданина принимать необходимые меры для уведомления своих должников и кредиторов о перемене его имени и риск последствий, вызванных отсутствием у этих лиц сведений о перемене его имени.

Праву субъекта персональных данных корреспондирует обязанность оператора вносить изменения в персональные данные,

которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных.

Иной порядок предусмотрен, например, для внесения изменений, дополнений и исправлений в записи актов гражданского состояния. Порядок осуществления данной процедуры определен главой 10 Положения о порядке регистрации актов гражданского состояния и выдачи документов и (или) справок органами, регистрирующими акты гражданского состояния, утвержденного постановлением Совета Министров Республики Беларусь от 14 декабря 2005 г. № 1454.

В качестве примера обработки персональных данных, которая не предполагает последующих изменений таких данных, можно привести хранение документов. Так, законодательством в сфере архивного дела и делопроизводства не предусмотрено изменение части (частей) документов, образующихся в процессе деятельности государственных органов, иных организаций и подлежащих хранению в течение установленных сроков. В течение всего срока хранения документов должна обеспечиваться их подлинность (оригинальность и целостность) независимо от вида носителя и порядка хранения.

Для реализации комментируемого права субъект персональных данных подает оператору заявление с приложением документов и (или) их заверенных в установленном порядке копий, подтверждающих необходимость внесения изменений в персональные данные. Порядок подачи заявления определен в ст. 14 Закона.

Оператор обязан в течение 15 дней с момента получения заявления внести соответствующие изменения в обрабатываемые персональные данные. Невыполнение данной обязанности в установленный срок может повлечь ответственность в соответствии с ч. 1 ст. 23.7 КоАП.

О внесении изменений или о причинах отказа в совершении этих действий оператор должен уведомить субъекта персональных данных в пятнадцатидневный срок после получения соответствующего заявления.

Статья 12. Право на получение информации о предоставлении персональных данных третьим лицам

Комментарий к статье 12

1. Ежедневно различные организации как государственного, так и коммерческого сектора осуществляют обработку персональных данных граждан, предоставляют такие данные третьим лицам (наниматель предоставляет сведения в органы статистики, органы Фонда социальной защиты населения, военкоматы и др., торговые сети обрабатывают данные о наших покупках, в том числе с привлечением иных лиц, налоговые органы обрабатывают данные в рамках налогового контроля, различные организации используют данные из истории нашего браузера и др.). При этом мы видим (осознаем) лишь незначительную часть такой обработки, в то время как основной ее массив осуществляется без нашего ведома.

Отсутствие такой информации препятствует осуществлению субъектом персональных данных контроля за обработкой его данных, эффективной реализации предоставленных ему прав. В этой связи настоятельной необходимостью становится выработка механизма информирования субъекта о получении различными организациями доступа к сведениям о нем.

Справочно:

Согласно ст. 14 GDPR, если персональные данные получены не от субъекта данных, контролер должен предоставить субъекту данных следующую информацию:

наименование (имя) и контактные данные контролера и при необходимости его представителя;

контактные данные инспектора по защите персональных данных при необходимости;

цели обработки, для которой предназначаются персональные данные, а также правовое основание для обработки;

категории соответствующих персональных данных;

получатели или категории получателей персональных данных, если таковые имеются и др.

При этом из данного правила есть исключения, когда нет необходимости предоставлять субъекту соответствующую информацию (например, получение или раскрытие информации прямо установлено правом Союза или государства-члена, под действие которого подпадает контролер и которое обеспечивает соответствующие меры для защиты легитимных интересов субъекта данных; предоставление указанной информации оказывается невозможным или требует непропорционального усилия и др.). Схожий механизм предусмотрен и в законодательстве Российской Федерации.

В Беларуси использован механизм соответствующего информирования субъекта, направленный с одной стороны на минимизацию бремени администрирования для операторов, а с другой – исключающий перегрузку субъектов ненужной им информацией.

В этой связи комментируемая статья закрепляет право субъекта персональных данных получать от оператора информацию

о предоставлении своих персональных данных третьим лицам. Наличие у субъекта такого права предполагает обязанность оператора обеспечить учет фактов передачи персональных данных третьим лицам.

Данное право может быть реализовано субъектом персональных данных один раз в календарный год (с 1 января по 31 декабря) бесплатно, если иное не предусмотрено Законом и иными законодательными актами.

Законодательными актами может быть предусмотрена:

возможность в целом не предоставлять информацию субъекту персональных данных в рамках комментируемой статьи (примером могут быть положения п. 3 ст. 12 Закона);

возможность получения соответствующей информации с иной периодичностью;

возможность получения такой информации только на платной основе;

возможность получения информации однократно бесплатно, а в дельнейшем – без ограничений на платной основе.

Пример.

В соответствии со ст. 13 Закона Республики Беларусь от 10 ноября 2008 г. № 441-З "О кредитных историях" субъекту кредитной истории кредитный отчет, в том числе в части сведений о запросах пользователей кредитной истории (банков, государственных органов и др.), предоставляется по его заявлению на получение кредитного отчета без уплаты вознаграждения один раз в течение календарного года и неограниченное количество раз в течение календарного года за вознаграждение.

Если в законодательных актах не содержится никаких оговорок, то по смыслу Закона после получения интересующей информации субъект персональных данных не может настаивать на предоставлении в течение календарного года оператором ему обновленной информации, в том числе на платной основе.

Для получения информации о предоставлении персональных данных третьим лицам субъект персональных данных подает заявление оператору в порядке, установленном ст. 14 Закона. В этой связи оператор имеет право отказать в предоставлении соответствующей информации, в случае несоответствия поданного заявления необходимым требованиям (например, заявление направляется на адрес электронной почты).

2. При поступлении от субъекта персональных данных заявления о получении информации о предоставлении персональных данных третьим лицам оператор обязан направить ему информацию о том, какие персональные данные (подлежат указанию конкретные данные, а не их обобщенное описание) этого субъекта и кому (с указанием конкретных организаций) предоставлялись в течение года, предшествовавшего дате подачи заявления.

Исключением являются случаи совершения многократных и типичных операций по обработке персональных данных, в связи с чем нет необходимости называть каждую из них отдельно. Если подобная передача носила многократный однотипный характер, то допустимо ограничиться указанием на период и периодичность такой передачи (например, 2 раза в ноябре текущего года; 3 раза в период с… по… и т.п.).

Информация предоставляется оператором в пятнадцатидневный срок после получения заявления. Если у оператора имеются причины для отказа в ее предоставлении, он должен уведомить об этом субъекта персональных данных в указанный срок. Неправомерный отказ в предоставлении сведений, невыполнение данной обязанности в установленный срок, предоставление неполных сведений являются нарушением законодательства о персональных данных и влекут ответственность по ч. 1 ст. 23.7 КоАП.

3. Информация о предоставлении персональных данных третьим лицам может не предоставляться в случаях:

перечисленных в ст. 11 Закона;

если обработка персональных данных осуществляется в соответствии с законодательством об исполнительном производстве, при осуществлении правосудия и организации деятельности судов общей юрисдикции.

Наибольший интерес представляют положения абзаца восьмого п. 3 ст. 11 Закона – если обработка осуществляется в иных случаях, предусмотренных законодательными актами.

По смыслу Закона как обработка, которая осуществляется в случаях, предусмотренных законодательными актами, рассматриваются ситуации, когда обязанность предоставления персональных данных прямо предусмотрена в законодательном акте и такое предоставление осуществляется без необходимости предварительного получения запроса.

Пример.

Организация, являющаяся плательщиком обязательных страховых взносов, согласно абзацу шестому п. 1 ст. 21 Закона Республики Беларусь от 15 июля 2021 г. № 118-З "О взносах в бюджет государственного внебюджетного фонда социальной защиты населения Республики Беларусь" обязана "представлять в органы Фонда (городские, районные, районные в городах отделах (секторах) областных, Минского городского управлений Фонда) установленные законодательством сведения и отчетность, обеспечивать своевременность выплаты пособий в счет начисленных обязательных страховых взносов".

Данные ситуации следует отличать от ситуаций, когда законодательный акт закрепляет возможность третьего лица направить с учетом особенностей конкретной ситуации запрос на получение таких сведений, который подлежит в каждом случае оценке

оператором на предмет наличия оснований для предоставления запрашиваемых данных, их неизбыточности и др. Эти случаи не подпадают под рассматриваемое исключение.

В случаях, которые не подпадают под исключения из права субъектов персональных данных на получение информации о предоставлении их персональных данных третьим лицам, согласно п. 3 ст. 12 Закона, необходимо вести учет фактов такого предоставления.

Статья 13. Право требовать прекращения обработки персональных данных и (или) их удаления

Комментарий к статье 13

1. Комментируемая статья закрепляет право субъекта персональных данных требовать от оператора бесплатного прекращения обработки своих персональных данных, включая их удаление.

Данное право вытекает из положений ст. 4 и является важнейшим и контрольным инструментом субъекта персональных данных по отношению к оператору. Если права, предусмотренные ст.ст. 11–12 Закона, носят преимущественно информационный характер, то рассматриваемое право дает возможность запрещать обработку, требовать удаления данных, то есть требовать от оператора осуществления фактических действий, которые нередко могут иметь для него серьезные последствия (финансовые, организационные и др.).

Дополнительный вес рассматриваемому праву придает установление административной ответственности за умышленную незаконную обработку персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных.

Обязательным условием реализации данного права является отсутствие оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами.

Как отсутствие оснований для обработки персональных данных должны рассматриваться не только ситуации, когда нет согласия или одного из оснований, предусмотренных в ст.ст. 6 и 8 Закона, но и ситуации, когда:

имеется согласие субъекта персональных данных, но оно не соответствует требованиям Закона (не является свободным, однозначным, информированным);

согласие имело место, но было отозвано субъектом персональных данных или срок согласия истек, а оператор не прекратил обработку персональных данных;

обрабатываемые персональные данные носят избыточный характер по отношению к цели обработки;

установленный законодательством или оператором срок хранения персональных данных истек, но оператор продолжает их хранить (например, хранение резюме непринятого на работу по истечении 1 года, хранение договора по истечении 3 лет после проведения налоговыми органами проверки соблюдения налогового законодательства) и др.

Справочно:

Аналогичное право предусмотрено и в законодательстве зарубежных стран. В частности, ст. 17 GDPR предусмотрено "право на забвение", в рамках реализации которого субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные при наличии одного из следующих оснований:

персональные данные больше не требуются для целей, для которых они были собраны или обработаны иным способом;

субъект данных отзывает свое согласие, на основании которого проводилась обработка, и отсутствует иное законное основание для обработки;

субъект данных возражает против обработки, и отсутствуют имеющие преимущественную юридическую силу законные основания для обработки;

персональные данные обрабатывались незаконно;

персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству, под действие которого подпадает контролер;

персональные данные собирались в отношении предоставления услуг информационного общества.

2. Для прекращения обработки персональных данных и (или) их удаления субъект персональных данных подает оператору заявление в порядке, установленном ст. 14 Закона.

3. Оператор обязан в пятнадцатидневный срок после получения заявления субъекта персональных данных прекратить обработку персональных данных, а также осуществить их удаление (обеспечить прекращение обработки персональных данных, а также их удаление уполномоченным лицом) и уведомить об этом субъекта персональных данных.

О механизме удаления (*см. подробнее комментарий к ст. 1 Закона*).

После удаления персональных данных целесообразным представляется также принятие оператором разумных мер для уведомления о прекращении обработки (удалении, блокировании) персональных данных третьих лиц, которым персональные данные этого субъекта были ранее переданы.

4. Право требовать прекращения и удаления персональных данных не является абсолютным. Оператор вправе отказать субъекту персональных данных в удовлетворении требований о прекращении

обработки его персональных данных и (или) их удалении при наличии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами, в том числе если они являются необходимыми для заявленных целей их обработки, с уведомлением об этом субъекта персональных данных в пятнадцатидневный срок.

В этой связи нельзя не отметить довольно распространенную на практике модель ”трансформации“ правового основания обработки персональных данных, когда несмотря на достижение первоначальной цели оператор не обязан удалять персональные данные.

Например, в случае, если хранение документов уволенного работника обусловлено необходимостью соблюдения требований о хранении документов, предусмотренных Законом Республики Беларусь от 25 ноября 2011 г. № 323-З ”Об архивном деле и делопроизводстве“ и принятым в его развитие постановлением Министерства юстиции Республики Беларусь от 24 мая 2012 г. № 140 ”О перечне типовых документов“, реализовать рассматриваемое право не представляется возможным, поскольку есть иное правовое основание обработки (хранения) персональных данных.

Статья 14. Порядок подачи заявления субъектом персональных данных оператору

Комментарий к статье 14

1. Комментируемая статья определяет порядок подачи заявлений субъектов персональных данных, направленных на реализацию предусмотренных Законом прав на:

отзыв согласия;

получение информации, касающейся обработки персональных данных;

изменение персональных данных;

получение информации о предоставлении персональных данных третьим лицам;

прекращение обработки персональных данных и (или) их удаления.

Адресатом заявления Закон определяет оператора. В случае направления заявления субъекта персональных данных для реализации своих прав уполномоченному лицу, последний не обязан отвечать по существу на данный запрос. Вместе с тем ответ уполномоченным лицом на заявление субъекта персональных данных не будет противоречить законодательству о персональных данных.

Определенные особенности имеет подача заявлений в ситуации сооператорства (обработки персональных данных несколькими операторами, совместно организующими или осуществляющими обработку персональных данных). В таком случае порядок рассмотрения заявлений субъектов персональных данных должен быть определен в договоре, регулирующем взаимодействие сооператоров.

Например, каждый оператор может самостоятельно рассматривать адресованные ему заявления субъектов персональных данных или ответственным за рассмотрение заявлений субъектов персональных данных может быть только один из операторов независимо от того, кому они адресованы. При этом независимо от того, кто из сооператоров будет ответственен за подготовку проектов ответов, сами ответы в силу императивного характера рассматриваемой нормы направляются субъектам персональных данных тем из сооператоров, кому было адресовано заявление.

Заявление должно быть подано в письменной форме или в виде электронного документа, удостоверенного электронной цифровой подписью. В случае реализации субъектом персональных данных права на отзыв согласия, возможна подача заявления в форме, в которой такое согласие было получено.

