Серия «Деловой советник»

ГУ "ВИТЕБСКАЯ ОБЛАСТНАЯ БИБЛИОТЕКА ИМЕНИ В.И.ЛЕНИНА"

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ВАЖНО ЗНАТЬ!

Информационный дайджест

Выпуск 2

Витебск, 2023

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

ВАЖНО ЗНАТЬ!

Информационный дайджест

Составители: **Гузова** Лариса Алексеевна,
Ответственный за выпуск Т. Н. Адамян
Компьютерная верстка Е. В. Юпатовой
Художественное оформление А. В. Лабунской

Тираж 3 экз.
Цифровая печать
210015 г. Витебск, ул. Ленина, д. 8а
E-mail : vlib@vlib.by

ГУ «ВИТЕБСКАЯ ОБЛАСТНАЯ БИБЛИОТЕКА ИМЕНИ В. И. ЛЕНИНА»
Отдел «Публичный центр правовой информации»

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. ВАЖНО ЗНАТЬ!

Информационный дайджест

Серия «Деловой советник»

Выпуск 2

Витебск, 2023

УДК 351
ББК 67.401.114(4Беи)
З-40

Составитель Л. А. Гузова
Редакционная коллегия:
О. М. Комендантова (отв. ред.), В. М. Овсянникова
Ответственный за выпуск Т. Н. Адамян

Защита персональных данных. Важно знать! : информационный дайджест / ГУ «Витебская областная библиотека имени В. И. Ленина», отдел «Публичный центр правовой информации» ; [сост. Л. А. Гузова]. – Витебск, 2023. – 76 с. – (Серия «Деловой советник» ; вып. 2).

В дайджесте содержится информация, раскрывающая понятие «персональные данные». Рассмотрены Рекомендации Национального центра защиты персональных данных по обработке персональных данных в сфере трудовых отношений.

Данный информационный дайджест адресован руководителям, специалистам юридических служб, студентам юридических факультетов, а также широкому кругу пользователей.

ИСТОЧНИКИ ИНФОРМАЦИИ

1. **Белявский, С. Ч.** Трансграничная передача персональных данных: когда она имеет место и как ее осуществить / С. Ч. Белявский, Е. Галушкина // Я – юрисконсульт организации. – 2022. – № 1. – С. 9–12.

2. **Дудко, М. О.** Понятие «персональные данные» в современном праве / М. О. Дудко // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 4, Правазнаўства. – 2020. – Т. 10, № 3. – С. 14–22.

3. **Кудрявец, Ю. Н.** Оператор и уполномоченный по обработке персональных данных: определяем обязанности и ответственность / Ю. Н. Кудрявец // Я – юрисконсульт организации. – 2022. – № 12. – С. 51–56.

4. **Орлова, О.** Как обрабатывать персональные данные в сфере трудовых отношений: НЦЗПД дал рекомендации / О. Орлова // Я – юрисконсульт организации. – 2022. – № 2. – С. 60–64.

5. **Пухов, А. А.** Уголовно-правовая защита неприкосновенности частной жизни и персональных данных в свете изменений уголовного закона / А. А. Пухов // Право.by. – 2021. – № 4. – С. 85–92.

6. **Саванович, Н. А.** Дефиниция персональных данных в Законе Республики Беларусь «О защите персональных данных» и проблемы ее применения / Н. А. Саванович // Юстиция Беларуси. – 2022. – № 6. – С. 41–44.

7. **Смирнов, В. Д.** Об административной ответственности за нарушение законодательства о персональных данных / В. Д. Смирнов // Отдел кадров. – 2023. – № 4. – С. 88–91.

предвидеть.

Санкция уголовно-правовой нормы является альтернативной, относительно-определенной и предполагает возможность назначения наказаний от штрафа, лишения права занимать определенные должности или заниматься определенной деятельностью, исправительных работ на срок до одного года, до ареста, ограничения свободы на срок до двух лет, лишения свободы на срок до одного года. По категории данное преступление – не представляющее большой общественной опасности.

Таким образом, основываясь на теоретических постулатах уголовного права и руководствуясь положениями уголовного закона, следует **заключить следующее**.

1. Установление и корректировка в отечественном уголовном законе ответственности за посягательства на персональные данные и неприкосновенность частной жизни является определенной ступенью к формированию целостной системы уголовно-правовых норм, позволяющих комплексно отрегулировать сферу этих важнейших для гражданина общественных отношений.

2. Юридические модели норм, предусматривающих ответственность за незаконные действия с персональными данными, могут быть подвергнуты дальнейшей доработке и оптимизации.

3. Уголовные дела, возбужденные по признакам состава преступления, предусмотренного ст. 179 УК, до вступления в силу Закона № 112-З, подлежат прекращению в связи с вступлением в силу законодательного акта, устраняющего наказуемость деяния (п. 10 ч. 1 ст. 29 УПК). Правило об обратной силе должно быть распространено, в том числе и на лиц, отбывающих наказание и отбывших наказание, но имеющих судимость по ст. 179 УК.

4. Уголовные дела по признакам состава преступления, ответственность за совершение которого предусмотрена ст. 203^1 УК, могут возбуждаться лишь по событиям, имевшим место после 19 июня 2021 г.

СОДЕРЖАНИЕ

ОТ СОСТАВИТЕЛЯ

Современный этап развития отношений общества и государства характеризуется исключительной емкостью различного характера сведений, относящихся к разным сферам человеческой деятельности. Важно и то, что общечеловеческая практика и возможности современных информационных и коммуникационных технологий в своей совокупности объективно позволяют и формируют необходимость сбора, хранения, использования и распространения информации, поскольку последняя представляет собой сведения об окружающем мире и процессах, протекающих в нем, которые воспринимаются человеком или специальными приборами. Характерно, что с каждым годом перечень оснований и поводов для сбора новых данных увеличивается. Наблюдается все возрастающая потребность граждан в защите личной информации. Граждане начинают не только воспринимать информацию о себе как ценность, которую необходимо беречь, но и понимать, где они могут получить реальную помощь и поддержку в отстаивании своих прав в сфере персональных данных. В этой связи возникают вопросы правовой регламентации хранения, защиты информации, а также ответственности за ее незаконное разглашение. Особую значимость приобретает реализация задачи по защите прав и свобод человека и гражданина при обработке его персональных данных, в том числе защите прав на неприкосновенность частной жизни, личной и семейной тайны. Гарантированные белорусским государством право каждого на защиту от неправомерного вмешательства в частную жизнь обуславливают особое значение защиты информации о его частной жизни и персональных данных.

Во втором выпуске дайджеста по праву «Деловой советник» содержится информация, раскрывающая понятие «персональные данные». Рассмотрены Рекомендации Национального центра защиты персональных данных по обработке персональных данных в сфере трудовых отношений, а также административная и уголовная ответственность за нарушение

времени, обстановки и иных обстоятельств несоблюдение с внутренней закономерностью повлекло сначала первичные, а потом и вторичные последствия. Даже если последствия будут следовать по времени за деянием, то доказыванию будет подлежать: являются ли данные следствия закономерным развитием деяния, а не результатом действия иных лиц и т.п. Таким образом, можно предположить, что объективно причинная связь может быть установлена только между несоблюдением мер и распространением сведений. В то же время проследить, а впоследствии доказать, связь между несоблюдением и причинением тяжких последствий в результате непосредственно распространения, а не иных факторов, будет практически невозможно.

«Несоблюдение мер обеспечения защиты персональных данных лицом, осуществляющим обработку персональных данных, повлекшее по неосторожности их распространение либо повлекшее изменения в реальной действительности, повлекшее по неосторожности причинение тяжких последствий...».

Субъект преступления – специальный. Помимо установления общих признаков (физическое лицо, достигшее 16-летнего возраста, находившееся в состоянии вменяемости в момент совершения общественно опасного деяния) необходимо определить, что лицо выполняло действие или совокупность действий по обработке персональных данных, т.е. сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление или удаление.

Субъективная сторона выражена неосторожной формой вины в виде как легкомыслия, так и небрежности. При легкомыслии виновный предвидит возможность наступления распространения персональных данных и причинения вследствие этого тяжких последствий, но без достаточных оснований рассчитывал на их предотвращение. При небрежности лицо не предвидит возможности распространения персональных данных и причинения вследствие этого тяжких последствий, хотя при необходимой внимательности и предусмотрительности должно было и могло их

моделировать через категорию «причинение существенного вреда...».

Состав преступления материальный и является юридически оконченным с момента причинения тяжких последствий (например, опорочивание деловой репутации, психическое расстройство (заболевание), создание политической или социальной напряженности в обществе и др.) потерпевшему в связи с распространением его персональных данных. Такой вывод обусловлен тем, что при формулировании общественно опасных последствий использован союз «и». Такое решение может привести к определенным проблемам в правоприменении. Например, лицо, осуществляющее обработку персональных данных, вследствие несоблюдения мер обеспечения защиты персональных данных допустило их распространение, но при этом никакие тяжкие последствия для потерпевшего не наступили. Наличие неосторожной формы вины исключает квалификацию содеянного как покушения. Следовательно, уголовная ответственность исключается вовсе. Кроме того, какой уголовно-правовой оценки заслуживает умышленное распространение персональных данных лицом, осуществляющим их обработку, в случае если потерпевший совершит на этой почве самоубийство, которого виновный не предвидел, хотя должен был и мог предвидеть? Уголовная ответственность будет отсутствовать вовсе. При этом при неосторожном варианте аналогичного посягательства не исключается постановка вопроса о привлечении к ответственности по ст. 203^2 УК.