Предоставление права подавать обращения указанными способами одновременно означает обязанность оператора обеспечить возможность подачи заявления любым из таких способов.

По общему правилу, подача заявления в письменной форме не требует личного присутствия и предъявления документа, удостоверяющего личность. Исходя из этого, заявления можно направить по почте. Однако законодательными актами могут быть предусмотрены исключения.

Например, согласно ч. 1 п. 4 ст. 26 Закона ”О регистре населения“ справки (выписки) из регистра населения предоставляются по письменному заявлению физического лица о предоставлении справки (выписки) из регистра при его личном обращении в регистрирующую службу с предъявлением документа, удостоверяющего личность.

2. Пункт 2 комментируемой статьи Закона закрепляет требования к содержанию заявлений субъектов персональных данных. Предусматривается, что заявление субъекта персональных данных должно содержать:

фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания);

дату рождения субъекта персональных данных;

идентификационный номер субъекта персональных данных, при отсутствии такого номера – номер документа, удостоверяющего личность субъекта персональных данных, в случаях, если эта информация указывалась субъектом персональных данных при даче своего согласия оператору или обработка персональных данных осуществляется без согласия субъекта персональных данных;

изложение сути требований субъекта персональных данных;

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

В случае несоблюдения субъектом персональных данных требований, установленных в п.п. 1 и 2 комментируемой статьи Закона, оператор вправе оставить заявление без рассмотрения по существу.

Вместе с тем закрепленные критерии на практике могут создавать проблемы в виде избыточной обработки оператором персональных данных в случае, если он идентифицирует субъекта посредством иных, не указанных в комментируемом пункте, данных.

Пример.

Субъект персональных данных получил доступ к онлайн-сервису, создав учетную запись пользователя. Обработка персональных данных осуществляется без согласия лица на основании договора. Владелец этого сервиса не осуществляет обработку фамилии, имени, даты рождения пользователя, а идентифицирует его с помощью логина и пароля. Направление пользователем заявления, содержащего данные, указанные в п. 2 ст. 14 Закона, не позволит оператору надлежащим образом на него отреагировать. В такой ситуации представляется целесообразным указание в заявлении той информации, которая поможет оператору идентифицировать субъекта. При этом отсутствие в заявлении закрепленной в п. 2 ст. 14 Закона информации не должно рассматриваться как нарушение законодательства о персональных данных.

При возникновении у оператора сомнений в идентификации лица, направившего заявление в соответствии с комментируемой статьей, он может использовать иные способы для подтверждения его личности. Например, в вышеприведенном случае – попросить субъекта персональных данных направить сообщение из личного кабинета пользователя.

3. Пункт 3 комментируемой статьи Закона определяет форму ответа оператора на заявление. Так, ответ на заявление, как правило, направляется субъекту персональных данных в форме, соответствующей форме подачи заявления.

Вместе с тем субъект персональных данных вправе указать в заявлении желаемую форму получения ответа. Например, электронный документ может содержать просьбу направить письменный ответ.

Статья 15. Право на обжалование действий (бездействия) и решений оператора, связанных с обработкой персональных данных

Комментарий к статье 15

1. Комментируемая статья Закона посвящена процедуре обжалования действий (бездействия) и решений оператора, связанных с обработкой персональных данных.

В соответствии с ч. 1 п. 1 комментируемой статьи Закона субъект персональных данных вправе обжаловать действия (бездействие) и решения оператора, нарушающие его права при обработке персональных данных, в уполномоченный орган по защите прав субъектов персональных данных.

Органом по защите прав субъектов персональных данных, уполномоченным на рассмотрение жалоб, является Национальный центр защиты персональных данных.

Законодательство не закрепляет обязанность обратиться к оператору до подачи жалобы в Центр, однако сложившаяся практика свидетельствует об эффективности подобного механизма.

Правом подачи жалобы обладает субъект персональных данных, чьи права были нарушены оператором. Он может обратиться с жалобой лично или через представителя. В последнем случае к жалобе должен быть приложен документ, подтверждающий полномочия представителя (доверенность, удостоверение на право представления интересов подопечного – например, в отношении лица, признанного ограниченно дееспособным).

Предметом жалобы могут быть действия (бездействие) оператора. Действия оператора могут быть оформлены соответствующим актом (решением), а могут такой формы не иметь и носить характер фактических действий. Бездействие, в свою очередь, может выражаться в несовершении оператором действий, направленных на защиту персональных данных субъекта (например, неудалении данных).

Рассмотрение жалоб Центром осуществляется в порядке, установленном Положением.

Жалобы в Центр подаются в письменной форме или в виде электронного документа, удостоверенного электронной цифровой подписью. Возможность подачи жалобы в электронной форме без электронной цифровой подписи не предусмотрена, в связи с чем жалобы, направленные на электронную почту Центра, оставляются без рассмотрения по существу. Такой подход обусловлен наличием у Центра существенных полномочий по вмешательству в деятельность

операторов и недопустимостью злоупотребления правом в виде направления жалоб от имени иных лиц, использования контрольных полномочий в качестве элемента неконкурентной борьбы и др.

Частью второй п. 27 Положения определен срок обращения с жалобой в Центр – три месяца со дня, когда лицу стало известно о действиях (бездействии), которые непосредственно затрагивают его права, свободы и законные интересы. Столь небольшой срок обусловлен динамичностью соответствующих правоотношений: по истечении времени ”информационный след“ может отсутствовать и установление действительных обстоятельств дела станет затруднительным.

Пунктом 28 Положения закреплены требования к содержанию жалобы. В частности, она должна содержать:

фамилию, собственное имя, отчество (если таковое имеется) субъекта персональных данных, адрес его места жительства (места пребывания);

изложение сути жалобы с указанием действий (бездействия), которыми нарушаются права, свободы и законные интересы субъекта персональных данных.

Важно учитывать, что от способа изложения жалобы (формулировки конкретных требований и обоснования позиции) часто зависит эффективность ее разрешения;

информацию о принятых мерах по восстановлению нарушенных прав, свобод и законных интересов субъекта персональных данных (в том числе обращение к оператору (уполномоченному лицу), в суд, органы прокуратуры или иные государственные органы) или об отсутствии таких мер.

Как уже отмечалось, предварительное обращение к оператору необходимо для обеспечения сохранности необходимых доказательств и ускорения защиты прав и свобод физических лиц при обработке их персональных данных;

личную подпись субъекта персональных данных в случае направления жалобы в письменной форме.

При наличии подтверждающих нарушение прав, свобод и законных интересов субъекта персональных данных материалов (документы, фотографии, скриншоты и т.п.) они прилагаются к жалобе.

Жалоба оставляется без рассмотрения по существу, если она:

не соответствует установленным требованиям о сроках, форме и содержании;

рассмотрена, рассматривается или подлежит рассмотрению в соответствии с законодательством о конституционном судопроизводстве, гражданским процессуальным, хозяйственным

процессуальным, уголовно-процессуальным законодательством, законодательством, определяющим порядок административного процесса, либо если в соответствии с законодательными актами установлен иной порядок подачи и рассмотрения такой жалобы.

На практике наиболее распространенными ошибками, влекущими оставление жалобы без рассмотрения по существу, являются следующие ситуации:

1) жалоба направлена в электронной форме (без электронной цифровой подписи) на адрес электронной почты Центра;

2) жалоба содержит данные, указывающие на признаки административного правонарушения и (или) преступления (хищение денежных средств с использованием банковских карт, разглашение охраняемой законом тайны и т.д.) и требование о привлечении виновного лица к административной ответственности.

В соответствии со ст. 3.30 ПИКоАП протоколы об административных правонарушениях по ст. 23.7 ”Нарушение законодательства о защите персональных данных“ имеют право составлять уполномоченные на то должностные лица органов внутренних дел, а также прокурор (при осуществлении им надзорных функций). Центр не уполномочен составлять протоколы или рассматривать дела об административных правонарушениях по данной статье КоАП, а также анализировать обстоятельства, изложенные в жалобе, на предмет наличия (отсутствия) признаков административного правонарушения и (или) преступления;

3) жалоба касается обработки персональных данных в ходе судебного разбирательства и судебного решения.

Если лицо не согласно с применением судом законодательства о персональных данных, то оно вправе обжаловать судебное постановление в порядке, предусмотренном соответствующим процессуальным кодексом.

Для принятия решения об оставлении жалобы без рассмотрения по существу определен срок в 10 рабочих дней со дня, следующего за днем ее регистрации.

В свою очередь, для рассмотрения жалобы по существу установлен срок 1 месяц со дня, следующего за днем ее регистрации, который может быть продлен при необходимости дополнительного изучения и проверки, но не более чем на один месяц.

Если установленные к подаче жалобы требования соблюдены, то она принимается к рассмотрению и субъект уведомляется о сроках ее рассмотрения и получения ответа. По результатам анализа сведений, содержащихся в жалобе, в целях установления возможных нарушений законодательства о персональных данных в отношении оператора может

быть назначена внеплановая или камеральная проверка. В ходе проверки осуществляется изучение, анализ и оценка документов и иной информации, в том числе полученной от оператора (уполномоченного лица) по запросу Центра. При этом проверке могут подлежать не только указанные в жалобе факты, но и иные вопросы.

В рамках рассмотрения жалобы Центр имеет право запрашивать и получать на безвозмездной основе от государственных органов, юридических лиц Республики Беларусь, иных организаций и физических лиц информацию (в том числе персональные данные физических лиц без их согласия) на основании абзаца второго п. 8 Положения. Например, при необходимости определить владельца интернет-ресурса, мобильного телефона, перечень лиц, которые имели в определенный период доступ к персональным данным, и др. Для предоставления запрашиваемых сведений установлен срок 10 календарных дней со дня поступления запроса. Непредставление запрашиваемой информации является административным правонарушением, предусмотренным ст. 24.11 КоАП.

В случае подтверждения указанных в жалобе нарушений при обработке персональных данных Центр принимает необходимые меры по защите нарушенных прав, свобод и законных интересов субъекта персональных данных, подавшего жалобу.

Например, в целях устранения нарушений законодательства о персональных данных Центр может обязать оператора исключить обработку избыточных персональных данных, удалить незаконно обрабатываемые персональные данные, проинформировать субъектов персональных данных об утечке, обеспечить получение согласия, соответствующего требованиям ст. 5 Закона в течение определенного срока, перечислить в политике в отношении обработки персональных данных уполномоченных лиц, которым передаются данные клиентов оператора, и т.д.

Если нарушения затрагивают не только заявителя, но и иных лиц, например, участников программы лояльности, социально уязвимых категорий субъектов персональных данных (несовершеннолетние, пенсионеры), либо установлены нарушения при трансграничной передаче персональных данных, либо установлены иные существенные нарушения, Центр направляет в органы внутренних дел материалы для инициирования начала административного или уголовного процесса.

Если содержащиеся в жалобе сведения о нарушениях при обработке персональных данных не подтверждаются, Центр оставляет жалобу без удовлетворения.

Субъект персональных данных уведомляется о принятом решении, а в случае оставления жалобы без удовлетворения ему дополнительно разъясняются причины такого решения и порядок его обжалования.

Поступление повторной жалобы, которая не содержит новых обстоятельств, имеющих значение для их рассмотрения по существу, является основанием для прекращения переписки. В таком случае субъекту персональных данных направляется соответствующее уведомление. Последующие жалобы по вопросам, по которым прекращена переписка, рассмотрению не подлежат (без уведомления субъекта персональных данных).

2. В п. 2 комментируемой статьи Закона определяется порядок обращения заявителя с жалобой в суд. Установлено, что принятое уполномоченным органом по защите прав субъектов персональных данных решение может быть обжаловано субъектом персональных данных в суд в порядке, установленном законодательством.

Учитывая, что заявителем выступает физическое лицо, такие жалобы подведомственны судам общей юрисдикции, рассматривающим гражданские дела. Соответственно, порядок обжалования решения регламентируется ГПК, а именно параграфом 6 ”Особенности рассмотрения и разрешения жалоб на действия (бездействие) государственных органов и иных юридических лиц, а также организаций, не являющихся юридическими лицами, и должностных лиц, ущемляющих права граждан, а в случаях, предусмотренных актами законодательства, – и права юридических лиц“ главы 29.

Если иное не предусмотрено ГПК, жалоба подается в суд по месту нахождения государственного органа, иного юридического лица, другой организации или по месту работы должностного лица, чьи действия обжалуются (ч. 3 ст. 354 ГПК). Исходя из этого, жалобы на решения Центра подсудны суду Московского района г. Минска.

В случае обжалования одновременно действий (бездействия) оператора и решения Центра заявитель вправе самостоятельно определить подсудность жалобы суду по месту нахождения одного из органов или работы должностных лиц, чьи действия обжалуются, применительно к ч. 13 ст. 47 ГПК (п. 8 постановления Пленума Верховного Суда Республики Беларусь от 24 декабря 2009 г. № 11 ”О применении судами законодательства, регулирующего защиту прав и законных интересов граждан при рассмотрении жалоб на неправомерные действия (бездействие) государственных органов, иных организаций и должностных лиц“).

Частью первой ст. 355 ГПК установлен месячный срок на подачу жалобы в суд, который исчисляется со дня получения гражданином отказа Центра в удовлетворении жалобы или со дня истечения месячного

срока после подачи жалобы, если заявителем не был получен на нее ответ. В последнем случае в связи с полномочием Центра продлевать срок рассмотрения жалобы исчисление срока обращения в суд при неполучении ответа начинается со дня, следующего за днем, указанным в уведомлении о принятии жалобы к рассмотрению.

Статья 16. Обязанности оператора

Комментарий к статье 16

1. В комментируемой статье закрепляется перечень обязанностей оператора. Указанные обязанности развивают положения ст. 4 Закона (в частности, требования о законности, прозрачности обработки персональных данных и т.п.), иные положения Закона (например, ст.ст. 10–13, 17), а также выступают одним из элементов механизма реализации прав субъекта персональных данных.

Оператор обязан:

а) разъяснять субъекту персональных данных его права, связанные с обработкой персональных данных.

Данная обязанность направлена на реализацию требования о прозрачном характере обработки персональных данных и предполагает доведение до сведения субъектов персональных данных его прав, связанных с обработкой персональных данных. Из Закона следуют два случая, когда субъекту персональных данных необходимо разъяснять его права:

при получении согласия на обработку персональных данных (п. 5 ст. 5 Закона) *(подробнее см. комментарий к ст. 5)*;

в документах, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных (абзац третий п. 3 ст. 17 Закона) *(см. соответствующий комментарий)*;

б) получать согласие субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами.

Комментируемая обязанность является развитием ч. 1 п. 3 ст. 4 Закона, согласно которой обработка персональных данных осуществляется с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом и иными законодательными актами.

Указанное положение также означает, что согласие не может выступать надлежащим правовым основанием в случае, когда имеются правовые основания обработки персональных данных без согласия (определены в ст. 6 и в п. 2 ст. 8 Закона).

Некоторые операторы (особенно на этапе вступления Закона в силу) определяли согласие как некое универсальное основание для обработки персональных данных, которое может легитимировать любую обработку персональных данных (например, в трудовых отношениях либо при заключении договора).

Такое ошибочное понимание системы правовых оснований обработки персональных данных привело к практике получения множества ”лишних“ согласий, что увеличивало объем документов и вызывало непонимание и раздражение граждан. При этом получаемые согласия не носили свободного характера, поскольку субъект персональных данных не мог отказать в его предоставлении (например, нанимателю в процессе трудовой деятельности), а отзыв его не приводил к прекращению обработки, поскольку персональные данные обрабатывались в силу иных оснований (например, при исполнении договора оказания услуг);

в) обеспечивать защиту персональных данных в процессе их обработки.

Обязанность обеспечивать защиту персональных данных – универсальное требование к любому оператору независимо от количества бизнес-процессов, требующих обработки персональных данных, масштабов обработки персональных данных, категорий персональных данных, численности работников, финансовых возможностей оператора и т.п. Данная обязанность вытекает из статуса оператора как лица, являющегося в целом ответственным за обработку персональных данных (принимающего решение о ключевых параметрах обработки).

Оператор несет обязанность по обеспечению защиты персональных данных и в том случае, когда он сам не осуществляет обработку персональных данных, а поручает ее уполномоченному лицу. В таком случае исполнение обязанности достигается путем соблюдения ст. 7 Закона (например, включение в договор с уполномоченным лицом положений по обеспечению защиты персональных данных). При этом именно оператор несет ответственность перед субъектом персональных данных за несоблюдение уполномоченным лицом мер по обеспечению защиты персональных данных. В этой связи оператор должен обеспечивать контроль за надлежащим исполнением договора уполномоченным лицом в этой части и при необходимости запрашивать подтверждение соблюдения мер по обеспечению защиты персональных данных (например, копии локальных правовых актов, документы, подтверждающие осуществление технической и криптографической защиты персональных данных, и т.п.);

г) предоставлять субъекту персональных данных информацию о его персональных данных, а также о предоставлении его персональных данных третьим лицам, за исключением случаев, предусмотренных Законом и иными законодательными актами.

Норма обеспечивает реализацию прав субъекта персональных данных, предусмотренных ст.ст. 11 и 12 Закона *(см. соответствующий комментарий к указанным статьям)*;

д) вносить изменения в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных.

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

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

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

получено заявление субъекта персональных данных об изменении персональных данных;

оператору становится известно, что персональные данные являются неполными, устаревшими или неточными (например, изменился адрес места жительства субъекта персональных данных, что выяснилось при посещении им банка в целях получения новых услуг в рамках уже заключенного комплексного договора банковского обслуживания).

Исключением из этого подхода может быть ситуация, когда устаревшие персональные данные продолжают обрабатываться в силу требований законодательства (цели обработки не предполагают актуализацию персональных данных). Например, в информационных ресурсах территориальной организации по государственной регистрации недвижимого имущества обрабатывается девичья фамилия женщины, регистрировавшей сделку по отчуждению недвижимого имущества. В таком случае данные должны сохраняться в оригинальном виде

для целей надлежащего ведения единого государственного регистра недвижимого имущества, прав на него и сделок с ним;

е) прекращать обработку персональных данных, а также осуществлять их удаление или блокирование (обеспечивать прекращение обработки персональных данных, а также их удаление или блокирование уполномоченным лицом) при отсутствии оснований для обработки персональных данных, предусмотренных Законом и иными законодательными актами.

Рассматриваемая обязанность призвана обеспечивать практическую реализацию права субъекта персональных данных, предусмотренного ст. 13 Закона (*подробнее см. комментарий к ст. 13*).

Данная обязанность не подлежит исполнению в случае, когда оператор обязан продолжить обработку персональных данных в силу требований законодательства (например, хранение собственниками пунктов коллективного пользования интернет-услугами персональных данных пользователей интернет-услуг и т.п.);

ж) уведомлять уполномоченный орган по защите прав субъектов персональных данных о нарушениях систем защиты персональных данных незамедлительно, но не позднее трех рабочих дней после того, как оператору стало известно о таких нарушениях, за исключением случаев, предусмотренных уполномоченным органом по защите прав субъектов персональных данных.

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

Нарушение систем защиты персональных данных способно причинить серьезный вред правам и законным интересам субъектов персональных данных. Уведомление о таком инциденте Центра направлено на минимизацию негативных последствий нарушений и выявление всех обстоятельств, ставших причиной инцидента.

Порядок уведомления Национального центра защиты персональных данных о нарушениях систем защиты персональных данных определен приказом Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 13 ”Об уведомлении о нарушениях системы защиты персональных данных“ (далее – Приказ № 13).

Согласно п. 1 данного Приказа уведомление о нарушениях систем защиты персональных данных направляется оператором в Центр при нарушении систем защиты персональных данных, за исключением случаев, когда нарушение систем защиты не привело к:

незаконному распространению, предоставлению персональных данных;

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

С учетом данного пункта обязанность направления такого уведомления не зависит от количества лиц, затронутых данным нарушением.

Пунктом 2 Приказа № 13 установлены сведения, которые в обязательном порядке подлежат отражению в уведомлении, а также форма направления такого уведомления – письменная либо в виде электронного документа.

Срок направления уведомления составляет три рабочих дня и начинает течь на следующий рабочий день после того, как оператору стало известно о нарушении систем защиты персональных данных. Ненаправление уведомления в указанный срок содержит признаки административного правонарушения, предусмотренного ст. 24.11 ”Непредставление документов, отчетов и иных материалов“ КоАП.

Необходимо отметить, что с развитием информационных технологий оператору крайне сложно скрыть ”утечку“ персональных данных, поскольку, как правило, информация о такой утечке незамедлительно публикуется на различных интернет-ресурсах (а нередко и сама база данных). При этом ненаправление уведомления в адрес Центра рассматривается как безусловное основание для назначения внеплановой проверки деятельности оператора;

з) осуществлять изменение, блокирование или удаление недостоверных или полученных незаконным путем персональных данных субъекта персональных данных по требованию уполномоченного органа по защите прав субъектов персональных данных, если иной порядок внесения изменений в персональные данные, их блокирования или удаления не установлен законодательными актами.

Оператор обязан по требованию уполномоченного органа осуществлять изменение, блокирование или удаление персональных данных в случае выявления:

недостоверных персональных данных;

персональных данных, полученных незаконным путем.

Подобные требования могут являться результатом проведенных проверок, рассмотрения жалоб субъектов персональных данных, обращений граждан и юридических лиц, изучения информации, размещенной в глобальной компьютерной сети Интернет либо полученной от других государственных органов и организаций.

При этом законодательными актами может предусматриваться иной порядок внесения изменений в персональные данные, их блокирования или удаления;

и) исполнять иные требования уполномоченного органа по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных.

Согласно абзацу шестому п. 8 Положения Центр имеет право требовать от операторов (уполномоченных лиц) изменения, блокирования или удаления недостоверных или полученных незаконным путем персональных данных, устранения иных нарушений законодательства о персональных данных.

Указанное право является ключевым, раскрывающим статус Центра как уполномоченного органа по защите прав субъектов персональных данных, который наделен обширными полномочиями по предъявлению обязательных к исполнению операторами требований по приведению их деятельности в соответствии с Законом.

На практике к числу таких требований относятся разработка (корректировка) необходимых документов (локальных правовых актов), доработка сайта (например, рубрик, посредством которых осуществляется сбор персональных данных), удаление персональных данных (например, обрабатываемых без надлежащих правовых оснований), повторное рассмотрение заявления субъекта персональных данных о реализации права, направление субъектам персональных данных писем в случае утечки персональных данных и т.п.;

к) выполнять иные обязанности, предусмотренные Законом и иными законодательными актами.

К числу таких обязанностей оператора, которые установлены Законом и иными законодательными актами (в частности, Указом № 422), следует отнести:

принятие комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при обработке специальных персональных данных для прав и свобод субъектов персональных данных (*см. подробнее комментарий к п. 3 ст. 8 Закона)*;

соблюдение оператором порядка привлечения к обработке персональных данных уполномоченных лиц;

обеспечение правовых оснований для трансграничной передачи персональных данных на территории иностранных государств, где не обеспечивается надлежащий уровень защиты прав субъектов персональных данных;

предоставление информации, необходимой для определения законности действий операторов (уполномоченных лиц);

размещение на официальном сайте в глобальной компьютерной сети Интернет информации об информационных ресурсах (системах), содержащих персональные данные, владельцем которых выступает оператор, являющийся республиканским органом государственного управления (п. 2 ст. 16 Закона);

организацию не реже одного раза в пять лет прохождения обучения по вопросам защиты персональных данных лицами, ответственными за осуществление внутреннего контроля за обработкой персональных данных, а также лицами, непосредственно осуществляющими обработку персональных данных (подп. 3.3 п. 3 Указа № 422);

внесение с 1 января 2024 г. в государственный информационный ресурс ”Реестр операторов персональных данных“ сведений об информационных ресурсах (системах), содержащих персональные данные, а также актуализацию соответствующих сведений (подп. 3.6 п. 3 Указа № 422);

установление и поддержание в актуальном состоянии:

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

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

общедоступные персональные данные;

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

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными;

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

г) срока хранения обрабатываемых персональных данных (подп. 3.5 п. 3 Указа № 422).

2. Пункт 2 комментируемой статьи предусматривает необходимость для операторов, являющихся республиканскими органами государственного управления, размещать на своих официальных сайтах в глобальной компьютерной сети Интернет информацию об информационных ресурсах (системах), содержащих персональные данные, владельцем которых они являются.

В соответствии с подп. 1.1 п. 1 Указа Президента Республики Беларусь от 5 мая 2006 г. № 289 ”О структуре Правительства Республики Беларусь“ республиканскими органами государственного управления являются министерства и государственные комитеты. Конкретный

перечень министерств и государственных комитетов содержится в приложении к названному Указу.

Вместе с тем из данной обязанности имеется ряд исключений. Так, не подлежит размещению информация об информационных ресурсах (системах), содержащая:

персональные данные, обработка которых осуществляется в случаях, предусмотренных абзацами четвертым–седьмым п. 3 ст. 11 Закона;

персональные данные его работников в процессе осуществления трудовой (служебной) деятельности;

служебную информацию ограниченного распространения.

Порядок отнесения сведений к служебной информации ограниченного распространения, а также перечень сведений, которые к ней могут относиться, определяется в соответствии со ст. 18[1] Закона ”Об информации, информатизации и защите информации“ и постановлением Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 ”О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну“.

Статья 17. Меры по обеспечению защиты персональных данных

Комментарий к статье 17

1. Комментируемая статья раскрывает содержание одной из ключевых обязанностей оператора (уполномоченного лица) – обеспечение защиты персональных данных.

Исходя из положений п. 3 ст. 17 Закона, термин ”защита персональных данных“ следует понимать достаточно широко. Как меры по обеспечению защиты персональных данных следует рассматривать не только сугубо технические меры защиты персональных данных (например, применение криптографических мер), но и мероприятия, которые способствуют надлежащей реализации мер, направленных на недопущение неправомерных действий в отношении персональных данных, а также исполнению иных обязанностей оператора по обеспечению требований Закона (например, осуществление внутреннего контроля за обработкой персональных данных, ведение реестра обработок, внесение изменений в должностные инструкции).

Закон определяет виды мер, которые следует принимать для защиты информации: правовые, организационные и технические. Однако содержание таких мер, в отличие от Закона ”Об информации, информатизации и защите информации“ (ст. 29), не раскрывается.

Зачастую бывает сложно определить, к какому конкретно виду относится та или иная мера. Так, например, реализация многих организационных мер невозможна без издания локальных правовых актов. Принятие технических мер требует совершения организационных действий. Тем не менее указанное деление имеет своей целью определить основные направления (векторы), по которым требуется принятие мер.

Принятие описанных мер имеет своей целью воспрепятствование несанкционированному или случайному доступу к персональным данным, изменению, блокированию, копированию, распространению, предоставлению, удалению персональных данных, а также иным неправомерным действиям в отношении персональных данных. Указанный перечень неправомерных действий не является исчерпывающим, но дает общее представление о круге возможных рисков, которые требуют принятия мер защиты.

2. Закон не содержит исчерпывающего перечня мер, принятие которых будет свидетельствовать о соблюдении оператором обязанности по обеспечению защиты персональных данных. Объясняется это тем, что с учетом разных сфер деятельности операторов, масштабов обработки персональных данных, способов обработки, категорий персональных данных и иных обстоятельств определение некоего универсального перечня мер не представляется возможным.

Более того, при выборе перечня мер, подлежащих принятию, следует учитывать в первую очередь потенциальные риски, связанные с обработкой персональных данных, которые определяются оператором самостоятельно с учетом своей деятельности. Это отражает содержание риск-ориентированного подхода, который положен в основу системы управления рисками в цифровой сфере во многих странах и реализован в комментируемом Законе.

С учетом риск-ориентированного подхода оператор (уполномоченное лицо) определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты персональных данных.

Тем не менее это не значит, что оператор абсолютно свободен в выборе таких мер, поскольку в п. 3 ст. 17 Закона и подп. 3.5 п. 3 Указа № 422 уже закреплен перечень обязательных мер, которые подлежат принятию каждым оператором (за некоторым исключением), – своеобразный фундамент, на который надстраиваются иные меры.