Отдельно стоит коснуться вопроса причинной связи в ст. 203^2 УК. По большому счету речь идет об определении необходимой причинно-следственной связи между деянием, первичным и вторичным последствиями. С точки зрения механизма установления причинной связи несоблюдение мер обеспечения защиты персональных данных должно предшествовать их распространению и причинению тяжких последствий. При этом несоблюдению должна быть присуща способность с внутренней закономерностью порождать как распространение, так и причинение тяжких последствий, чего в реальной действительности может и не быть. Кроме того, должно быть установлено, что с учетом условий места,

законодательства о персональных данных.

Источниками информации являются: ИПС ЭТАЛОН. Законодательство Республики Беларусь, сайт Национальный центр защиты персональных данных Республики Беларусь.

Данный информационный дайджест адресован руководителям, специалистам юридических служб, студентам юридических факультетов, а также широкому кругу пользователей.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

1. **Конституция** Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г., 27 февр. 2022 г. : в ред. Закона Респ. Беларусь от 12.10.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2. **Гражданский** кодекс Республики Беларусь [Электронный ресурс] : 7 дек. 1998 г., № 218-З : принят Палатой представителей 28 окт. 1998 г. : одобр. Советом Респ. 19 нояб. 1998 г. : в ред. Закона Респ. Беларусь от 03.01.2023 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. **Гражданский** процессуальный кодекс Республики Беларусь [Электронный ресурс] : 11 янв. 1999 г., № 238-З : принят Палатой представителей 10 дек. 1998 г. : одобр. Советом Респ. 18 дек. 1998 г. : в ред. Закона Респ. Беларусь от 27.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

4. **Кодекс** Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 91-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. : в ред. Закона Респ. Беларусь от 09.12.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

5. **Процессуально-исполнительный** кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., № 92-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. : в ред. Закона Респ. Беларусь от 09.12.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

предписания, идеи, обязательные для законодателя, субъектов правоприменения и граждан. Содержание принципа законности предполагает, что нормы уголовного закона подлежат строгому толкованию, а его применение по аналогии не допускается. С семантической точки зрения это воплощается в буквальном (дословном) понимании текста закона, т.е. путем установления точного соответствия. Парадигма механического сопоставления диспозиций ст.ст. 179 и 203^1 УК при квалификации преступлений путем технического перенесения норм из одного (глава 21) структурного элемента кодекса в другой (глава 23) является попыткой применения уголовного закона по аналогии, что категорически запрещено.

Статья 203^2. Несоблюдение мер обеспечения защиты персональных данных

Непосредственным объектом являются общественные отношения, возникающие по поводу защиты персональных данных. Предмет преступления – персональные данные.

Объективная сторона состава преступления (ст. 203^2 УК) состоит из деяния (несоблюдение мер), общественно опасных последствий (распространение персональных данных и причинение тяжких последствий) и причинной связи между ними. В самом общем виде несоблюдение мер – это неисполнение требований законодательства об обеспечении защиты персональных данных.

В качестве общественно опасных последствий указано «распространение персональных данных и причинение тяжких последствий». Стоит отметить, что описание оценочного признака через категорию «причинение» является определенной новацией в УК. Как правило, для описания наступления иных тяжких последствий используется термин «повлекшие» (ст.ст. 218, 279, 290, 325 УК и др.). В диспозиции ст. 203^2 УК для избежания повтора законодатель был вынужден использовать формулу «причинение», которая, как правило, используется в случае констатации вреда или ущерба (ст.ст. 197, 218, 226, 349 УК и др.). Логичнее было бы и в данном случае оценочный признак

устанавливающая ответственность за распространение сведений, перешла в категорию менее тяжких преступлений, т.к. наказание установлено в виде ограничения свободы на срок до трех лет или лишения свободы на тот же срок со штрафом. В квалифицированном составе преступления (ч. 3 ст. 203[1] УК) при сохранении категории (менее тяжкое преступление) произошло существенное усиление наказания – ограничение свободы на срок до пяти лет или лишение свободы на тот же срок со штрафом.

Иные аспекты положения лица. Положение лица, совершившего рассматриваемое общественно опасного деяние, ухудшено. Согласно ст. 33 УК деяния, содержащие признаки ч. 1 ст. 179 УК, влекли уголовную ответственность лишь при наличии выраженного в установленном уголовно-процессуальным законом порядке требования лица, пострадавшего от преступления, любого из его совершеннолетних близких родственников или членов семьи в случаях, предусмотренных уголовно-процессуальным законом, или его законного представителя либо представителя юридического лица привлечь виновного к уголовной ответственности, т.е. относились к делам частного обвинения. С принятием Закона № 112-З изменилась категория дел, к которой относится ч. 1 ст. 203[1] УК. В настоящее время это дела частно-публичного обвинения. Это означает, что данная категория возбуждается не иначе как по заявлению лица, пострадавшего от преступления, его законного представителя или представителя юридического лица, рассмотрение в суде происходит при обязательном участии прокурора, но производство по делам частно-публичного обвинения за примирением сторон императивно прекращению не подлежит (п. 5 ч. 1 ст. 29 и п. 4 ч. 1 ст. 30 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК)).

В-третьих, в Республике Беларусь уголовная ответственность основывается на принципах законности, равенства граждан перед законом, неотвратимости ответственности, личной виновной ответственности, справедливости и гуманизма. Принципы – это основополагающие исходные

6. **Трудовой** кодекс Республики Беларусь [Электронный ресурс] : 26 июля 1999 г., № 296-З : принят Палатой представителей 8 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 30.12.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

7. **Уголовно-процессуальный** кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 09.03.2023 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

8. **Уголовный кодекс** Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275- З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 09.03.2023 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

9. **О защите** персональных данных [Электронный ресурс] : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : принят Палатой Представителей 2 апр. 2021 г. : одобр. Советом Респ. 21 апр. 2012 г. : в ред. Закона Респ. Беларусь от 01.06.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

10. **О переписи** населения [Электронный ресурс] : Закон Респ. Беларусь, 13 июля 2021 г., № 144-З : принят Палатой Представителей 23 июня 2006 г. : одобр. Советом Респ. 30 июня 2006 г. : в ред. Закона Респ. Беларусь от 13.06.2016 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

11. **О регистре** населения [Электронный ресурс] : Закон Респ. Беларусь, 21 июля 2008 г., № 418-З : принят Палатой Представителей 24 июня 2008 г. : одобр. Советом Респ. 28 июня 2008 г. : в ред. Закона Респ. Беларусь от 10.10.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

12. **Об индивидуальном** (персонифицированном) учете в системе государственного социального страхования [Электронный ресурс] : Закон Респ. Беларусь, 6 янв. 1999 г., № 230-З : принят Палатой Представителей 16 дек. 1998 г. : одобр. Советом Респ. 19 дек. 1998 г. : в ред. Закона Респ. Беларусь от 10.12.2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023

13. **Об информации**, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : принят Палатой Представителей 9 окт. 2008 г. : одобр. Советом Респ. 22 окт. 2008 г. : в ред. Закона Респ. Беларусь от 10.10.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023

14. **О мерах** по совершенствованию защиты персональных данных военнослужащих [Электронный ресурс] : Указ Президента Респ. Беларусь, 28 окт. 2021 г., № 422 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

15. **О совершенствовании** государственного регулирования в области защиты информации [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 дек. 2019 г., № 449 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

16. **Об утверждении** Положения о порядке создания и ведения автоматизированной информационной системы персональных данных пассажиров воздушных судов [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 15 июля 2015 г., № 593 : в ред. постановления Совета Министров Респ. Беларусь от 12.11.2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

17. **Об установлении** порядка обезличивания персональных данных, содержащихся в регистре населения [Электронный ресурс] : постановление М-ва внутренних дел Респ. Беларусь, 27 сент. 2012 г., № 341 : в ред. постановления М-ва внутренних дел Респ. Беларусь от 14.03.2020 г. //

до 19 июня 2021 г., по ст. 203[1] УК. Полагаем, что данная ситуация должна разрешаться по правилам ст. 9 УК.

Во-первых, преступность и наказуемость деяния определяются законом, действовавшим во время совершения этого деяния. Со дня вступления в силу закона, устраняющего преступность деяния, соответствующее деяние, совершенное до его вступления в силу, не считается преступным. Следовательно, со вступлением в силу Закона № 112-З уголовная ответственность за незаконные собирание либо распространение информации о частной жизни исключается.

Во-вторых, в части шестой ст. 104 Конституции Республики Беларусь установлено, что закон не имеет обратной силы, за исключением случаев, когда он смягчает или отменяет ответственность граждан. В УК эта конституционная формула трансформирована в 3 логические ситуации. Уголовный закон а) устанавливающий преступность деяния, б) усиливающий наказание или в) иным образом ухудшающий положение лица, совершившего это деяние, обратной силы не имеет.

Криминализация. Приведенный выше анализ объективных и субъективных признаков состава незаконных действий в отношении информации о частной жизни и персональных данных (ст. 203[1] УК) позволяет утверждать о криминализации более широкого спектра деяний, нежели в ст. 179 УК. Следовательно, сфера действия уголовно-правового запрета расширилась.

Пенализация. Произошло усиление наказания за совершение рассматриваемого преступления. По категории ч. 1 ст. 179 УК относилась к преступлениям, не представляющим большой общественной опасности (наиболее суровое наказание – арест), а ч. 2 – менее тяжким преступлениям (лишение свободы на срок до 3 лет со штрафом). Несмотря на то, что ч. 1 ст. 203[1] УК относится к преступлениям, не представляющим большой общественной опасности, санкция данной уголовно-правовой нормы дополнена такими видами наказаний, как ограничение свободы и лишение свободы на срок до двух лет. В свою очередь, ч. 2 ст. 203[1] УК,

Одним из районных судов г. Минска гражданин Г. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 179 УК. Судом было установлено, что в течение 2008 года и по 22 апреля 2009 г. он незаконно собирал и распространял сведения о частной жизни гражданки М. без ее согласия. Так, 20 сентября 2008 г. и дважды 31 октября 2008 г. с использованием компьютерно-множительной техники Г. изготовил заведомо поддельный оттиск печати государственной нотариальной конторы, которую разместил в поддельной доверенности, якобы выданной ему гражданкой М., и незаконно получил в центрах обслуживания клиентов одного из сотовых операторов детализацию исходящих звонков абонентского номера (за июнь, сентябрь, декабрь 2007 года, январь, март–июль 2008 года), принадлежащего М. Часть незаконно полученной детализации (за декабрь 2007 года и май 2008 года) Г. распространил, предъявив их 15 декабря 2008 г. в судебном заседании на бракоразводном процессе с М., причинив тем самым вред ее правам, свободам и законным интересам. Помимо этого, гражданин Г. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 380 УК, т.е. в подделке официального документа, предоставляющего права, в целях использования такого документа самим исполнителем, а также в использовании заведомо подложного документа.

Полагаем, что расширение сферы уголовно-правового запрета позволит давать адекватную уголовно-правовую оценку нарушению анонимности, заключающееся в публикации персональных данных граждан.

Таким образом, по сути, в ст. 203^1 УК была перенесена диспозиция ст. 179 УК, утратившей силу в связи с принятием Закона № 112-З, что тоже порождает определенные вопросы в правоприменении. Так, достаточно интересным представляется вопрос о возможности квалификации деяний, содержащих признаки состава преступления, ответственность за совершение которого была предусмотрена ст. 179 УК, и имевших место

ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

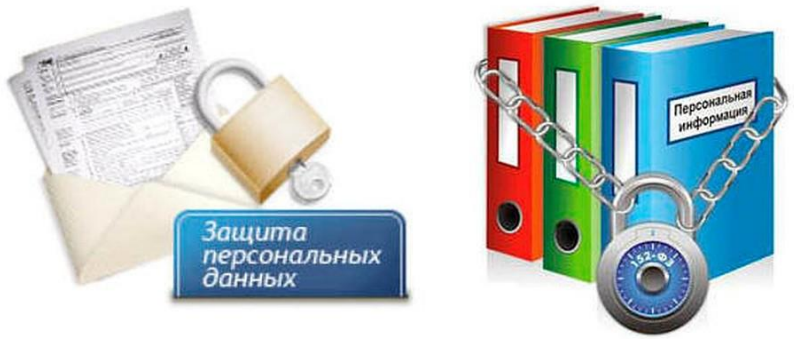
18. **Об установлении** образцов электронных документов, содержащих персональные данные физических лиц, вносимые Министерством внутренних дел Республики Беларусь в регистр населения [Электронный ресурс] : постановление М-ва внутренних дел Респ. Беларусь, 18 сент. 2017 г., № 262 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

19. **Об обучении** по вопросам защиты персональных данных [Электронный ресурс] : приказ Оперативно-аналит. центра при Президенте Респ. Беларусь, 12 нояб. 2021 г., № 194 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

20. **О государственном** информационном ресурсе «Реестр операторов персональных данных» [Электронный ресурс] : приказ Оперативно-аналит. центра при Президенте Респ. Беларусь, 1 июня 2022 г., № 94 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

21. **О мерах** по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 [Электронный ресурс] : приказ Оперативно-аналит. центра при Президенте Респ. Беларусь, 20 февр. 2020 г., № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

22. **Рекомендации** об обработке персональных данных в связи с трудовой (служебной) деятельностью [Электронный ресурс] : рекомендации Нац. центра защиты персональных данных Респ. Беларусь, 18 янв. 2022 г., : в ред. Рекомендации Нац. центра защиты персональных данных Респ. Беларусь от 9 июня 2022 г. // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.



ПОНЯТИЕ «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» В СОВРЕМЕННОМ ПРАВЕ

С каждым годом современный человек все больше и больше времени проводит в онлайн среде. Становится очевидно, что она постепенно вытесняет офлайн среду из всех сфер общественной жизни. В режиме онлайн человек заказывает товары и услуги, общается с другими людьми, оплачивает счета, совершает административные процедуры и т.д. При этом, участвуя в информационном взаимодействии с иными индивидами, обществом и государством, человек представляет сведения, позволяющие его идентифицировать. Такие сведения получили название «персональные данные». При этом сам термин «персональные данные» явление не новое, однако с развитием информационно-коммуникационных технологий, позволяющих обрабатывать и хранить огромные массивы информации (так называемые big data технологии), стирается грань между определением персональных и неперсональных данных. Таким образом, изучение того, что входит в понятие «персональные данные» приобретает особую актуальность.

В Республике Беларусь базовым нормативным документом, закрепляющим понятие персональных данных, является Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации,

Субъект преступления в ст. 203[1] УК – общий, т.е. физическое лицо, достигшее 16-летнего возраста, находившееся в состоянии вменяемости в момент совершения общественно опасного деяния.

Субъективная сторона (ст. 203[1] УК) выражена умышленной формой вины в виде как прямого, так и косвенного умысла. Виновный сознает, что совершает деяния, направленные на нарушение установленного законодательством порядка оборота информации о частной жизни и персональных данных, предвидит неизбежность или возможность причинения вреда правам, свободам и законным интересам гражданина и желает наступления указанных последствий либо не желает, но сознательно допускает их наступление либо относится к ним безразлично. Мотивы и цели указанных действий на квалификацию не влияют.

В ч. 3 ст. 203[1] УК в качестве квалифицирующего признака предусмотрено совершение деяния в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга. Это означает, что потерпевшим помимо непосредственно гражданина могут выступать и его близкие (близкие родственники и члены семьи потерпевшего либо иные лица, которых потерпевший обоснованно признает своими близкими). Под осуществлением служебной деятельности следует понимать законные действия любого лица, входящие в круг его служебных обязанностей, вытекающих из трудового договора (контракта) с государственными, частными и иными зарегистрированными в установленном порядке предприятиями и организациями независимо от формы собственности, а также с предпринимателями, выполнение общественного долга – осуществление гражданином как специально возложенных на него обязанностей в интересах общества или законных интересах отдельных лиц, так и других общественно полезных действий.

Практика применения ст. 179 УК, как правило, ограничивалась сферой конфликтов в бытовой сфере, что подтверждается следующим примером.

произошла определенная декриминализация. Вместе с тем не вполне ясно, как решать вопрос о применении правил об обратной силе уголовного закона, в случае если до 19 июня 2021 г. потерпевшему в результате незаконного собирания сведений о его частной жизни уже был причинен существенный вред.

Объективная сторона состава преступления (ч. 2 ст. 203[1] УК) состоит из деяния (незаконное распространение), общественно опасных последствий (причинение существенного вреда правам, свободам и законным интересам гражданина) и причинной связи между ними.

Распространением является раскрытие информации о частной жизни и (или) персональных данных другого лица неопределенному кругу лиц. Именно в этом заключается отличие распространения от предоставления сведений. При распространении всегда преследуется цель ознакомить с данными неопределенный круг лиц, в то время как при предоставлении – индивидуально-определенное лицо. Способами распространения могут быть устное или письменное сообщение, размещение в глобальной компьютерной сети Интернет, публичная демонстрация или упоминание и т.п.

Обязательным условием наступления уголовной ответственности по ст. 203[1] УК является отсутствие согласия потерпевшего на действия с информацией о частной жизни и (или) персональными данными. Требования к форме получения согласия для обработки персональных данных, а также к его содержанию установлены ст. 5 Закона № 99-З. Так, согласие субъекта может быть получено в письменной форме, в виде электронного документа или в иной электронной форме. Что же касается получения согласия на доступ к информации о частной жизни, то, как правило, этот порядок регулируется специальным законодательством (Закон Республики Беларусь от 21 июля 2008 г. № 418-З «О регистре населения», Закон Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» и др.). Кроме того, получение сведений о частной жизни гражданина без его согласия возможно в уголовном процессе и оперативно-розыскной деятельности.