Оператору не следует ограничиваться принятием необходимого минимума (что является достаточно типичным нарушением законодательства), а необходимо принять и иные меры, прямо не указанные в законодательстве о персональных данных, но требующиеся с учетом его специфики.

Например, операторам, которые осуществляют на постоянной основе масштабную обработку персональных данных, целесообразно осуществить систематизацию и вести дальнейший учет обработок персональных данных. Отсутствие такого учета в крупных организациях может привести к ”выпадению“ отдельных бизнес-процессов, в ходе которых обрабатываются персональные данные. Как следствие, подобные бизнес-процессы не будут надлежащим образом приведены в соответствие с требованиями Закона (например, в части соблюдения общих требований к обработке персональных данных), а информация о таких бизнес-процессах не будет доведена до субъектов персональных данных (например, в политике в отношении обработки персональных данных). Кроме того, отсутствие такой меры не позволит выполнять и иные обязанности оператора (например, своевременно проинформировать об утечке персональных данных, принять меры по установлению порядка доступа к таким персональным данным).

Несмотря на закрепление перечня обязательных мер, подлежащих принятию любым оператором (за некоторым исключением), глубина реализации таких мер определяется с учетом деятельности конкретного оператора, что также является отражением риск-ориентированного подхода.

При осуществлении контрольных мероприятий учитывается эффективность принимаемых мер. В этой связи формальный подход к их принятию и исполнению является недопустимым (например, назначение лица, ответственного за осуществление внутреннего контроля, без реального осуществления такого контроля).

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

3. В п. 3 комментируемой статьи закрепляются обязательные меры по обеспечению защиты персональных данных, которые подлежат исполнению всеми операторами (уполномоченными лицами), независимо от их размера, формы собственности и количества обрабатываемых персональных данных.

3.1. Назначение ответственного за осуществление внутреннего контроля за обработкой персональных данных.

Институт ответственного за осуществление внутреннего контроля за обработкой персональных данных (далее в данной статье – ответственный за контроль) представляет собой один из основных

инструментов обеспечения надлежащего соблюдения обязанностей, возложенных на операторов (уполномоченных лиц) Законом.

В любой организации ежедневно принимается множество решений, связанных со сбором персональных данных, их предоставлением третьим лицам, использованием таких данных для принятия решений и др., ошибки в которых могут влечь нарушение прав субъектов персональных данных, а также создавать предпосылки для привлечения организации к ответственности. В этой связи основная цель ответственного за контроль – предотвращение возможных нарушений со стороны оператора (уполномоченного лица). Ведь в большинстве случаев допускаемые нарушения являются не столько следствием умысла, сколько ошибочного представления о допустимых пределах обработки персональных данных.

В этой связи крайне важно иметь возможность оперативных консультаций с лицом, которое может дать квалифицированную оценку складывающимся отношениям и не допустить возможного нарушения законодательства. В этих целях для наиболее крупных операторов, чья деятельность связана с масштабной обработкой персональных данных (банки, страховые организации, риэлтерские агентства и др.), устанавливаются специальные требования к обучению ответственных за контроль в Национальном центре защиты персональных данных.

Закон не перечисляет конкретных функций ответственных за контроль. Соответствующие функции перечислены в Едином квалификационном справочнике должностей служащих (ЕКСД) «Должности служащих для всех видов деятельности», утвержденном постановлением Министерства труда Республики Беларусь от 30 декабря 1999 г. № 159, куда включена квалификационная характеристика специалиста по внутреннему контролю за обработкой персональных данных.

Так, на указанного специалиста возлагаются функции, которые можно разделить на следующие блоки:

организационные *(*изучение и анализ процессов обработки персональных данных, определение рисков, связанных с процессами обработки персональных данных, выработка предложений по их минимизации, разработка и поддержание в актуальном состоянии документов, определяющих политику оператора в отношении обработки персональных данных, порядка доступа к персональным данным, иных документов (форм) по вопросам обработки персональных данных, разработка формы реестра персональных данных и координация его ведения, участие в определении и осуществлении мер технической и криптографической защиты персональных данных и т.п.)*;*

консультативные (консультирование работников и уполномоченных лиц по вопросам обработки и защиты персональных данных, согласование локальных правовых актов, договоров на предмет их соответствия законодательству о персональных данных, ознакомление работников с законодательством о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных и т.п.);

контрольные (осуществление контроля за своевременным внесением работниками изменений в персональные данные, которые являются неполными, устаревшими или неточными, прекращением обработки персональных данных, а также осуществлением их удаления или блокирования при отсутствии оснований для обработки персональных данных, предусмотренных законодательными актами; проведение проверки по соблюдению требований законодательства о персональных данных в структурных подразделениях организации для выявления нарушений и предупреждения их возникновения, проведение расследования по нарушениям работниками требований обработки персональных данных, внесение предложений по привлечению виновных к ответственности и т.п.);

информационно-образовательные (организация прохождения обучения работников, осуществляющих обработку персональных данных, по вопросам обработки и защиты персональных данных в порядке, установленном законодательством, поиск оптимальных форм обучения работников, исходя из их трудовых функций и т.п.);

иные функции, связанные с обеспечением комплексной работы по соблюдению законодательства о персональных данных (рассмотрение (участие в рассмотрении) заявлений и жалоб субъектов персональных данных по вопросам обработки персональных данных, принятие необходимых мер по восстановлению их нарушенных прав, обеспечение взаимодействия с Национальным центром защиты персональных данных, в том числе по вопросам уведомления о нарушениях систем защиты персональных данных, исполнения требований по защите прав субъектов персональных данных об устранении нарушений законодательства о персональных данных и т.п.).

Учитывая, что принимаемые меры по обеспечению защиты персональных данных зависят в том числе от сферы деятельности, объема обрабатываемых персональных данных, требования к наличию у лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных, конкретного образования не установлены. В соответствии с квалификационной характеристикой

специалист по внутреннему контролю за обработкой персональных данных должен иметь высшее образование.

Вместе с тем с учетом возлагаемых на данных лиц функций такое лицо должно назначаться с учетом знания законодательства о персональных данных (что, как правило, предполагает наличие юридического образования) и практики его применения, а также способности выполнять функции, возложенные на данное лицо.

Ответственный за контроль назначается государственным органом, юридическим лицом Республики Беларусь, иной организацией. Оператор (уполномоченное лицо) из числа физических лиц, включая индивидуальных предпринимателей, адвокатов, нотариусов, ремесленников, репетиторов, медиаторов и др., такое лицо не назначает.

Одним из наиболее распространенных вопросов среди операторов является вопрос о вариантах назначения ответственного за контроль, поскольку Закон не предусматривает конкретных моделей или критериев назначения соответствующего лица, что объясняется разнообразием условий функционирования и возможностей операторов. При этом избираемая модель должна соответствовать цели назначения такого лица и позволять ему выполнять возлагаемые на него функции. С учетом изложенного при назначении ответственного за контроль рекомендуется воспользоваться одним из следующих вариантов:

создать отдельное структурное подразделение. Такую модель, как правило, следует избирать крупным операторам, осуществляющим масштабную обработку персональных данных, в том числе трансграничную передачу, и имеющим множество информационных ресурсов, содержащих персональные данные (банки, операторы электросвязи, страховые организации, крупные торговые сети и др.). В состав таких подразделений целесообразно включать не только юристов, но и лиц, имеющих техническое образование, в целях комплексного анализа бизнес-процессов, связанных с обработкой персональных данных;

назначить освобожденного работника. Условия реализации данной модели во многом схожи с условиями создания соответствующего структурного подразделения. При этом масштаб организации (масштаб обработки персональных данных) не такой значительный, что позволяет выполнять функции ответственного за контроль одному лицу.

возложить дополнительные функции на одного из работников. Такой вариант выбирается, когда организация небольшая и в информационных системах (ресурсах), которыми она владеет, обрабатывается незначительное количество персональных данных. Для такого лица обработка персональных данных не должна быть основным видом деятельности, что призвано исключить потенциальный

конфликт интересов. В связи с этим следует исключить назначение ответственного за осуществление внутреннего контроля из числа руководителей организации (их заместителей), а также структурных подразделений или работников, основные функции которых связаны с обработкой большого объема персональных данных (например, кадровые и бухгалтерские службы, структурные подразделения по обращениям граждан и т.п.). Кроме того, у назначенного работника должна быть объективная возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей. С учетом задач ответственного за контроль не соответствует Закону практика тех организаций, где соответствующие функции возлагаются исключительно на ответственного за обеспечение защиты информации или инженера (программиста, системного администратора, специалиста по информационной безопасности и т.п.);

возложить дополнительные функции на нескольких работников. Как правило, при такой модели функции ответственного за контроль возлагаются на двух работников: на одного (например, юрисконсульт) – в части организационных и правовых мер; на другого (например, специалист по информационной безопасности) – в части мер по технической и криптографической защите персональных данных. При таком варианте требуется четкое распределение функций между указанными лицами, исключение противоречий в их деятельности. Как и в предыдущем варианте, у назначенного работника должна быть объективная возможность выполнять соответствующие функции с учетом уже имеющихся должностных обязанностей.

Не соответствует цели введения рассматриваемого института практика тех организаций, в которых лица, ответственные за осуществление внутреннего контроля за обработкой персональных данных, назначаются в каждом структурном подразделении. Это приводит к сложностям при их взаимодействии, конкуренции, возможности появления различных подходов по реализации законодательства о персональных данных в различных подразделениях, а также может приводить к конфликту интересов.

Важно также отграничивать деятельность ответственного за контроль от схожей, но не идентичной деятельности ответственного за обеспечение защиты информации. Ответственный за контроль действует в соответствии с законодательством о персональных данных, обязан проходить обучение по вопросам защиты персональных данных, в основном взаимодействует с работниками, клиентами, регуляторами и проверяет наличие правовых оснований на обработку персональных данных и иные требования к обработке персональных данных. Ответственный за обеспечение защиты информации действует

в соответствии с законодательством об информации, информатизации и защите информации, должен иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование, пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации и в основном проверяет работу оборудования и программного обеспечения на соответствие требованиям информационной безопасности.

В целях надлежащего выполнения организацией возложенных Законом обязанностей рекомендуется обеспечить независимость ответственного за контроль и необходимые условия для осуществления его функций посредством:

предоставления доступа к документам и информации, в том числе обрабатываемой в информационных системах (ресурсах) в объеме, необходимом для выполнения возложенных на него обязанностей;

организации непосредственной подчиненности руководителю организации или его заместителю.

Следует учитывать, что формальное выполнение этой меры по защите персональных данных (факт назначения) без реальной деятельности такого лица (проведения фактического контроля, ведения реестра обработок, консультирования и др.) не рассматривается как надлежащее выполнение обязанности, предусмотренной абзацем вторым п. 3 ст. 17 Закона, и является основанием для привлечения юридического лица к административной ответственности согласно ч. 4 ст. 23.7 КоАП. В этой связи наряду с назначением ответственного за контроль необходимо разработать порядок осуществления внутреннего контроля за обработкой персональных данных, включающий периодичность и формат контрольных мероприятий, их оформление и порядок принятия решений по результатам таких мероприятий.

Нередко на практике возникает вопрос о допустимости привлечения ответственного за контроль по гражданско-правовому договору. Такая модель не согласуется с положениями Закона. Вместе с тем это не исключает возможности привлечения иных лиц на основании гражданско-правового договора для оказания содействия в выполнении отдельных функций ответственного за контроль (например, для разработки документов, определяющих политику в отношении обработки персональных данных, и иных документов, проведения обучения работников и иных лиц, непосредственно осуществляющих обработку персональных данных по вопросам защиты персональных данных).

Важно учитывать, что в связи с назначением ответственного за контроль ни оператор, ни уполномоченное лицо, ни работники, непосредственно осуществляющие обработку персональных данных, не освобождаются от ответственности, предусмотренной законодательством.

3.2. Издание документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных (далее в рамках статьи – Политика), направлено на реализацию принципа прозрачности обработки персональных данных (п. 6 ст. 4 Закона).

Поскольку во многих случаях персональные данные обрабатываются без согласия субъекта персональных данных и зачастую получаются от третьей стороны без ведома субъекта персональных данных, цель издания Политики – это предоставление субъектам персональных данных информации об обработке их персональных данных, чтобы исключить неосведомленность субъекта персональных данных относительно действий с его персональными данными. С этой целью в Политике должно содержаться разъяснение того, кем, как и для каких целей персональные данные собираются, используются или иным образом обрабатываются, а также информирование об имеющихся у субъектов персональных данных правах в контексте этой обработки и механизме их реализации. Такая информация необходима для возможности совершения информированного выбора (например, давать или не давать согласие) и создания условий для осознанной реализации и защиты своих прав.

В целях реализации принципа прозрачности в Политике подлежат отражению бизнес- и иные процессы оператора, в ходе которых осуществляется обработка персональных данных. Указанные процессы раскрываются путем перечисления целей и правовых оснований обработки персональных данных, категорий субъектов персональных данных, чьи данные подвергаются обработке, а также перечня обрабатываемых персональных данных, порядка и условий их обработки, в том числе срока хранения персональных данных, прав субъектов персональных данных.

Требование о прозрачном характере обработки персональных данных достигается путем соотношения в Политике целей обработки, категорий субъектов персональных данных, чьи данные подвергаются обработке, перечня обрабатываемых персональных данных. Иной подход, например, часто выявляемое при осуществлении контроля ”механическое“ перечисление целей обработки без их соотношения с перечнем персональных данных не позволит субъекту персональных данных уяснить, какие его персональные данные и для каких целей

обрабатываются, что делает Политику документом, который лишен для субъекта персональных данных практической пользы.

По этой же причине в Политике неприемлемо указывать слишком общие цели обработки либо их открытый перечень, неконкретные сроки, неисчерпывающий перечень обрабатываемых персональных данных и т.п.

Справочно:

Схожий подход закреплен и в Российской Федерации. Так, в июне 2022 г. в Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" внесены изменения, направленные на необходимость определения для каждой цели обработки персональных данных категории и перечня обрабатываемых персональных данных, категорий субъектов, персональные данные которых обрабатываются, способов, сроков их обработки и хранения.

Типичные нарушения (недостатки) при подготовке Политики:

не отражены все бизнес- и иные процессы, в ходе которых осуществляется обработка персональных данных;

не обеспечено соотношение целей обработки, правовых оснований, категорий субъектов персональных данных, чьи данные подвергаются обработке, и перечня обрабатываемых персональных данных;

излишнее дублирование положений Закона, приведение положений, изложенных с учетом подходов российского законодательства, использование "типовых" политик;

указание слишком общих либо неконкретных целей обработки (обеспечение соблюдения законодательства, осуществление деятельности в соответствии с уставом);

отсутствие ссылок на правовые основания обработки;

отсутствие сроков обработки персональных данных либо указание неконкретных сроков ("не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных установлен законодательством", "согласие действует до момента отзыва этого согласия либо до момента, установленного законодательством");

отсутствие информации о механизме реализации прав субъектов персональных данных, в том числе о лице, ответственном за осуществление внутреннего контроля;

несоответствие положений Политики реальным процессам;

несогласованность положений Политики и прямое противоречие их друг другу;

опубликование на разных страницах интернет-сайта разных версий Политики;

возложение на субъектов персональных данных обязанностей, не предусмотренных Законом (досудебный порядок разрешения споров, обязанность уведомления об изменении персональных данных)[19].

3.3. Ознакомление работников оператора (уполномоченного лица) и иных лиц, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных, а также обучение указанных работников и иных лиц в порядке, установленном законодательством.

Реализация рассматриваемой меры направлена на уяснение соответствующими лицами сути возлагаемых на них обязанностей, связанных с обработкой персональных данных, и исключение ссылок на незнание как на оправдание допускаемых нарушений.

Данная обязанность распространяется как на действующих, так и на вновь принимаемых работников. Таким образом, реализация комментируемой обязанности не может рассматриваться как некая единовременная кампания, но должна являться постоянно действующим механизмом.

Комментируемая норма включает в себя несколько самостоятельных мероприятий:

ознакомление с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Такое ознакомление не может быть простой отсылкой к Закону, размещенному на сайте или в сетевом ресурсе. Оно должно касаться тех положений актов законодательства, которые имеют отношение к функциям конкретного работника. Иными словами, ознакомление должно носить ”адресный“ характер, поскольку для разных категорий работников (например, для сотрудников кадрового подразделения и подразделения по маркетингу) будут иметь значение различные институты законодательства. В этой связи важная роль в реализации данной меры отводится лицу, уполномоченному на осуществление внутреннего контроля за обработкой персональных данных.

Ознакомление осуществляется с:

положениями законодательства о персональных данных. Это Закон, иные акты, имеющие значение для выполнения функций конкретным

[19] Подробнее см. Рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица) в отношении обработки персональных данных, размещенные на официальном интернет-сайте Центра.

работником. Например, для работников маркетингового подразделения актуальными являются соответствующие положения Закона Республики Беларусь от 10 мая 2007 г. № 225-З ”О рекламе“. Кроме того, целесообразно доводить информацию о мерах ответственности, предусмотренных ТК, КоАП и УК;

требованиями по защите персональных данных. Это меры, предусмотренные ст. 17 Закона, а также иные меры, предусмотренные законодательством;

документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных.

Ознакомление должно осуществляться в отношении:

работников оператора (уполномоченного лица), непосредственно осуществляющих обработку персональных данных. Данная мера распространяется на всех лиц, которые в силу своих трудовых обязанностей осуществляют обработку персональных данных. При этом не имеет значения ни частота такой обработки, ни объем обрабатываемых персональных данных;

иных лиц, непосредственно осуществляющих обработку персональных данных. Это лица, которые работают в организации по гражданско-правовому договору, но не признаются уполномоченными лицами (*подробнее см. комментарий к термину ”уполномоченное лицо“ в ст. 1*).

Порядок ознакомления (ознакомление под роспись и др.) определяет сам оператор (уполномоченное лицо).

Распространенные ошибки при реализации этой меры:

ознакомление с информацией лишь отдельных работников, которые обрабатывают персональные данные (чаще всего – сотрудников кадровой службы);

ознакомление с неполным объемом требуемой информации (например, только с Законом и документами, определяющими политику оператора (уполномоченного лица) в отношении обработки персональных данных);

ознакомление с информацией, которая не имеет отношения к выполняемым функциям лица (например, ознакомление менеджера с информацией, касающейся, прежде всего, работников бухгалтерии);

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

Само по себе ознакомление с информацией об обработке персональных данных может не дать желаемого результата как в силу различного образования у работников, так и в силу различных способностей людей самостоятельно воспринимать информацию.

В этой связи мера по ознакомлению с информацией об обработке персональных данных дополняется Законом требованием об организации обучения соответствующих лиц.

Порядок такого обучения, в том числе его периодичность, определен в подп. 3.3 п. 3 Указа № 422.

Так, операторы (уполномоченные лица) должны организовывать не реже одного раза в 5 лет прохождение обучения по вопросам защиты персональных данных лиц, ответственных за осуществление внутреннего контроля за обработкой персональных данных, а также лиц, непосредственно осуществляющих обработку персональных данных, по вопросам защиты персональных данных:

в Национальном центре защиты персональных данных по образовательной программе повышения квалификации руководящих работников и специалистов – в отношении категорий лиц, определенных Оперативно-аналитическим центром при Президенте Республики Беларусь;

в учреждениях образования, а также иных организациях, которым предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов, по образовательной программе повышения квалификации руководящих работников и специалистов, либо в других организациях по образовательной программе обучающих курсов (лекториев, тематических семинаров, практикумов, тренингов, офицерских курсов и иных видов обучающих курсов), либо у оператора (уполномоченного лица) путем изучения установленных требований в области защиты персональных данных и проверки им знаний по вопросам защиты персональных данных (в виде собеседования, опроса, тестирования и других форм контроля знаний) – в отношении иных лиц.

Категории лиц, обучаемых непосредственно в Национальном центре защиты персональных данных, определены приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 194 ”Об обучении по вопросам защиты персональных данных“. Это лица, ответственные за осуществление внутреннего контроля за обработкой персональных данных, выполняющие эти функции:

в банках и небанковских кредитно-финансовых организациях;

в страховых организациях;

у операторов электросвязи (за исключением индивидуальных предпринимателей);

в республиканской и территориальных организациях по государственной регистрации недвижимого имущества, прав на него и сделок с ним;

в Белорусской нотариальной палате, областных (Минской городской) нотариальных палатах;

в риэлтерских организациях;

в организациях здравоохранения;

в местных исполнительных и распорядительных органах (за исключением сельских (поселковых) исполнительных комитетов), их структурных подразделениях с правами юридического лица;

у операторов (уполномоченных лиц), организующих и (или) осуществляющих обработку персональных данных не менее 10 тыс. физических лиц, за исключением персональных данных работников этих операторов (уполномоченных лиц) в процессе осуществления трудовой (служебной) деятельности. Указанный количественный критерий (обработка персональных данных не менее 10 тыс. физических лиц) не ограничен дополнительными временными критериями (например, обработка в течение только текущего календарного года). Необходимо принимать во внимание все категории лиц, в отношении которых оператором в текущем периоде осуществляется обработка персональных данных (включая хранение), в том числе клиентов в процессе предыдущей деятельности оператора.

Лица, непосредственно осуществляющие обработку персональных данных в названных организациях, могут пройти обучение как в Национальном центре защиты персональных данных, так и у иных лиц, указанных в подп. 3.3 п. 3 Указа № 422.

Если же операторы (уполномоченные лица) не относятся к категории субъектов, обязанных обеспечить прохождение обучения в Национальном центре защиты персональных данных, они организуют прохождение обучения по вопросам защиты персональных данных в учреждениях образования, а также в иных организациях, которым предоставлено право реализации образовательной программы повышения квалификации руководящих работников и специалистов, в других организациях по образовательной программе обучающих курсов, у оператора (уполномоченного лица), то есть в самой организации, где трудятся лица, осуществляющие обработку персональных данных.

3.4. Установление порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе).

При разработке порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе), операторам и уполномоченным лицам следует отразить различия в предоставлении такого доступа к документам в информационных ресурсах и к документам в бумажном виде.

Доступ к персональным данным, отраженным в документах в бумажном виде, можно ограничить посредством организации мест их хранения. Доступ к персональным данным, обрабатываемым в цифровом виде, может быть ограничен посредством настроек программного обеспечения.

Отсутствие такого порядка приводит к тому, что доступ к персональным данным имеют работники, должностные обязанности которых не связаны с обработкой персональных данных.

Порядок доступа к персональным данным целесообразно закрепить в одном документе, но отдельные его положения могут быть детализированы в иных документах, в том числе положениях об информационных ресурсах (системах), о видеонаблюдении, о контроле управления доступом в помещения организации.

Важно подчеркнуть, что порядок доступа к персональным данным должен основываться на принципе предоставления минимально необходимого уровня доступа к персональным данным исключительно в целях выполнения работником своих должностных обязанностей, а уполномоченными лицами – обязательств, определенных договором, решением государственного органа или актом законодательства.

Кроме того, со временем могут понадобиться изменения в правах доступа к персональным данным в случаях перевода работника на другую должность, его увольнения, а также изменения условий договора с уполномоченным лицом (решения государственного органа, акта законодательства), окончания срока действия или расторжения этого договора (утраты силы решения государственного органа, акта законодательства).

Может возникнуть также ситуация, когда необходимо предоставить временный правомерный доступ к персональным данным работнику (иному лицу). Например, в целях подготовки отчета, справки, проведения контроля, аудита. Механизм предоставления такого временного доступа также следует закрепить в порядке доступа к персональным данным.

Работники или представители уполномоченного лица могут случайно получить доступ к персональным данным в результате компьютерных сбоев или иных стечений обстоятельств. Модель поведения в этой ситуации также целесообразно описать, чтобы своевременно выявить и устранить недостатки в подходах к обработке персональных данных.

Определение целей обработки и категорий персональных данных позволит упростить распределение доступа к персональным данным относительно занимаемых должностей (оказываемых услуг, выполняемых работ). Однако нецелесообразно осуществлять распределение доступа к персональным данным на поименной основе

ввиду постоянного движения кадров и корректировок в связи с изменениями бизнес-процессов.

3.5. Шестой абзац п. 3 комментируемой статьи предусматривает необходимость *осуществления технической и криптографической защиты персональных данных в порядке, установленном ОАЦ, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные*.

Требование защиты персональных данных от несанкционированного доступа является характерной чертой любого государства, в котором регулируются вопросы обработки персональных данных. В Беларуси указанные требования предусмотрены тремя ключевыми нормативными правовыми актами, которые регулируют техническую защиту любой информации, распространение и (или) предоставление которой ограничено, не отнесенной в установленном порядке к государственным секретам.

Основу соответствующего правового регулирования составляет Закон ”Об информации, информатизации и защите информации“. Им предусматривается необходимость использования системы защиты информации, которая создается в порядке, определяемом ОАЦ. Система защиты информации представляет собой совокупность правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации, распространение и (или) предоставление которой ограничено, в том числе и персональных данных.

Вопросы защиты информации получают свое развитие в Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 ”О некоторых мерах по совершенствованию защиты информации“. Этот нормативный правовой акт детализирует требования к собственникам (владельцам) информационных систем, обрабатывающим информацию, распространение и (или) предоставление которой ограничено. Например, закрепляется требование об использовании средств защиты информации, имеющих сертификат соответствия, выданный в национальной системе подтверждения соответствия. Кроме того, уточняется, что осуществлять мероприятия по осуществлению технической защиты информации должны ответственные сотрудники (подразделения) собственника (владельца) информационной системы либо организации, имеющие лицензию на осуществление данной деятельности.

Конкретные технические требования к защите информации, в том числе и персональных данных, определяются Приказом № 66, которым утверждено Положение о технической и криптографической защите информации, распространение и (или) предоставление которой

ограничено, не отнесенной в установленном порядке к государственным секретам.

После реализации вышеуказанных мер проводится аттестация системы защиты информации, которая представляет из себя окончательную проверку корректности выполнения мероприятий по технической защите. Успешное прохождение данной проверки позволяет получить аттестат соответствия, срок действия которого составляет 5 лет.

Важно отметить, что в Приказе № 66 наряду с общей процедурой предусматривается упрощенная процедура проектирования и аттестации системы защиты информации. Речь идет о ситуациях, когда функционирование такой системы осуществляется на основе информационной системы, уже имеющей аттестованную систему защиты информации, владелец которой и проводит все необходимые мероприятия.

Закрепленные в Приказе № 66 требования являются типовыми мерами, которые присущи и аналогичным нормативным правовым актам зарубежных стран. Существенным отличием является лишь необходимость проведения обязательной процедуры аттестации, тогда как в зарубежных странах действует принцип декларирования.

Конкретные требования к технической и криптографической защите персональных данных при их обработке в информационных системах зависят от класса информационной системы. Это вытекает из требований комментируемой нормы о том, что ОАЦ определяет порядок технической и криптографической защиты персональных данных в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Такая классификация, исходя из положений п. 5 ст. 17 Закона, устанавливается уполномоченным органом по защите прав субъектов персональных данных. В развитие указанной нормы принят приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 12 ”О классификации информационных ресурсов (систем)“. Данным приказом установлено, что информационные ресурсы (системы), содержащие персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных подразделяются на информационные ресурсы (системы), содержащие:

общедоступные персональные данные;

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

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными.

На основании данной классификации в Приказе № 66 в отношении обработки персональных данных выделены следующие классы типовых информационных систем:

класс 4-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных;

класс 4-спец – информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных;

класс 4-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных;

класс 3-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных;

класс 3-спец – информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных;

класс 3-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.

В свою очередь, в приложении 3 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному Приказом № 66, применительно к указанным классам типовых информационных систем установлены конкретные требования к системе защиты информации, которые подлежат включению в техническое задание.