информатизации и защите информации». Однако это далеко не единственный правовой акт Республики Беларусь, в котором присутствует термин «персональные данные». Помимо вышеназванного Закона, понятие персональных данных закреплено более чем в двадцати нормативных актах. Исходя из цели принятия и сферы правового регулирования общественных отношений, весь массив нормативных документов можно разделить на несколько групп. Первую группу правовых актов образуют международные договоры, заключенные между Республикой Беларусь и иными участниками международных отношений. Содержащиеся в международных договорах определения персональных данных достаточно разнообразны, а их специфика обусловлена тем кругом общественных отношений, на которые распространяется действие данных нормативных документов. Так, например, в состав первой группы входит ряд модельных правовых актов, выполняющих гармонизирующую и консолидирующую функции. Перечень вопросов, урегулированных данной группой нормативных документов, достаточно обширен: отношения, возникающие в сфере оборота персональных данных в целом; регуляция отношений, связанных с хранением, обработкой, передачей информации и обеспечением информационной безопасности; правовое регулирование оборота персональных данных при проведении национального референдума. Однако понятие персональных данных, содержащихся в модельных актах, носят узконаправленный характер и обусловлены той спецификой отношений, на регулирование которых направлены данные нормативные акты. Также в первую группу правовых актов, закрепляющих понятие персональных данных, входят двусторонние соглашения, заключенные с иностранными государствами. Сфера действия данного рода нормативных документов еще более специализирована, чем в модельных актах. Так, например, Республикой Беларусь заключено Соглашение о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их

развитии, и использовании в государствах – участниках СНГ; двусторонними соглашениями с рядом иностранных государств урегулированы вопросы реадмиссии, а также сотрудничества и взаимной помощи в таможенных делах; заключены договоры о почтовых платежных услугах. Таким образом, термин «персональные данные», содержащийся в двусторонних соглашениях, трактуется узконаправленно, исходя из цели заключения данного рода договоров.

Национальные правовые акты, закрепляющие понятие «персональные данные», образуют вторую группу нормативных документов. В Законе Республики Беларусь от 21 июля 2008 г. № 419-З «О Государственной границе Республики Беларусь», исходя из цели его принятия, понятие персональных данных носит ограничительный характер и отражает лишь те данные, которые нужны физическому лицу для въезда в Республику Беларусь или выезда из ее пределов. Аналогичный узконаправленный характер носит определение персональных данных, закрепленное в Законе Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения». Расширяет понятие персональных данных определение, закрепленное в уже упомянутом выше Законе Республики Беларусь «Об информации, информатизации и защите информации», при этом, норма, содержащаяся в вышеназванном нормативном документе, является бланкетной по отношению к норме, закрепленной в Законе Республики Беларусь от 21 июля 2008 г. № 418-З «О регистре населения». Так, в Законе «Об информации, информатизации и защите информации» под персональными данными понимаются основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо. В Законе «О регистре населения» указан исчерпывающий перечень данных, отнесенных к основным и дополнительным. Однако стоит понимать, что сферой регулирования Закона «О регистре населения» является внесение

широкого понятия – обработка персональных данных (ст. 1 Закона № 99-З). Полагаем, что в тексте уголовного закона применению подлежит устоявшаяся лексика (собирание).

Под предоставлением информации о частной жизни и (или) персональных данных другого лица без его согласия следует понимать действия, направленные на ознакомление с их содержанием третьего лица. Появление в законе новой формы общественно опасного поведения обусловлено тем, что далеко не всегда собирание сведений осуществляется без помощи сторонних лиц. Например, лицо для сбора данных о частной жизни другого лица подкупает работника игорного или увеселительного заведения. По ранее действующему законодательству (ст. 179 УК) деяния работника можно было при определенных условиях рассматривать как распространение сведений о частной жизни. Вместе с тем факт опубликования сведений, например, о слишком частом посещении потерпевшим, являющимся публичным лицом, игорного заведения в средствах массовой информации явно вредоноснее, нежели предоставление такой информации какому-либо конкретному лицу. Таким образом, по аналогии с другими корреспондирующимися уголовно-наказуемыми деяниями (дача/получение взятки) криминализирована не только деятельность по сбору конфиденциальной информации, но и ее предоставлению.

Состав преступления материальный. Преступление признается оконченным с момента причинения существенного вреда правам, свободам и законным интересам гражданина. Такой вред может иметь как имущественный, так и неимущественный характер. Это может быть выражено в опорочивании деловой репутации, моральных либо психических переживаниях, заболевании, отказе в приеме на работу, упущенной выгоде от незаключенной сделки и т.п. Следует обратить внимание, что в ст. 179 УК речь шла о «причинении вреда правам, свободам и законным интересам потерпевшего». Следовательно, в части описания общественно опасных последствий рассматриваемого деяния

и достоинство потерпевшего. Человек имеет право на секретность и положительной информации о себе.

При этом следует учитывать, что информация о частной жизни и персональные данные – это не абсолютные категории. К примеру, желание человека сохранить в тайне совершенное им и нераскрытое преступление не является законным интересом и, соответственно, не может охраняться положениями ст. 203^1 УК.

Объективная сторона состава преступления (ч. 1 ст. 203^1 УК) состоит из деяния (незаконные сбор и предоставление), общественно опасных последствий (причинение существенного вреда правам, свободам и законным интересам гражданина) и причинной связи между ними.

Сбор и предоставление информации должны быть незаконными, т.е. совершаться в нарушении установленного законодательством порядка.

Для описания одной формы деяния законодателем использован термин «сбор», который не характерен для УК 1999 года. Как правило, в УК используется формулировка «собирание» (ч. 1 ст.ст. 254, 358, 375^1 и др.). Собирание рассматривают как процесс, а не как оконченное действие. Поэтому в содержание данного понятия входят любые начавшиеся и продолжающиеся целенаправленные незаконные действия виновного, в результате которых он получает определенную информацию. Использование термина «сбор» может обусловить постановку вопроса о том, что уголовно-правовой оценке подлежат лишь оконченные действия, т.е. непосредственное аккумулирование некого объема информации. Способы сбора могут быть тайными и открытыми. Это наблюдение, подслушивание, фотографирование, видеозапись, ознакомление с документами, приобретение письменных свидетельств, опросы родственников или сослуживцев, а также любое иное несанкционированное приобретение сведений о частной жизни или персональных данных потерпевшего, в том числе с использованием глобальной компьютерной сети Интернет. Вместе с тем нельзя не отметить, что в УК использована терминология специального законодательства. И сбор, и предоставление сведений – это элементы более

и актуализация персональных данных в регистр населения Республики Беларусь.

Таким образом, в Республике Беларусь реализован секторальный подход к закреплению понятия «персональные данные», во многом норма, содержащая легальное определение, зависит от целей принятия того или иного правового акта, а также от сферы общественных отношений, регулируемых нормативным документом. Можно констатировать тот факт, что в Республике Беларусь назрела необходимость в принятии межотраслевого нормативного документа, комплексно регулирующего отношения в сфере защиты персональных данных, в котором понятие персональных данных будет гибким, а также сможет отвечать современному уровню развития информационно-коммуникационных технологий. Стоит отметить, что такой документ уже подготовлен. Так, Национальным центром законодательства и правовых исследований Республики Беларусь был разработан и внесен на рассмотрение Национального собрания Республики Беларусь законопроект «О персональных данных». Однако после второго чтения данный проект закона был отправлен на доработку.

Как уже отмечалось выше, понятие «персональные данные» явление не новое. Впервые на международном уровне данная правовая категория появилась в тексте Директивы Организации по экономическому сотрудничеству и развитию «О защите неприкосновенности частной жизни и международных обменов персональными данными» в 1982 г. Под персональными данными в абзаце б. п. 2 Директивы понимается любая информация, относящаяся к индивидууму («субъекту данных»), чья личность либо известна, либо может быть установлена. Заложенные в данной Директиве основы достаточно расширительного толкования понятия «персональные данные» в последующем были учтены и в тексте Конвенции Совета Европы «О защите частных лиц в отношении автоматизированной обработки данных личного характера». Фактически легальные

определения персональных данных, содержащиеся в Конвенции и Директиве, ничем не отличаются друг от друга. Однако в отличие от Директивы Конвенция Совета Европы обязывает государства-участники, присоединившиеся к ней, имплементировать нормы Конвенции в национальное законодательство. Большинство европейских государств, а в последующем не только европейских (так как Конвенция носит открытый характер, присоединиться к ней могут государства, не являющиеся членами Совета Европы), пошли по пути закрепления абстрактного, максимально широкого понятия персональных данных, реализованного в Конвенции. Приведем лишь несколько примеров: в Органическом законе Испании 15/1999 от 13 декабря 1999 г. «О защите персональных данных» правовая трактовка понятия персональных данных закреплена в абзаце а артикула 3, в котором под персональными данными понимается любая информация, касающаяся идентифицированных или идентифицируемых физических лиц; в Великобритании Закон «О защите данных» определяет персональные данные как любую информацию, относящуюся к идентифицированному или идентифицируемому живому лицу; в п. 1 § 46 немецкого Федерального закона «О защите данных» правовая категория персональных данных понимается как любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъекту данных»); в п. 1 ст. 3 Федерального закона Российской Федерации «О персональных данных» под персональными данными понимают любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). Помимо вышеназванных стран, аналогичная, максимально широкая и абстрактная модель к определению понятия «персональные данные» реализована в Швеции, Франции, Нидерландах, Сингапуре, Украине, Казахстане, Аргентине и ряде других государств.

• незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203^1);

• несоблюдение мер обеспечения защиты персональных данных (ст. 203^2).

Статья $2O3^1$. Незаконные действия в отношении информации о частной жизни и персональных данных

По сути, в рамках одной нормы, предусмотренной ст. 203^1 УК, установлены два самостоятельных состава преступления. В ч. 1 ст. 203^1 УК предусмотрена ответственность за 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, а в ч. 2 ст. 203^1 УК – умышленное незаконное распространение информации о частной жизни и (или) персональных данных другого лица без его согласия, повлекшее аналогичные последствия. Такой прием иногда используется при построении уголовно-правовых запретов для более лаконичного изложения текста закона (ст.ст. 159, 201, 261^1, 294, 328 УК и др.).