Данные требования представлены в виде нескольких групп технических мер. К основным мерам относятся:

необходимость осуществления защиты от вредоносного программного обеспечения, которое должно выявляться как на рабочих местах пользователей информационной системы, так и в сервисах обмена электронной почты;

мониторинг событий информационной безопасности. Указанный мониторинг необходим для своевременного выявления инцидентов

и позволяет минимизировать последствия от неправомерного воздействия на информационный ресурс (систему);

осуществление собственниками (владельцами) информационных ресурсов (систем) резервирования информации;

разграничение доступа пользователей (что коррелирует с требованиями Закона);

отдельное внимание уделяется процессам безопасной настройки объектов и их непрерывного обновления до наиболее актуальных версий программного обеспечения.

Следует также учитывать, что требования Приказа № 66 не распространяются на собственников (владельцев) информационных систем, в которых обрабатываются только общедоступные персональные данные.

4. На операторе лежит обязанность обеспечить неограниченный доступ, в том числе с использованием глобальной компьютерной сети Интернет, к документам, определяющим политику оператора (уполномоченного лица) в отношении обработки персональных данных, до начала такой обработки.

Реализация указанного требования должна осуществляться с учетом круга субъектов персональных данных, на которых она распространяется. Так, Политика оператора в отношении ”внешнего контура“ (клиентов, контрагентов, граждан, направляющих обращения, и т.п.) размещается в сети Интернет на интернет-сайте оператора. Такая информация должна быть опубликована на странице не ниже второго уровня, а также дополнительно может размещаться на иных интернет-ресурсах или распространяться другими способами. При отсутствии у оператора (уполномоченного лица) сайта обеспечение неограниченного доступа к Политике осуществляется посредством ее размещения на информационных стендах или иными способами.

В случае, если у оператора несколько сайтов, то целесообразно публиковать Политику на каждом из них (а в случае подготовки нескольких Политик по отдельным направлениям – Политику применительно к бизнес-процессу, связанному с данным сайтом).

Иной подход может быть применен в отношении политики оператора в отношении работников. Такой документ нет необходимости размещать в открытом доступе для неограниченного круга лиц. В этом случае допустимо опубликовать соответствующий документ на корпоративном портале (при его наличии), а также на информационных стендах.

ГЛАВА 4
УПОЛНОМОЧЕННЫЙ ОРГАН ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ЗАКОНА

Статья 18. Уполномоченный орган по защите прав субъектов персональных данных

Комментарий к статье 18

1. Пункты 1 и 2 рассматриваемой статьи предусматривают необходимость наличия в стране уполномоченного органа, призванного принимать меры по защите прав субъектов персональных данных и действующего на основании актов законодательства независимо от иных структур.

Такой подход, принятый законодателем, не является чем-то новым в мировой практике.

Современный век характеризуется стремительным развитием информационных технологий, ростом складывающихся между организациями, гражданами и странами потоков информации, содержащей персональные данные. Новые способы и возможности их обработки постоянно порождают в отношении личной сферы людей ранее не встречавшиеся вопросы и риски.

Они отличаются разнообразием, зависят в каждом случае от конкретных обстоятельств и требуют оперативного реагирования, поскольку цифровые следы ”затираются“ очень быстро. Урегулирование таких проблем в законодательстве всегда требует определенного времени. Учитывая это, а также ”точечный“ характер многих ситуаций, их разрешение в нормативном порядке далеко не всегда является возможным и целесообразным.

Наиболее быстрое, эффективное и гибкое реагирование на возникающие вопросы при обработке персональных данных обеспечивается функционированием уполномоченного органа по их защите, ответственного за надлежащее единообразное применение законодательства и осуществление контроля в этой сфере.

При этом поскольку персональные данные обрабатываются юридическими лицами всех форм собственности, в том числе государственными органами и иными организациями, относящимися ко всем ветвям власти (законодательной, исполнительной и судебной), а также гражданами, деятельность такого органа с целью недопущения конфликта интересов должна носить беспристрастный и независимый характер.

Предоставление такой независимости является не привилегией, а необходимым инструментом реализации полномочий, возлагаемых на уполномоченный орган. Ее гарантии обеспечиваются законодательным закреплением государством права принятия решений независимо от любого прямого или косвенного воздействия извне, процедуры назначения руководителя и выделением достаточного количества ресурсов для бесперебойной работы этого органа.

На основании Дополнительного протокола к Конвенции о защите физических лиц при автоматизированной обработке персональных данных уполномоченные органы по защите персональных данных сформированы и действуют в государствах, присоединившихся к данной Конвенции. Аналогичный подход реализован и в большинстве иных стран, в которых приняты единые акты в области защиты персональных данных, например, в Канаде, Австралии, Новой Зеландии, Молдове, а также в государствах Евразийского экономического союза.

Такие органы создаются как в виде специализированных структур, деятельность которых по защите персональных данных является для них основной (например, в Кыргызстане, Армении), так и органов, которыми выполнение данной задачи совмещается с выполнением возложенных на них иных полномочий (например, в Российской Федерации).

В нашей республике 15 ноября 2021 г. в соответствии с Указом № 422 образован специализированный уполномоченный орган по защите персональных данных – Национальный центр защиты персональных данных Республики Беларусь. Его учредителем и государственным органом, осуществляющим от имени Республики Беларусь права собственника имущества Центра, является Оперативно-аналитический центр при Президенте Республики Беларусь.

Центр занимает самостоятельное место в системе органов и иных организаций. Он является юридическим лицом, действует в форме государственного учреждения на основании Конституции, Закона, Положения и иных актов законодательства.

В соответствии с п. 2 Положения Центр осуществляет предоставленные ему полномочия независимо от иных органов и организаций. Возложение на него функций, несовместимых с обработкой персональных данных и защитой прав их субъектов, не допускается.

Финансирование Центра производится как за счет средств республиканского бюджета, так и средств от приносящей доходы деятельности и иных источников, не запрещенных законодательством (п. 34 Положения).

Возглавляет Центр директор, который руководит его деятельностью, осуществляет иные полномочия, связанные

с непосредственным руководством Центром, и несет персональную ответственность за выполнение возложенных на него основных задач и функций. Назначение директора на должность и освобождение от нее осуществляется Главой государства.

В целях оказания Центру содействия в реализации им своих полномочий при нем на общественных началах создан консультативный совет. Его деятельность направлена на обеспечение соблюдения операторами и гражданами законодательства о персональных данных, выработку предложений и рекомендаций по его совершенствованию, формирование единообразной правоприменительной деятельности, распространение положительного опыта защиты прав субъектов персональных данных, а также на осуществление анализа практики осуществления контроля за обработкой персональных данных операторами. Персональный состав совета, порядок его организации и функционирования установлены директором Центра. В настоящее время в состав совета входят представители государственных органов и иных организаций, научного и бизнес-сообществ.

2. Пункт 3 рассматриваемой статьи определяет полномочия Центра, которые закреплены также главой 2 Положения.

На Центр возложены две основные задачи:

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

организация обучения по этим вопросам.

Названные основные задачи раскрываются выполняемыми Центром функциями и предоставленными для их реализации правами.

Значительный их объем связан с осуществлением контрольных мероприятий за соблюдением законодательства о персональных данных (абзацы второй – четвертый комментируемого пункта).

Так, Центр осуществляет контроль за обработкой персональных данных операторами (уполномоченными лицами) (далее в рамках статьи – контроль) и рассматривает жалобы субъектов персональных данных по вопросам их обработки.

Проведение контроля является самостоятельным видом осуществляемой в стране контрольной деятельности и в его отношении не применяются положения Указа № 510 (абзац тридцать седьмой п. 23 этого Указа).

Правила проведения контроля определены главой 4 Положения, согласно которой он осуществляется в форме плановых (в соответствии с ежегодно утверждаемым директором Центра планом), внеплановых (без включения в названный план) и камеральных (проводимых по месту нахождения Центра) проверок соблюдения законодательства о персональных данных.

При этом внеплановые проверки могут назначаться директором Центра при наличии информации (кроме анонимной), в том числе полученной от организации или гражданина, а также жалоб субъектов персональных данных, свидетельствующих о совершаемом (совершенном) нарушении требований законодательства о персональных данных (*подробнее о рассмотрении жалоб см. в комментарии к ст. 15 Закона*).

При выявлении по итогам деятельности операторов (уполномоченных лиц) нарушений законодательства о персональных данных Центр уполномочен выносить им письменные требования (предписания) об устранении таких нарушений и (или) приостановлении (прекращении) обработки персональных данных в информационном ресурсе (системе), т.е. фактически приостанавливать его (ее) работу на срок до шести месяцев.

Установление в деятельности операторов или иных лиц признаков административных правонарушений или уголовно наказуемых деяний может влечь направление соответствующих материалов в правоохранительные органы для решения вопроса о привлечении виновных соответственно к административной или уголовной ответственности *(см. комментарий к ст. 19 Закона)*.

Характерной особенностью осуществляемых Центром контрольных мероприятий является возможность проведения им камеральных проверок. Они организовываются по месту нахождения Центра без выдачи предписаний на их проведение, уведомления и выезда к проверяемым субъектам. При этом изучаются, анализируются и оцениваются документы и информация, размещенные в средствах массовой информации, Интернете (сайтах, мессенджерах и т.п.) или полученные по запросам Центра от операторов (уполномоченных лиц), на предмет соответствия деятельности последних законодательству о персональных данных.

Рассматриваются, в частности, вопросы наличия либо отсутствия компетенции на обработку персональных данных, выполнения обязательных мер, предусмотренных Законом (издание документов, определяющих политику в отношении обработки персональных данных, назначение лиц, ответственных за осуществление внутреннего контроля за их обработкой, и т.п.), а также размещения в открытых ресурсах личной информации о гражданах в нарушение законодательства о персональных данных (списков должников, членов товариществ собственников и т.п.).

По результатам таких проверок операторам (уполномоченным лицам) могут быть направлены рекомендации об устранении выявленных

нарушений законодательства о персональных данных либо, при наличии оснований, назначены их внеплановые проверки.

К контрольному блоку полномочий Центра относится также предоставленное абзацем четвертым комментируемого пункта право требовать от операторов и уполномоченных ими лиц (независимо от назначения плановых, внеплановых, камеральных проверок в их отношении или рассмотрения жалоб) изменения, блокирования или удаления недостоверных или полученных незаконным путем персональных данных, устранения иных нарушений законодательства о персональных данных.

В развитие этой нормы в соответствии с абзацем седьмым п. 8 Положения Центр наделен компетенцией требовать от названных лиц прекращения обработки персональных данных при невозможности обеспечить защиту прав субъектов персональных данных иными способами. Невыполнение этого требования влечет административную ответственность.

Центр в соответствии с абзацами пятым и шестым комментируемого пункта, а также абзацами четвертым, пятым, восьмым и девятым п. 7 Положения принимает обязательные для применения правовые акты, необходимые для реализации Закона.

Так, в частности, Центром определяется перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных, выдаются разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных, а также определяется порядок выдачи таких разрешений.

Эти вопросы урегулированы приказом директора Центра от 15 ноября 2021 г. № 14 ”О трансграничной передаче персональных данных“, согласно которому в названный перечень включены иностранные государства, являющиеся сторонами Конвенции о защите физических лиц при автоматизированной обработке персональных данных, а также иностранные государства, являющиеся членами Евразийского экономического союза.

Кроме того, Центр определяет случаи, когда операторам не требуется уведомлять его о нарушениях систем защиты персональных данных. В соответствии с приказом директора Центра от 15 ноября 2021 г. № 13 ”Об уведомлении о нарушениях системы защиты персональных данных“ оно направляется оператором незамедлительно, но не позднее трех рабочих дней после того, как ему стало известно о таких нарушениях.

Уведомление не направляется, если нарушение систем защиты не привело к незаконному распространению, предоставлению персональных данных, их изменению, блокированию либо удалению без возможности восстановления доступа к ним.

Центр также наделен компетенцией устанавливать классификацию информационных ресурсов (систем), содержащих персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных. Приказом директора Центра от 15 ноября 2021 г. № 12 ”О классификации информационных ресурсов (систем)“ они подразделяются на информационные ресурсы (системы), содержащие:

общедоступные персональные данные;

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

биометрические и генетические персональные данные;

персональные данные, не являющиеся общедоступными или специальными.

Центр уполномочен участвовать в подготовке проектов актов законодательства о персональных данных и вносить предложения о его совершенствовании (абзац седьмой комментируемого пункта, абзац шестой п. 7 Положения).

Это право реализуется Центром посредством внесения в нормотворческие органы инициатив о принятии или корректировке нормативных правовых актов по вопросам, связанным с защитой персональных данных, участием в деятельности соответствующих рабочих групп, рабочих совещаниях, дачей заключений по направляемым на рассмотрение в Центр проектам актов законодательства и иных формах.

Абзацем восьмым рассматриваемого пункта Центр наделен компетенцией давать разъяснения по вопросам применения законодательства о персональных данных и проводить иную разъяснительную работу об этом законодательстве.

Нормативными правовыми актами не установлены требования к форме и содержанию подготавливаемых Центром разъяснений. Они отражают официальную позицию по существу рассмотренных им вопросов и подразделяются на два вида:

1) разрабатываемые по итогам обобщения и анализа актуальных моментов правоприменительной практики обработки персональных данных в соответствующих областях (сферах) и рассчитанные на применение всеми заинтересованными лицами.

Их примером, в частности, являются Рекомендации по составлению документа, определяющего политику оператора (уполномоченного лица)

в отношении обработки персональных данных, а также Рекомендации об обработке персональных данных в связи с трудовой (служебной) деятельностью, свободный доступ к которым обеспечен через официальный сайт Центра;

2) адресуемые конкретному субъекту (субъектам). В большинстве случаев такие разъяснения даются по результатам изучения конкретных ситуаций (например, изложенных в поступающих в Центр обращениях).

Иные формы проведения им разъяснительной работы охватывают широкий спектр обучающих и информационно-консультационных мероприятий, рабочих встреч, взаимодействие со средствами массовой информации, работу в Интернете и развитие информационной составляющей социальных сетей, мессенджеров и официального сайта Центра.