Непосредственным объектом в ст. 203^1 УК являются общественные отношения, возникающие по поводу охраны информации о частной жизни и защите персональных данных. Важность данного уголовно-правового запрета заключается в необходимости установления и защиты границ индивидуальной свободы человека в различных аспектах проявления для обеспечения невмешательства в эти сферы со стороны любых других лиц.

Предмет преступления – информация о частной жизни и персональные данные. Информация о частной жизни – конфиденциальная информация, оберегаемая ее владельцем от пользования другими людьми, обеспечивающая его покой и уверенность в себе именно при условии нераспространения. Следует отметить, что сами эти сведения не обязательно должны порочить честь

о частной жизни (ст. 179 Уголовного кодекса Республики Беларусь (далее – УК));

• нарушение неприкосновенности жилища и иных законных владений граждан (ст. 202 УК);

• нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203 УК).

По сути, в национальном уголовном законе были воспроизведены положения модельного уголовного кодекса для государств – участников Содружества Независимых Государств. В частности, в главе 21 «Преступления против конституционных прав и свобод человека и гражданина» модельного УК предусматривались нормы о незаконном собирании и распространении информации о частной жизни (ст. 151), нарушении тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 153), нарушении неприкосновенности жилища (ст. 154).

С принятием и вступлением в силу Закона Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» (далее – Закон № 112-З) положения отечественного УК были скорректированы. Так, из текста кодекса была исключена ст. 179 УК, а глава 23 была дополнена ст.ст. 203^1 и 203^2, устанавливающими ответственность за незаконные действия в отношении информации о частной жизни и персональных данных и несоблюдение мер обеспечения защиты персональных данных соответственно. Таким образом, с 19 июня 2021 г. совокупность уголовно-правовых норм, направленных на охрану неприкосновенности частной жизни и персональных данных, включает:

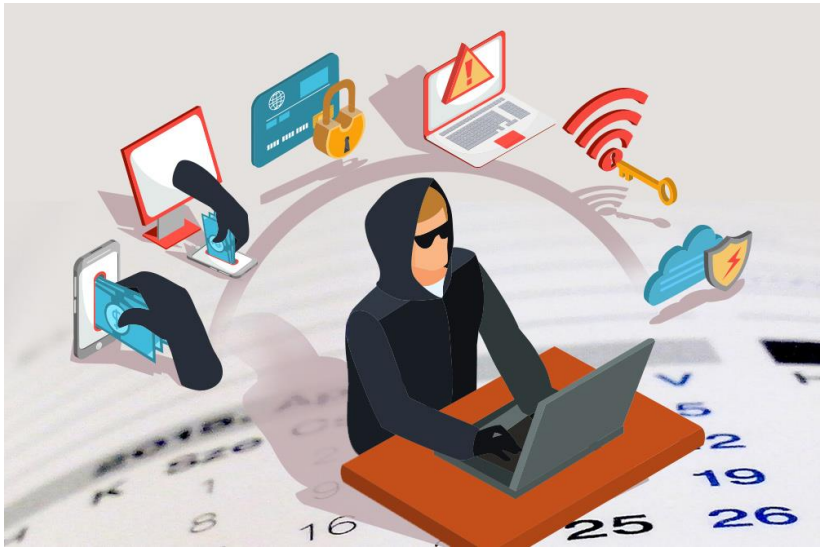
• нарушение неприкосновенности жилища и иных законных владений граждан (ст. 202);

• нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203);

Помимо Конвенции Совета Европы «О защите частных лиц в отношении автоматизированной обработки данных личного характера», в рамках Европейского Союза действует еще один нормативный документ, закрепивший понятия персональных данных. Им является Общий регламент по защите данных, принятый в 2016 году, а вступивший в силу в 2018 году. Данный Регламент пришел на смену ранее действующей Директиве 95/46/ЕС «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных». Как и в Конвенции, термин «персональные данные» Регламент трактует максимально абстрактно. Однако отличительной чертой понятия персональных данных, закрепленного в Регламенте, является наличие примерного перечня идентификаторов, на основании которых лицо может быть идентифицировано. Так, в абз. 1 арт. 4 установлено, что персональные данные – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъект данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько характерных для указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности. На наш взгляд, включение в понятие персональных данных примерного перечня идентификаторов является обоснованным, так как позволяет детализировать абстрактную дефиницию, при этом уточняя перечень данных, однозначно отнесенных к персональным, со всеми вытекающими требованиями к обработке и защите данного рода информации. Стоит отметить, что после вступления в силу Регламента, ряд государств Европейского Союза (Германия, Великобритания и др.) скорректировали понятие персональных данных путем включения в него примерного

перечня идентификаторов. Таким образом, законодательство европейских стран, а также законодательство Японии (п. 1 арт. 2 Акта о защите персональной информации) используют смешанный подход в определении понятия персональных данных: с одной стороны, правовая дефиниция носит абстрактный характер, а с другой – понятие персональных данных уточняется путем включения в него примерного перечня данных, однозначно являющихся персональными.

Иной подход к определению понятия «персональные данные» реализован в Соединенных Штатах Америки. В США термин «персональные данные» не используется. Вместо него применяются понятия «конфиденциальная информация», «личная информация» и «информация, идентифицирующая личность». Для США характерно закрепление вышеназванных понятий в зависимости от сферы человеческой деятельности: здравоохранение, финансы, сектор государственного управления, защита детей и т.д. Так, например, в Законе о защите частной жизни в сфере видеопроката (The US Video Privacy Protection Act of 1988) используется термин «информация, идентифицирующая личность», под которой понимают любую информацию, которая определяет лицо. Для финансового сектора используется иное понимание персональных данных. Однако наиболее типичное для США определение персональных данных строится через перечисление категорий информации, относящихся к персональной. Например, Законом о защите частной жизни детей в онлайновой среде, к персональным данным несовершеннолетнего относятся: имя и фамилия, адрес проживания, адрес электронной почты или идентификатор в мессенджере, номер телефона, номер карты социального страхования, онлайн идентификатор (уникальный идентификатор в cookie-файле, IP-адрес, уникальный номер устройства и т.п.), аудио, фото и видео, содержащие изображение или голос несовершеннолетнего, геолокационная информация, позволяющая идентифицировать улицу или город местонахождения лица, любая иная информация, которую оператор



УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ И ПЕРСОНАЛЬНЫХ ДАННЫХ В СВЕТЕ ИЗМЕНЕНИЙ УГОЛОВНОГО ЗАКОНА

В Конституции Республики Беларусь 1994 года закреплено право на неприкосновенность частной жизни. В ст. 28 Основного Закона Республики Беларусь установлено, 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 целях восстановления человеком его права на охрану персональных данных, в том числе на неприкосновенность частной жизни, установлено ответственность за совершение соответствующих деяний. Наиболее суровым видом ответственности является уголовная. До 19 июня 2021 г. совокупность уголовно-правовых норм, направленных на охрану неприкосновенности частной жизни, как правило, включала:

- незаконные собирание либо распространение информации

− ликвидации юридического лица, смерти заявителя или получателя персональных данных;

− нарушения требований Закона;

− если представленных заявителем документов недостаточно, чтобы сделать вывод о надлежащей защите прав субъектов персональных данных, в т.ч. когда правовые, организационные и технические меры, принимаемые получателем персональных данных, не являются достаточными для обеспечения их защиты, находятся на низшем уровне, чем обеспеченные законодательством Республики Беларусь.

В любой момент до окончания трансграничной передачи НЦЗПД может отозвать разрешение, если:

− заявителем или получателем персональных данных нарушены условия, в соответствии с которыми осуществлялась выдача разрешения;

− получена информация, подтверждающая, что на территории иностранного государства не обеспечивается уровень защиты персональных данных не ниже, чем это предусмотрено законодательством Республики Беларусь.

В случае отзыва разрешения заявитель незамедлительно уведомляется об этом, но не позднее дня, следующего за днем принятия такого решения.

Если ведем речь про трансграничную передачу, то она распространяется на все персональные данные или есть исключения?

− Трансграничная передача – способ обработки персональных данных.

Таким образом, в законодательстве нет исключений к определению персональных данных при их передаче на территорию иностранного государства. Следовательно, под персональными данными в таком случае нужно понимать любые данные о физическом лице, которые его идентифицируют или могут идентифицировать.

собирает о несовершеннолетнем или его законном представителе и соединяет с одним из вышеуказанных видов данных. Помимо федеральных законов, понятие «персональные данные» закреплено и в законах каждого отдельного штата (за исключением Южной Дакоты и Алабамы). Во многом закрепленные определения понятия персональных данных соответствуют федеральным законом. Исключением является лишь законодательство Калифорнии, на которое существенное влияние оказал Общий регламент по защите данных. Обусловлено это тем, что в Калифорнии находится так называемая «кремниевая долина», в которой расположены штаб-квартиры большинства крупный IT-компаний (Google, Facebook, Apple и т.д.). Так, например, в Законе о защите частной жизни потребителей (California Consumer Privacy Act) используется дефиниция, которая максимально схожа по своему объему на ту, что закреплена в европейском регламенте по защите данных. Таким образом, в большинстве случаев в США используется секторальный подход к определению понятия «персональные данные». Во многом формулировка понятия зависит от той сферы общественной жизни, в которой оно используется.

Анализируя современные подходы к правовому закреплению понятия «персональные данные», можно прийти к выводу, что в большинстве государств преобладает достаточно расширительное толкование данного термина, а само определение носит максимально абстрактный характер.

Проанализированы различные подходы к определению понятия «персональные данные». Структурно данные подходы можно разделить на три категории. Первый подход характерен для Республики Беларусь и США, где понятие персональных данных носит узконаправленный, специализированный характер и во многом зависит от сферы применения того нормативного акта, в котором данное определение закреплено. Второй подход характеризуется максимально абстрактным и широким пониманием такой правовой категории, как персональные данные.

Закрепленные в Директиве ОЭСР и Конвенции Совета Европы определения персональных данных послужили основой для последующего развития законодательства ряда государств европейских и не европейских государств (Испания, Швеция, Россия, Сингапур, Казахстан и т.д.).

Третий подход характеризуется смешанным типом определения понятия персональных данных. С одной стороны, термин «персональные данные» трактуется достаточно широко, а само определение является гибким и абстрактным, а с другой стороны, наличие примерного перечня идентификаторов, позволяющих идентифицировать лицо, уточняет абстрактную дефиницию, внося ясность и определенность. На наш взгляд, смешанный подход к определению понятия «персональные данные» является наиболее обоснованным.

передача персональных данных, согласованных заявителем и получателем персональных данных, на дату, предшествующую дате подачи заявления;

− иной документ, в соответствии с которым производится трансграничная передача персональных данных (подтверждающий основания, указанные в части первой ст. 9 Закона № 99-З).

Заявитель может представить и иные документы, подтверждающие гарантии соблюдения прав субъектов персональных данных в иностранном государстве.

В заявлении необходимо указать:

− наименование организации, в которое оно подается (в нашем случае – НЦЗПД);

− сведения о заявителе (наименование организации или ФИО физического лица, адрес, собственноручно проставленную подпись или электронную цифровую подпись);

− в случае если заявитель – юридическое лицо, то представляются документы, подтверждающие его полномочия на подписание такого заявления, а также указывается лицо, ответственное за осуществления внутреннего контроля за обработкой персональных данных;

− сведения о получателе персональных данных (наименование или ФИО и адрес его места жительства(нахождения));

− сведения, относящиеся к передаче персональных данных (цели их обработки получателем, категории обрабатываемых персональных данных, срок хранения получателем, возможные способы защиты прав субъектов персональных данных в случае их нарушения).

Могут ли отказать в передаче данных? Если да, то в каких случаях?

− Заявление на получение разрешения на трансграничную передачу персональных данных рассматривается в течение 30 дней со дня его регистрации. НЦЗПД вправе отказать в выдаче разрешения на трансграничную передачу персональных данных в следующих случаях:

их хранения не допускается);

– получено соответствующее разрешение уполномоченного органа по защите прав субъектов персональных данных (Национальный центр защиты персональных данных Республики Беларусь; далее – НЦЗПД);

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

Каков порядок трансграничной передачи? Необходимо ли получать разрешение?

– Существует два порядка трансграничной передачи данных. Первый порядок – упрощенный и работает в том случае, если на территории иностранного государства обеспечивается надлежащий уровень защиты прав субъектов персональных данных. Такими странами выступают участники Страсбургской Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. В настоящий момент это более 50 стран, ратифицировавших данную Конвенцию. В таком случае соблюдение дополнительных условий со стороны оператора не требуется.

Теперь рассмотрим второй порядок: если трансграничная передача данных осуществляется в иностранное государство, не являющееся членом Страсбургской Конвенции. В таком случае оператор обязан получить разрешение на трансграничную передачу персональных данных в НЦЗПД и согласие самого субъекта персональных данных.

Разрешение НЦЗПД выдается на основании поданного оператором заявления.

Заявление может быть составлено как в письменной форме, так и в виде электронного документа. К заявлению необходимо приложить следующие документы:

– проект договора, которым оформляется трансграничная

НАЦИОНАЛЬНЫЙ ЦЕНТР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

15 ноября 2021 г., для обеспечения надлежащего исполнения Закона Республики Беларусь «О защите персональных данных» был создан Национальный центр защиты персональных данных, который является уполномоченным органом по защите прав субъектов персональных данных и действует в форме государственного учреждения.

Национальный центр защиты персональных данных действует независимо на основе Конституции Республики Беларусь, Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», Положения о Национальном центре защиты персональных данных, утвержденного Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных», и иных актов законодательства.

С первых дней создания Центра упор был сделан на методологическое направление деятельности, упреждение нарушений. Организациям нужно было дать полный набор возможностей для работы по защите прав граждан в соответствии с Законом. О необходимости принятия предусмотренных Законом мер по обеспечению защиты

персональных данных информированы министерства, иные органы госуправления, облисполкомы, бизнес-ассоциации, объединяющие предпринимателей, большинство организаций торговли, банков, страховых организаций и т.п. Были подготовлены необходимые алгоритмы, пошаговые действия, формы документов. Все разработанные Центром материалы, включая ответы на наиболее актуальные вопросы, оперативно размещаются на официальном сайте, Telegram-канале и других социальных сетях. Все образцы, документы, пошаговые алгоритмы действий созданы, чтобы правильно организовать работу юридическим лицом по обработке персональных данных.

Основные задачи и функции

Основными задачами Национального центра защиты персональных данных являются:

- принятие мер по защите прав субъектов персональных данных при обработке их персональных данных;
- организация обучения по вопросам защиты персональных данных.

Национальный центр защиты персональных данных в соответствии с основными задачами выполняет следующие функции:

- осуществляет контроль за обработкой персональных данных операторами (уполномоченными лицами);
- рассматривает жалобы субъектов персональных данных по вопросам обработки персональных данных;
- определяет перечень иностранных государств, на территории которых обеспечивается надлежащий уровень защиты прав субъектов персональных данных;
- выдает разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается

информация, обеспечивается надлежащий уровень защиты прав субъектов персональных данных и используется надежная система для их хранения и использования. В случае если надлежащий уровень защиты персональных данных не может быть предоставлен, трансграничная передача данных запрещена.

Надо ли получать согласие субъекта на трансграничную передачу данных?

− Так как трансграничная передача данных является формой обработки персональных данных, то получение разрешения необходимо. Однако из любого правила есть исключения. В частности, в Положении № 14 отмечается возможность направлять персональные данные в иностранное государство без письменного согласия субъекта. Случаи, при которых получение согласия субъекта персональных данных не требуется, указаны в пп. 2–7 части первой ст. 9 Закона № 99-З:

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

− обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь;

− передача осуществляется органом финансового мониторинга в рамках предотвращения финансирования террористической деятельности, распространения оружия массового поражения и предотвращения легализации доходов, полученных преступным путем;

− получение согласия субъекта персональных данных невозможно, но их передача необходима для защиты жизни, здоровья и иных жизненно важных интересов данного субъекта;

− данные получены на основании договора, заключенного с субъектом персональных данных, и используются для исполнения указанных в нем обязательств (дальнейшее внесение изменений в проект договора в части изменения целей обработки персональных данных, срока

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ: КОГДА ОНА ИМЕЕТ МЕСТО И КАК ЕЕ ОСУЩЕСТВИТЬ

Что представляет собой трансграничная передача персональных данных?

– Термин «трансграничная передача» в прямом своем толковании означает передачу данных «через границу». Так, согласно ст. 1 Закона № 99-З трансграничная передача персональных данных – это передача персональных данных на территорию иностранного государства.

К примеру, организации, находящейся на территории Республики Беларусь, необходимо направить паспортные данные своего сотрудника контрагенту в Германии. В таком случае организации необходимо получить письменное согласие сотрудника и осуществить трансграничную передачу его персональных данных.

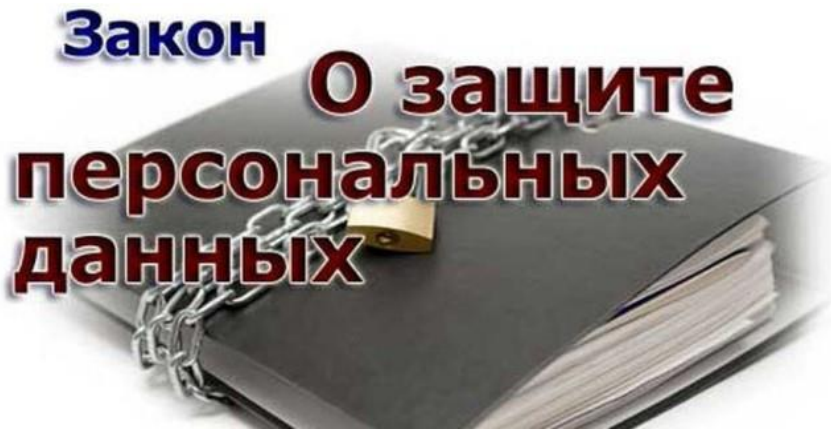
Когда трансграничная передача персональных данных возможна, а когда запрещается?