В соответствии с абзацем девятым комментируемого пункта, абзацем одиннадцатым п. 7 и абзацем двенадцатым п. 8 Положения Центр уполномочен осуществлять международное сотрудничество, участвовать в работе международных организаций по вопросам защиты персональных данных, организовывать и осуществлять сотрудничество с органами (организациями) по защите прав субъектов персональных данных в иностранных государствах. На практике рассматриваемая норма применяется посредством заключения и реализации соглашений о сотрудничестве с аналогичными структурами иных государств, участия в мероприятиях международного характера и иных направлений взаимодействия с зарубежными партнерами.

Деятельность Центра носит открытый (публичный) характер. Ежегодно не позднее 15 марта он публикует в средствах массовой информации отчет о своей деятельности, который также размещается и на официальном сайте Центра (абзац десятый комментируемого пункта).

Согласно абзацу одиннадцатому рассматриваемого пункта комментируемой статьи и абзацу пятнадцатому п. 8 Положения Центр реализует также иные полномочия, предусмотренные законодательством о персональных данных, и осуществляет иную не запрещенную законодательством деятельность, направленную на реализацию своих основных задач и функций.

Так, одно из важнейших полномочий, необходимых для эффективной работы Центра, закреплено в абзаце восьмом п. 8 Положения, которым установлен обязательный для исполнения государственными органами, иными организациями и гражданами, осуществляющими деятельность по обработке персональных данных, характер решений, принимаемых Центром по вопросам, входящим в его компетенцию.

Как упоминалось, одной из возложенных на Центр основных задач является организация обучения по вопросам защиты прав субъектов персональных данных *(подробнее о ее выполнении см. в комментарии к ст. 17 Закона)*.

С этой целью согласно абзацу тринадцатому п. 7 Положения Центр реализует образовательные программы дополнительного образования взрослых в соответствии с законодательством об образовании.

При этом кроме обучения по вопросам защиты персональных данных Указом № 422 Центру предоставлено право реализовывать образовательную программу повышения квалификации руководящих работников и специалистов и по иным направлениям и профилям образования, охватывая вопросы технической и (или) криптографической защиты информации.

Данным законодательным актом Главы государства установлена обязательность обеспечения собственниками (владельцами) информационных систем[20] и владельцами критически важных объектов информатизации, а также организаций, осуществляющих лицензируемую деятельность по технической и (или) криптографической защите информации[21], обучения в Национальном центре защиты персональных данных не реже одного раза в три года своих работников и (или) иных лиц, в обязанности которых входит обеспечение информационной безопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам технической и (или) криптографической защиты информации.

В целом образовательная деятельность Центра носит плановый, системный характер. В соответствии с абзацем третьим подп. 3.2 и ч. 2 подп. 3.3 п. 3 Указа № 422 заинтересованные лица обеспечивают ежегодное до 15 ноября представление Центру соответственно информации о количестве лиц, в обязанности которых входит обеспечение информационной безопасности и ответственных за осуществление внутреннего контроля за обработкой персональных данных, а также лиц, непосредственно осуществляющих обработку персональных данных, которым необходимо пройти повышение квалификации в Центре.

Еще одним важным полномочием Центра является проведение им на договорной основе добровольного аудита соблюдения операторами (уполномоченными лицами) требований законодательства

---

[20] Указанных в ч. 1 п. 3 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196.

[21] В соответствии с главой 21 Положения о лицензировании отдельных видов деятельности, утвержденного Указом Президента Республики Беларусь от 1 сентября 2010 г. № 450, и п. 13 приложения 1 к этому Положению.

о персональных данных (абзац десятый п. 8 Положения). Любой из них имеет возможность обратиться по этому вопросу в Центр и убедиться в правильности и полноте реализованных правовых, организационных и технических мер по обеспечению защиты персональных данных. При получении по итогам аудита положительного заключения Центра оператор (уполномоченное лицо) не подлежат плановым проверкам в течение пяти лет.

3. Пункт 4 комментируемой статьи предусматривает обязанность государственных органов, иных организаций и граждан предоставлять Центру любую информацию, необходимую для определения законности действий операторов (уполномоченных лиц).

Эта обязанность корреспондируется с предоставленными Центру абзацами вторым и третьим п. 8 Положения правами при осуществлении контроля и без согласия субъектов персональных данных:

запрашивать и получать на безвозмездной основе от государственных органов, иных юридических и физических лиц информацию, необходимую для определения законности действий (бездействия) операторов (уполномоченных лиц) по обработке персональных данных;

получать из информационных ресурсов (систем) сведения, в том числе содержащие банковскую, коммерческую, профессиональную и иную охраняемую законом тайну, а также персональные данные физических лиц, кроме информационных ресурсов (систем), содержащих государственные секреты, на основании письменных запросов, запросов в виде электронных документов либо соглашений (договоров), заключенных с собственниками (владельцами) информационных ресурсов (систем).

Предоставление информации при осуществлении Центром контроля осуществляется в течение 10 календарных дней со дня поступления от него запроса, а в ходе проведения плановых или внеплановых проверок – не позднее следующего рабочего дня со дня предъявления проверяющими требования о представлении документов (их копий).

Статья 19. Ответственность за нарушение настоящего Закона

Комментарий к статье 19

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

Так, за нарушение законодательства о персональных данных в Республике Беларусь предусмотрена дисциплинарная (п. 10 ч. 1 ст. 47 ТК), административная (ст. 23.7 КоАП), уголовная (ст.ст. 203^1, 203^2 УК) и гражданско-правовая ответственность (п. 2 ст. 19 Закона предусматривает возмещение морального вреда, имущественного вреда и понесенных субъектом персональных данных убытков).

Дисциплинарная ответственность.

Меры дисциплинарной ответственности, порядок и сроки их применения, порядок обжалования, снятия и погашения дисциплинарных взысканий урегулированы главой 14 ТК, а также другими актами законодательства: Декретом Президента Республики Беларусь от 26 июля 1999 г. № 29 "О дополнительных мерах по совершенствованию трудовых отношений, укреплению трудовой и исполнительской дисциплины", Декретом Президента Республики Беларусь от 15 декабря 2014 г. № 5 "Об усилении требований к руководящим кадрам и работникам организаций" и др.

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

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

Таким образом, привлечение к дисциплинарной ответственности за нарушение законодательства о персональных данных возможно только в отношении тех категорий работников, на которых возложена обязанность по обработке персональных данных, в связи с нарушением ими порядка обработки персональных данных.

Важно отметить, что, несмотря на предусмотренную Законом в качестве обязательной меры по назначению ответственного за осуществление внутреннего контроля, ни оператор, ни уполномоченное лицо, ни работники организации, непосредственно осуществляющие обработку персональных данных, не освобождаются от ответственности за допущенные ими нарушения.

Законом Республики Беларусь от 28 мая 2021 г. № 114-З "Об изменении законов по вопросам трудовых отношений" в ТК введено новое основание прекращения трудовых отношений – нарушение работником порядка сбора, систематизации, хранения, изменения, использования, обезличивания, блокирования, распространения,

предоставления, удаления персональных данных (п. 10 ч. 1 ст. 47 ТК). Увольнение как мера дисциплинарного взыскания по данному основанию возможна, если работник исполнил свою трудовую обязанность ненадлежащим образом либо она не исполнена вовсе. При этом совершенное действие или бездействие должно быть виновным, а поведение работника должно быть противоправным.

Следует отметить, что данное установление носит диспозитивный характер. Наниматель самостоятельно оценивает степень вины работника в нарушении законодательства о персональных данных и с учетом обстоятельств совершенного дисциплинарного проступка принимает решение о выборе дисциплинарного взыскания. Если наниматель посчитает, что достижение целей привлечения к ответственности возможно без прекращения трудовых отношений, то он может избрать иной вид дисциплинарных взысканий.

Привлечение работника к дисциплинарной ответственности за нарушение законодательства о персональных данных не влияет на возможность привлечения его к гражданско-правовой, административной или уголовной ответственности за те же нарушения в порядке и на основаниях, установленных законодательством.

Административная ответственность.

Статьей 23.7 КоАП предусмотрена административная ответственность за нарушение законодательства о защите персональных данных. Составы административных правонарушений, объединенные в данной статье, являются формальными. Законодатель признает административно наказуемым сам факт совершения противоправного виновного деяния независимо от наступления последствий. Важно также учитывать, что данная статья является общей и подлежит применению к нарушению порядка обработки персональных данных независимо от того, распространяется ли на данные отношения действие Закона или нет (например, в силу изъятия, предусмотренного абзацем вторым п. 2 ст. 2 Закона).

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

В КоАП законодатель использует отдельно термин ”обработка“ как самостоятельное деяние, при этом одновременно перечисляя часть деяний, которые в соответствии с абзацем шестым ст. 1 Закона также относятся к обработке, что можно объяснить временем принятия КоАП и ориентацией на терминологию действовавшего на тот момент Закона об информации, информатизации и защите информации.

Нарушение прав субъекта, связанных с обработкой персональных данных, может иметь различные формы:

отсутствие ответа на заявления, поданные в соответствии со ст. 14 Закона;

несоблюдение сроков ответов на данные заявления;

неправомерный отказ в удовлетворении соответствующих требований субъектов персональных данных (например, отказ в прекращении обработки данных и их удалении при отсутствии правовых оснований для обработки);

предоставление неполной информации в ответ на поступившее заявление (например, при подаче заявления в соответствии со ст. 11 Закона субъекту вместо конкретных персональных данных указывается общая характеристика таких данных; при подаче заявления в соответствии со ст. 12 Закона указывается лишь, что данные передавались субъектам, имеющим право на их получение).

Субъектом данного правонарушения является любое вменяемое физическое лицо, достигшее возраста 16 лет. В силу требований п. 2 ч. 1 ст. 4.6 КоАП индивидуальный предприниматель также может являться субъектом рассматриваемого правонарушения.

Санкция предусматривает наложение штрафа в размере до пятидесяти базовых величин.

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

При привлечении лица к административной ответственности в данном случае следует установить, что соответствующие действия по обработке персональных данных охватывались трудовой функцией работника, отражены в его должностной инструкции.

Пример.

В качестве подобного нарушения можно рассматривать, например, неофициальную практику "пробива" по базам по просьбе знакомых и др.

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

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

Особая опасность распространения персональных данных заключается в том, что информация выходит из-под контроля субъекта,

субъект теряет возможность управления доступом к персональным данным, нарушается конфиденциальность соответствующих сведений.

Распространение может осуществляться в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет).

Пример.

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

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

В ч. 4 ст. 23.7 КоАП закреплен еще один самостоятельный состав административного правонарушения – несоблюдение мер обеспечения защиты персональных данных физических лиц.

Соответствующие меры вытекают из требований ст. 17 Закона. Перечень обязательных мер содержится в п. 3 данной статьи. Кроме того, ряд обязательных мер предусмотрен и в Указе № 422. Это установление и поддержание соответствующими организациями в актуальном состоянии:

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

перечня уполномоченных лиц, если обработка персональных данных осуществляется уполномоченными лицами.

Наиболее распространенными на сегодняшний день примерами нарушений, связанных с несоблюдением мер защиты персональных данных, являются:

отсутствие лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных. Как нарушение рассматривается также формальное назначение данного лица без подтверждения выполнения таким лицом каких-либо контрольных функций;

необеспечение неограниченного доступа к документам, определяющим политику оператора (уполномоченного лица) в отношении обработки персональных данных, до начала такой обработки;

отсутствие порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе (системе);

неосуществление технической и криптографической защиты персональных данных в порядке, установленном ОАЦ, в соответствии

с классификацией информационных ресурсов (систем), содержащих персональные данные.

Законодатель применительно к данному нарушению в санкции статьи установил дифференцированный подход. Так, несоблюдение мер обеспечения защиты персональных данных физических лиц влечет наложение штрафа в размере от двух до десяти базовых величин, на индивидуального предпринимателя – от десяти до двадцати пяти базовых величин, а на юридическое лицо – от двадцати до пятидесяти базовых величин.

Исходя из положений ст. 4.4 КоАП, ответственность за данное правонарушение применяется независимо от требования потерпевшего, его законного представителя. Однако это не лишает их права обратиться в уполномоченные органы с заявлением о начале административного процесса по ст. 23.7 КоАП по факту нарушения законодательства о защите персональных данных.

В соответствии со ст. 3.30 ПИКоАП протоколы об административных правонарушениях по ст. 23.7 КоАП имеют право составлять уполномоченные на то должностные лица органов внутренних дел, а также прокурор (при осуществлении им надзорных функций), дела рассматриваются единолично судьей районного (городского) суда.

Уголовная ответственность.

На сегодняшний день в УК существуют две статьи, касающиеся защиты персональных данных и информации о частной жизни. Так, в ст. 203^1 УК устанавливается ответственность за незаконные действия в отношении информации о частной жизни и персональных данных, а в ст. 203^2 УК – ответственность за несоблюдение мер обеспечения защиты персональных данных.

Диспозиция ч. 1 ст. 203^1 УК сформулирована как умышленные незаконные сбор, предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшие причинение существенного вреда правам, свободам и законным интересам гражданина.

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

Общественно опасное деяние представлено в виде двух альтернативных действий: незаконный сбор или незаконное

предоставление. Каким образом производится сбор и предоставление соответствующей информации другим организациям, гражданам или общественности, не имеет значения.

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

В диспозиции ч. 1 ст. 203[1] УК в качестве обязательного признака объективной стороны предусмотрены общественно опасные последствия – причинение существенного вреда правам, свободам и законным интересам гражданина. Наличие общественно опасных последствий выступает основным критерием разграничения административного правонарушения и уголовно наказуемого деяния.

С субъективной стороны рассматриваемое преступление характеризуется умышленной формой вины. При этом мотив и цель для квалификации деяния как преступления значения не имеют.

Субъектом преступного посягательства является физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летного возраста.

Обращаем внимание, что только деяние, предусмотренное ч. 1 ст. 203[1] УК влечет уголовную ответственность по требованию потерпевшего. Степень вреда и целесообразность уголовной ответственности в данном случае определяются потерпевшей стороной, и именно требование потерпевшего инициирует возбуждение уголовного дела.