– Трансграничная передача данных возможна в том случае, если на территории иностранного государства, в которое направляется

надлежащий уровень защиты прав субъектов персональных данных, а также определяет порядок выдачи таких разрешений;

- вносит предложения о совершенствовании законодательства о персональных данных, участвует в подготовке проектов актов законодательства о персональных данных;
- дает разъяснения по вопросам применения законодательства о персональных данных, проводит иную разъяснительную работу о законодательстве о персональных данных;
- определяет случаи, когда не требуется уведомления Национального центра защиты персональных данных о нарушениях систем защиты персональных данных;
- устанавливает классификацию содержащих персональные данные информационных ресурсов (систем) в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных;
- участвует в работе международных организаций по вопросам защиты персональных данных;
- осуществляет сотрудничество с органами (организациями) по защите прав субъектов персональных данных в иностранных государствах;
- ежегодно не позднее 15 марта публикует в средствах массовой информации отчет о своей деятельности;
- реализует образовательные программы дополнительного образования взрослых в соответствии с законодательством об образовании;
- осуществляет иные полномочия, предусмотренные законодательством о персональных данных.

Центром реализуется целый ряд обучающих программ, проводятся семинары, корпоративные обучающие мероприятия, образовательные онлайн-марафоны, практикумы.



СОБЛЮДЕНИЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

С 15 ноября 2021 г. вступил в силу Закон Республики Беларусь от 07.05.2021 «О защите персональных данных» (далее–Закон). Это первый закон, специально посвященный персональным данным в Республике Беларусь. Его положения значительно изменяют и уточняют регулирование обработки персональных данных.

Для начала следует разобраться, кто же такой субъект персональных данных и что понимается под персональными данными?

Субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка его персональных данных. Обработка подразумевает под собой любое действие или совокупность действий, совершаемых с персональными данными. В свою очередь, персональными данными является любая информация, с помощью которой возможно идентифицировать лицо. Это, например, Ф.И.О., номер паспорта, пол, дата рождения, гражданство, место жительства, телефон, биометрические данные и т.п.

Обработка персональных данных осуществляется с согласия субъекта. Таким образом, согласие является базовым основанием для осуществления обработки. Однако в Законе также отражены случаи, при

личный мобильный), может осуществляться без согласия работника, но только непосредственно оператором без распространения или предоставления данной информации иным лицам, если иное не предусмотрено законодательными актами (и только если работник входит в категорию лиц, в отношении которых требуется ведение личного дела).

Предоставление персональных данных работника третьим лицам

Если предоставление персональных данных работника в процессе его трудовой деятельности предусмотрено законодательством, то оно осуществляется без согласия работника.

Например, законодательством о воинском учете предусмотрена обязанность представлять необходимые для занесения в документы воинского учета сведения о гражданах, состоящих или обязанных состоять на воинском учете, законодательством о пенсионном обеспечении – обязанность нанимателей представлять в органы, осуществляющие пенсионное обеспечение, необходимые для назначения пенсий документы, а также сведения о приеме пенсионеров на работу (их увольнении).

Если законодательством предусмотрено представление сведений, содержащих персональные данные уволенных работников, то оно осуществляется также без согласия.

Запрос на предоставление персональных данных должен содержать:

− правовые основания для запроса. Если они не указаны, то необходимо получить согласие субъекта на предоставление персональных данных третьим лицам;

− цель обработки;

− содержание и объем запрашиваемых персональных данных;

− копию согласия субъекта (если оно является основанием для обработки персональных данных).

установлена дисциплинарная ответственность не за разглашение, а за нарушение работником порядка обработки персональных данных. Поэтому в случае разглашения персональных данных привлечение работника к дисциплинарной ответственности за нарушение порядка обработки персональных данных осуществляется независимо от того, было ли подписано обязательство о неразглашении персональных данных.

Поэтому получение от работников обязательства о неразглашении приведет лишь к появлению дополнительного, не основанного на законодательстве документа, содержащего персональные данные работника.

Обязанность соблюдения положений законодательства о персональных данных и принятых в соответствии с ним локальных правовых актов оператора целесообразно закрепить в должностных инструкциях работников.

3. ***Что необходимо учитывать относительно даты рождения и номеров телефонов работника?***

При приеме на работу информация о дате рождения в обязательном порядке заполняется в личном листке по учету кадров, так как его форма утверждена законодательством. Эта личная информация предоставляется нанимателю исключительно для целей трудовых отношений и используется без согласия работника, например, для предоставления гарантий, предусмотренных коллективным договором (выплата материальной помощи на юбилей), для пенсионного обеспечения и т.д.

При этом, как разъясняет НЦЗПД, на случаи, например, поздравления работника коллегами действие Закона № 99-З не распространяется. Основания для получения сведений о днях рождения работников для таких целей в кадровой службе без согласия работника отсутствуют. Данные сведения могут быть получены только у самого работника.

Что касается номера телефона, то графа о телефоне работника также предусмотрена формой личного листка по учету кадров. Обработка таких персональных данных, как номер телефона работника (домашний или

которых обработка персональных данных будет законной и без получения на это согласия.

Перечень таких случаев достаточно широкий и в основном связан с деятельностью государственных структур при осуществлении ими своих функций (ст. 6 Закона). Однако некоторые из них важны и непосредственно применимы в деятельности для субъектов хозяйствования. Так, например, согласие на обработку персональных данных не требуется при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта персональных данных. Также отдельное согласие не требуется, когда физическое лицо указывает персональные данные в документе, подписанном им и адресованном оператору – тому, кто осуществляет обработку персональных данных (запрос, заявление, обращение и т.п.).

Важно! Согласие субъекта персональных данных – это свободное, однозначное, информированное выражение его воли, посредством которого он разрешает обработку своих персональных данных (п. 1 ст. 5 Закона).

До принятия вышеуказанного Закона единственным основанием для сбора, обработки и передачи третьим лицам персональных данных было согласие субъекта данных, предоставленное в письменной форме.

Теперь, с 15 ноября 2021 г., Закон сохраняет возможность фиксации дачи согласия не только в письменной форме, но и в виде электронного документа или в иной электронной форме (например, введение подтверждающего кода из смс-сообщения, проставление отметки «я согласен» в соответствующей форме на сайте и т.п.) (п. 3 ст. 5 Закона).

Закон предоставляет субъекту персональных данных право определенным образом распоряжаться своими персональными данными. Перечень предоставленных прав закреплен в ст. 10–13 Закона, а именно субъекты персональных данных вправе:

- в любое время без объяснения причин отозвать свое согласие

на обработку персональных данных;

- получить информацию об обработке своих персональных данных, при этом не обосновывая свой интерес к запрашиваемой информации;
- изменить персональные данные в случае если они являются неполными, устаревшими или неточными;
- один раз в году бесплатно получить информацию о том, кому (каким третьим лицам) предоставлялись персональные данные субъекта;
- требовать бесплатного удаления персональных данных или прекращения их обработки.

Для реализации вышеуказанных прав субъект персональных данных подает оператору (тому, кто осуществляет обработку персональных данных) заявление в письменном либо электронном виде. Получив такое заявление, оператор обязан в течение 15 дней, а в отношении права на получение информации об обработке персональных данных – 5 дней, выполнить одно из следующих действий:

- предоставить запрашиваемую информацию;
- выполнить запрашиваемые действия;
- отказать в предоставлении информации или выполнении действий.

Если оператор отказался от предоставления информации или выполнения действий, он должен уведомить субъект персональных данных о причине такого отказа. Законом также предусмотрено право субъекта персональных данных на обжалование действия (бездействие) и решения оператора, нарушающие его права при обработке персональных данных: сначала в уполномоченный орган по защите прав субъектов персональных данных, а далее – в суд (ст. 15 Закона).

Таким образом, законодатель создал все необходимые условия для обеспечения соблюдения прав субъектов персональных данных. Особое внимание Закон также уделил мерам по защите персональных данных (ст. 17 Закона). Оператор (уполномоченное лицо) обязан принять

Так как в рассматриваемых ситуациях обработка персональных данных осуществляется в силу законодательства, то согласно Рекомендациям НЦЗПД наниматель не вправе прекратить обработку персональных данных и осуществить их удаление при поступлении от субъекта соответствующего требования. Это обусловлено тем, что у нанимателя есть обязанность соблюдать требования о хранении документов (в т.ч. о приеме на работу), предусмотренных Законом № 323-З и постановлением № 140, принятым в его развитие.

Обработка персональных данных в процессе трудовой деятельности

Приведем некоторые вопросы, возникающие при применении Закона № 99-З.

1. ***Необходимо ли согласие при размещении информации о работниках на интернет-сайтах организаций?***

Согласно Рекомендациям НЦЗПД размещение информации о работниках на сайте организации без их согласия на основании абзаца восьмого ст. 6 Закона № 99-З возможно:

1) в объеме, предусмотренном законодательством. В качестве примера можно привести требования о размещении на интернет-сайте информации о руководителе государственного органа и организации (должность, фамилия, собственное имя, отчество, номер служебного телефона);

2) для рациональной организации труда работника. Например, размещение информации об HR-специалистах, специалистах по работе с клиентами и других работниках, в должностные обязанности которых входит активное контактирование с широким кругом лиц.

2. ***Должны ли работники подписывать обязательство о неразглашении персональных данных?***

Законом № 99-З подписание работниками обязательства о неразглашении персональных данных не предусматривается.

Кроме того, как поясняет НЦЗПД, трудовым законодательством

платы на предыдущем месте работы, указание идентификационного номера, если это не предусмотрено законодательством).

Запрещается передавать резюме кандидата без его согласия третьим лицам, в т.ч. другим нанимателям, если иное не вытекает из содержания резюме.