Дела частного обвинения возбуждаются лицом, пострадавшим от преступления, его законным представителем или представителем юридического лица, и производство по ним подлежит прекращению в случае примирения его с обвиняемым (ч. 2 ст. 26 УПК). Вместе с тем согласно ч. 5 ст. 26 УПК прокурор вправе возбудить уголовное дело о преступлениях частного и частно-публичного обвинения и при отсутствии заявления лица, пострадавшего от преступления, если они затрагивают существенные интересы государства и общества или совершены в отношении лица, находящегося в служебной или иной зависимости от обвиняемого либо по иным причинам не способного самостоятельно защищать свои права и законные интересы.

В ч. 2 ст. 203[1] УК установлен квалифицированный состав преступления, касающийся *распространения информации о частной жизни и (или) персональных данных* при аналогичных последствиях.

Усиление ответственности в данном случае продиктовано тем, что, в отличие от предоставления, распространение информации о частной жизни и (или) персональных данных связано с ознакомлением с ними неопределенного круга лиц.

Формы распространения могут быть различными: это может быть распространение информации в сети Интернет или в социальных сетях, средствах массовой информации, посредством доведения информации до широкого круга лиц путем расклейки объявлений (сообщений) на информационных стендах, дверях подъездов, местах массового скопления людей и т.п. Как распространение информации следует рассматривать также устное озвучивание информации неопределенному кругу людей (например, в общественном месте) и др. Сказанное свидетельствует о том, что распространение закономерно расширяет границы причинения вреда, чему, несомненно, должна даваться самостоятельная правовая оценка.

Часть 3 ст. 203^1 УК предусматривает повышенную уголовную ответственность за рассмотренные действия, совершенные в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга. Таким образом, данной нормой установлены особые требования к потерпевшему, и наступление уголовной ответственности зависит от установления его особого статуса.

В соответствии с п. 3 ч. 2 ст. 4 УК под близкими признаются близкие родственники и члены семьи потерпевшего либо иные лица, которых он обоснованно признает своими близкими.

Понятия ”осуществление служебной деятельности“ или ”выполнение общественного долга“ раскрываются в п. 14 постановления Пленума Верховного Суда Республики Беларусь от 17 декабря 2002 г. № 9 ”О судебной практике по делам об убийстве (ст. 139 УК)“.

В ст. 203^2 УК установлена ответственность за **несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных**, повлекшее по неосторожности их распространение и причинение тяжких последствий.

Перечень обязательных мер по обеспечению защиты персональных данных (правовых, организационных и технических) определен в п. 3 ст. 17 Закона. Кроме того, Указом № 422 установлены дополнительные меры, связанные с обеспечением защиты персональных данных (*подробнее см.: комментарий к п. 3 ст. 17*).

Рассматриваемый состав является материальным и будет окончен с момента наступления последствий. В качестве общественно опасных последствий, предусмотренных ст. 203^2 УК, выступает *одновременное распространение персональных данных* (ознакомление с ними неопределенного круга лиц) *и причинение тяжких последствий*.

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

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

Лицо может осуществлять обработку персональных данных в связи с должностным положением, трудовыми или служебными обязанностями, выполнением обязательств по гражданско-правовому договору и на иных законных основаниях.

Гражданско-правовая ответственность.

Как самостоятельная правовая форма гражданско-правовой ответственности за нарушение законодательства о персональных данных может быть использован гражданско-правовой институт обязательств вследствие причинения вреда, предусмотренный главой 58 ГК. Этот институт пригоден для принуждения виновных лиц к полному или частичному возмещению имущественного вреда, нанесенного гражданину в результате неприятия мер, предусмотренных Законом, а также нарушения его прав незаконными действиями оператора или уполномоченного лица.

Так, юридическое лицо либо гражданин возмещает вред, причиненный его работником при исполнении своих трудовых (служебных, должностных) обязанностей (п. 1 ст. 937 ГК). При этом наниматель не несет ответственности в случае, если работник причинил вред третьему лицу не при исполнении трудовых обязанностей.

Работник, причинивший вред, может добровольно возместить его полностью или частично. В случае отказа работника от возмещения причиненного его противоправными действиями (бездействием) при исполнении им служебных, должностных или иных трудовых обязанностей вреда, он может быть взыскан в судебном порядке.

После вынесения судом решения о взыскании с организации в пользу третьего лица вреда руководитель в случаях и пределах, установленных законодательством, имеет право возложить на виновное должностное лицо понесенный при этом ущерб, если он не был возмещен в добровольном порядке (п. 1 ст. 950 ГК).

При этом следует руководствоваться положениями п. 50 постановления Пленума Верховного Суда Республики Беларусь от 29 марта 2001 г. № 2 ”О некоторых вопросах применения судами законодательства о труде“. Споры, связанные с регрессными требованиями, относят к трудовым спорам.

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

В п. 2 ст. 19 Закона особо отмечается, что моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, установленных Законом, подлежит возмещению.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков, поскольку право гражданина на компенсацию (материальное возмещение) морального вреда гарантировано Конституцией (ст. 60) и является способом защиты гражданских прав, неприкосновенности и достоинства личности в установленном законом порядке.

Возмещение морального вреда осуществляется по правилам ст. 152 ГК и § 4 главы 58 ГК и детализировано в постановлении Пленума Верховного Суда Республики Беларусь от 28 сентября 2000 г. № 7 ”О практике применения судами законодательства, регулирующего компенсацию морального вреда“ (далее – постановление Пленума № 7). При этом в п. 12 постановления Пленума № 7 особо отмечается, что правило, изложенное в ст. 937 ГК об ответственности юридических лиц или граждан по возмещению вреда, причиненного их работниками при исполнении ими своих трудовых (служебных, должностных) обязанностей, распространяется и на случаи причинения морального вреда.

Под моральным вредом следует понимать испытываемые гражданином физические и (или) нравственные страдания (ч. 1 ст. 152 ГК).

Если гражданину причинен моральный вред действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законодательством, гражданин вправе требовать от нарушителя денежную компенсацию указанного вреда. При определении размеров компенсации морального вреда суд принимает во внимание степень вины нарушителя и иные заслуживающие внимания обстоятельства. Суд должен также учитывать степень физических и нравственных страданий, связанных с индивидуальными особенностями лица, которому причинен вред.

Понятие физических и нравственных страданий раскрывается в п. 8 постановления Пленума № 7.

Пример.

К числу наиболее распространенных физических страданий относятся повышение артериального давления, сердечная аритмия, постоянные головные боли, обострение хронических заболеваний (астма, язва, гипертония), проблемы

со сном, а также общее ухудшение состояния здоровья. Нравственные страдания выражаются в ощущениях страха, стыда, унижения, тревоги, беспокойстве за здоровье, состоянии постоянного стресса, раздражительности, эмоциональном потрясении, а равно в иных неблагоприятных для человека в психологическом аспекте переживаниях.

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

Истец в заявлении о компенсации морального вреда должен указать, кем, при каких обстоятельствах и какими действиями (бездействием) причинены ему физические или нравственные страдания, в чем они выражаются, в какой денежной сумме он оценивает их компенсацию.

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

ГЛАВА 5
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 20. Меры по реализации положений настоящего Закона

Комментарий к статье 20

Комментируемая статья предусматривает поручченческие нормы, направленные на реализацию положений Закона.

В целом можно выделить три блока мер:

создание уполномоченного органа;

приведение законодательства в соответствие с Законом;

реализация иных мер.

Учитывая, что одной из ключевых мер по обеспечению реализации Закона является создание уполномоченного органа по защите прав субъектов персональных данных, Совету Министров Республики Беларусь совместно с Оперативно-аналитическим центром при Президенте Республики Беларусь было поручено принять меры по созданию такого органа.

Уполномоченный орган по защите прав субъектов персональных данных был создан Указом № 422, которым было также утверждено Положение. Указ № 422 вступил в силу 15 ноября 2021 г. одновременно со вступлением в силу Закона.

Принятию данного Указа предшествовала значительная подготовительная работа, в рамках которой рассматривались различные модели создания уполномоченного органа (создание в виде отдельной организации, возложение функций на уже существующий орган и др.), его место в системе органов власти, изучался зарубежный опыт правового регулирования. В итоге по примеру многих стран было принято решение о создании отдельной организации, которая будет осуществлять функции уполномоченного органа.

Наряду с созданием уполномоченного органа, принятие Закона потребовало приведения актов законодательства в соответствие с ним.

В частности, Совету Министров Республики Беларусь совместно с Национальным центром законодательства и правовых исследований было поручено подготовить и внести предложения о приведении законодательных актов в соответствие с Законом.

В развитие указанного поручения был принят Закон Республики Беларусь от 10 октября 2022 г. № 209-З ”Об изменении законов по вопросам обработки персональных данных“.

Им внесены изменения в Закон Республики Беларусь от 22 июля 2002 г. № 133-З ”О государственной регистрации недвижимого

имущества, прав на него и сделок с ним“, Закон ”О регистре населения“, Закон Республики Беларусь от 21 июля 2008 г. № 419-З ”О Государственной границе Республики Беларусь“, Закон ”Об информации, информатизации и защите информации“.

Наиболее значимыми были изменения в Закон ”Об информации, информатизации и защите информации“. В частности, устранено противоречие в определении персональных данных, требованиях к форме получения согласия, регулировании мер по защите обезличенных персональных данных и др. Соответствующие положения либо исключены из Закона ”Об информации, информатизации и защите информации“, либо изложены по аналогии с положениями Закона.

Вносились изменения и в иные акты законодательства. К сожалению, в большинстве случаев такие изменения касались формальной корректировки терминологии (например, ссылка на законодательство об информации, информатизации и защите информации менялась ссылкой на законодательство о персональных данных). В итоге при практическом применении Закона выявляются проблемы несоответствия ряда ведомственных актов, в частности, предусматривающих формы согласия, круг обрабатываемых данных и др., требованиям Закона.

Наиболее сложная ситуация с реализацией в актах законодательства требований ст. 4 Закона о соразмерности обработки, конкретности целей обработки, недопустимости избыточности обрабатываемых данных. Учитывая довольно общий характер данных критериев, оценка различными заинтересованными положений актов законодательства на предмет соответствия таким критериям зачастую бывает неоднозначной.

Несмотря на важность работы по приведению актов законодательства в соответствие с Законом, очевидно, что только этим действием в данном случае нельзя ограничиться. Требуется перестройка многих бизнес-процессов, доработка информационных ресурсов, подготовка разъяснительных писем и организация иной разъяснительной работы.

Статья 21. Вступление в силу настоящего Закона

Комментарий к статье 21

Комментируемая статья определяет порядок вступления Закона в силу.

Предусматривается, что Закон (ст.ст. 1–19) вступает в силу через 6 месяцев после его официального опубликования. Закон был

опубликован на Национальном правовом Интернет-портале Республики Беларусь 14 мая 2021 г. Соответственно, Закон вступил в силу 15 ноября 2021 г.

Иные положения Закона (ст.ст. 20, 21) вступают в силу после его официального опубликования, то есть с 15 мая 2021 г.

Принятие Закона сформировало новый правовой институт, став важной вехой в развитии всего законодательства. Вместе с тем обработка персональных данных осуществлялась и до его принятия, в связи с чем возникло множество вопросов о применении Закона к обработке персональных данных, которая имела место до его вступления в силу.

Наиболее распространенным вопросом является вопрос о необходимости получения нового согласия на обработку персональных данных, если ранее полученное согласие в той или иной степени не соответствовало требованиям ст. 5 Закона. Учитывая, что многие операторы (банки, торговые сети и др.) обрабатывают персональные данные сотен тысяч и даже миллионов граждан, решение данного вопроса имеет крайне важное значение и может повлечь серьезные затраты для операторов.

В этой ситуации следует исходить из следующего.

До 15 ноября 2021 г. (до вступления в силу Закона) сбор, обработка, хранение информации о частной жизни и персональных данных физического лица осуществлялись с его письменного согласия в соответствии со ст. 18 Закона ”Об информации, информатизации и защите информации“.

С 15 ноября 2021 г. вступили в силу основные положения Закона, которыми существенно меняются требования к порядку получения согласия и его содержанию, что направлено на дополнительную защиту прав физических лиц при обработке их персональных данных.

Учитывая положения ст. 66 Закона Республики Беларусь от 17 июля 2018 г. № 130-З ”О нормативных правовых актах“, если согласие было получено до вступления в силу Закона и соответствовало требованиям Закона ”Об информации, информатизации и защите информации“, такое согласие признается надлежащим для целей Закона, и получение нового согласия не требуется. При этом условия обработки таких персональных данных после 15 ноября 2021 г. должны соответствовать требованиям Закона.

В частности, если согласие являлось частью договора, заключенного до вступления в силу Закона, и касалось обработки персональных данных в рамках заключения (исполнения) договора, а информация, указанная в ст. 5 Закона, не предоставлялась, то с 15 ноября 2021 г. дальнейшая обработка признается правомерной. Правовым основанием на такую обработку выступает абзац пятнадцатый

ст. 6 Закона (обработка на основании договора, заключенного (заключаемого) с субъектом персональных данных).

Если согласие получалось также для иных целей (например, рекламных рассылок), то в части иных целей действует согласие, а в части обработки для заключения (исполнения) договора – основание, предусмотренное абзацем пятнадцатым ст. 6 Закона.

Если ранее полученное согласие не соответствовало Закону ”Об информации, информатизации и защите информации“ (не соблюдена письменная или приравненная к ней форма) и в соответствии с Законом отсутствуют иные правовые основания для обработки персональных данных, то оператор должен либо получить согласие в соответствии с требованиями, установленными ст. 5 Закона, либо прекратить обработку и удалить персональные данные субъекта.

В случае, если до 15 ноября 2021 г. законодательством не предусматривалась возможность обработки персональных данных без согласия и не было получено согласие, а после вступления в силу Закона обработка продолжается и подпадает под одно из оснований, предусмотренных ст. 6 Закона (например, обработка при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных), то такая обработка может вестись без согласия на основании соответствующих положений ст. 6 Закона.

Если до 15 ноября 2021 г. законодательством не предусматривалась возможность обработки персональных данных без согласия и согласие не было получено, а после вступления в силу Закона обработка продолжается и не подпадает под основания, предусмотренные ст. 6 Закона, то оператор должен либо получить согласие в соответствии с требованиями, установленными ст. 5 Закона, либо прекратить обработку и удалить персональные данные субъекта.