Обработка персональных данных при оформлении трудовых (служебных) отношений

Согласие субъекта персональных данных на обработку персональных данных, в т.ч. специальных персональных данных, не требуется при оформлении трудовых (служебных) отношений **в случаях, предусмотренных законодательством** (абзац восьмой ст. 6 и абзац третий п. 2 ст. 8 Закона № 99-З). Такими случаями, предусмотренными законодательством, например, являются:

– согласование на должность (ст. 48 Закона № 108-З);

– представление документов при приеме на работу. Например, декларацию о доходах и имуществе обязаны представлять лица, поступающие на государственную службу (ст. 30 Закона № 305-З), медицинскую справку о состоянии здоровья – лица моложе 18 лет; лица, занятые на работах с вредными и (или) опасными условиями труда и т.д.;

– представление характеристики с предыдущего места работы. Право на запрос характеристики является правом нанимателя, предусмотренным законодательством (часть третья ст. 26 ТК). Однако при приеме на работу в государственные органы, иные государственные организации, а также организации, более 50 % акций (долей в уставном фонде) которых находится в государственной собственности, наниматель **обязан** запрашивать характеристику (п. 11 Декрета № 5).

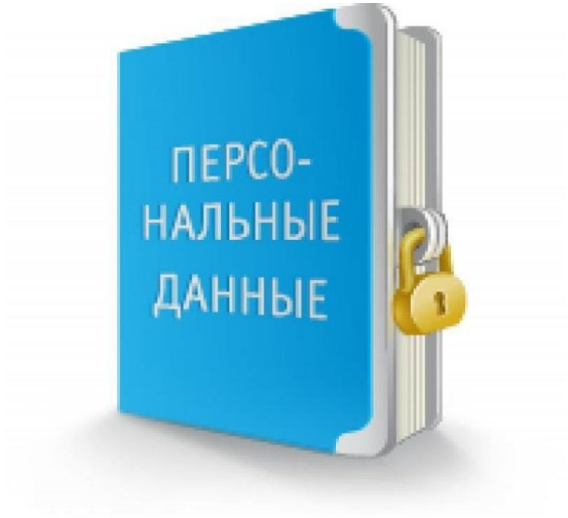
В вышеперечисленных и иных подобных случаях получение согласия субъекта персональных данных на обработку персональных данных не требуется.

правовые, организационные и технические меры по обеспечению защиты персональных данных. То есть организации должны будут скорректировать данные меры с учетом дополнительных требований, которые устанавливаются Законом, а именно:

- назначить структурное подразделение или лицо, ответственное за осуществление внутреннего контроля за обработкой персональных данных либо расширить функции имеющихся подразделений (ответственных лиц);
- разработать политику в отношении обработки персональных данных и сделать ее доступной для неограниченного круга лиц, например, через интернет;
- ознакомить работников с положениями законодательства о защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, а также провести необходимое обучение работников;
- установить порядок доступа к персональным данным;
- принять меры по осуществлению на должном уровне технической и криптографической защиты персональных данных.

Законодательством также предусмотрена административная и уголовная ответственность за нарушения в сфере персональных данных. Еще возмещению подлежит моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Важно соблюдать права субъектов персональных данных, т.к. в случае их нарушения могут наступить неблагоприятные последствия, как для самих субъектов, так и для лиц, осуществляющих обработку таких данных.



ДЕФИНИЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Поступающие в Национальный центр защиты персональных данных (далее – НЦЗПД) запросы организаций зачастую содержат вопросы об отнесении тех или иных сведений к персональным данным. Характерной чертой таких запросов является стремление операторов (уполномоченных лиц) обосновать непризнание конкретных сведений персональными данными и тем самым сузить дефиницию персональных данных.

Довольно распространенными являются ссылки на то, что поскольку та или иная информация не содержит фамилии, имени, отчества (ФИО), 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 могут быть 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, вероятность ошибки.

Позицию сторонников «узкого» понимания персональных данных

Как указано в Рекомендациях НЦЗПД, порядок работы с резюме во втором варианте зависит от используемого алгоритма его обработки.

Отметим сразу, что согласие субъекта персональных данных не потребуется, так как документ подписан лично субъектом персональных данных (абзац 16 ст. 6 Закона № 99-З).

Если информация из резюме не вносится в картотеки, базы данных и т.д., то такая обработка вообще не подпадает под действие Закона № 99-З. Если полученные от соискателей резюме группируются по определенным критериям или вносятся в информационные ресурсы (системы, базы данных), то эти действия подпадают под предмет регулирования Закона № 99-З.

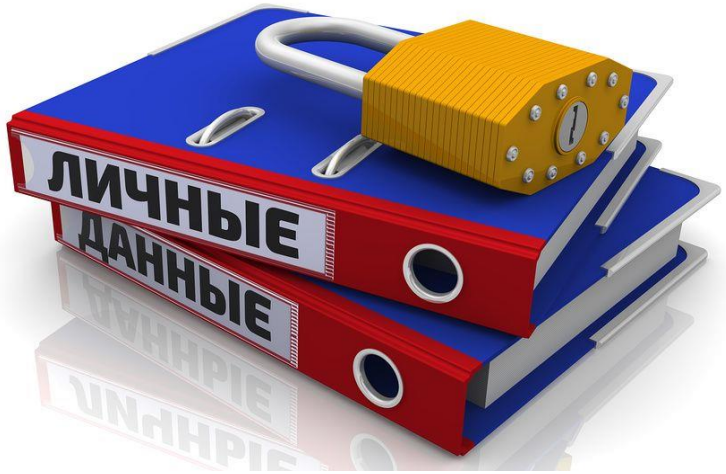
Вариант 3. Заполнение анкеты на сайте нанимателя.

В данном случае наниматель (оператор) должен:

– получить согласие субъекта персональных данных на обработку его персональных данных, например, посредством проставления соответствующей отметки на интернет-ресурсе;

– предоставить субъекту персональных данных необходимую информацию, содержащую в т.ч. перечень действий с персональными данными, на совершение которых дается согласие субъекта персональных данных, общее описание используемых оператором способов обработки персональных данных, срок, на который дается согласие субъекта персональных данных.

Следует также помнить, например, об исключении избыточности обрабатываемых персональных данных по отношению к заявленным целям их обработки, обеспечении соответствия содержания и объема обрабатываемых персональных данных заявленным целям их обработки. НЦЗПД отмечает, что довольно распространены нарушения, когда наниматель посредством резюме осуществляет сбор данных о кандидате, которые не имеют отношения к выполнению планируемой работы (например, сбор информации о его родственниках, размере заработной



КАК ОБРАБАТЫВАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В СФЕРЕ ТРУДОВЫХ ОТНОШЕНИЙ: НЦЗПД ДАЛ РЕКОМЕНДАЦИИ

Обработка персональных данных соискателей на трудоустройство

Основания обработки персональных данных соискателя на трудоустройство зависят от способа подачи информации, содержащей персональные данные, потенциальному нанимателю.

Вариант 1. Направление резюме на электронную почту потенциального нанимателя.

В данном случае необходимо согласие претендента на обработку резюме. То есть наниматель, получивший резюме, должен, например, отправить претенденту письмо на электронную почту, с которой получено резюме, с информацией о необходимости дачи согласия претендента на его обработку. В противном случае резюме подлежит удалению.

Вариант 2. Направление резюме нанимателю в письменной форме с подписью претендента (либо передача его в ходе личного приема).

можно объяснить желанием уменьшить издержки организаций 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 аттестации такой системы, что требует немалых финансовых затрат. Соответственно, операторы пытаются избежать таких 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, «узкий» подход к персональным данным 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 ФИО лица.

Подобный подход 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.

Более того, нередко для обработки персональных данных оператору не требуется знать ФИО конкретного лица, чтобы оценивать или оказывать влияние на него. Отслеживание поведения на сайтах, оценка предпочтений на основе анализа просмотренной информации позволяют прогнозировать с высокой степенью точности индивидуальные предпочтения и использовать данную информацию, в том числе для

оказания влияния на человека.

Ответом на соответствующие риски, которые несут новейшие технологии, во многих странах становится постепенное расширение круга сведений, которые должны относиться к персональным данным. Яркой иллюстрацией являются положения наиболее известного акта в сфере защиты персональных данных – GDPR. Так, в GDPR все онлайн-идентификаторы прямо отнесены к персональным данным, что должно положить конец дискуссиям о том, является ли, например, IP-адрес персональными данными или нет.

В русле данного подхода дефиниция персональных данных в Законе также широко определяет круг сведений, относящихся к персональным данным, по сравнению с подходом, отраженным в Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

Сторонники «узкого» подхода в связи с этим отмечают, что определение персональных данных становится слабо предсказуемо и при желании к персональным данным можно отнести практически любые сведения.

Как и в большинстве подобных ситуаций, истина где-то посередине. С одной стороны, сужение определения персональных данных хотя и делает данное определение более ясным и четким, но во многом выхолащивает его, выводя из-под правовой защиты многие бизнес-процессы, порожденные развитием информационных технологий (профилирование, прямой маркетинг и др.). С другой стороны, чрезмерное его расширение может привести к созданию нерабочего механизма всеобъемлющего регулирования всего имеющегося объема информации.

Сложность в определении границ рассматриваемого понятия в отечественных реалиях дополнительно обусловливается и его новизной в существующей редакции, отсутствием наработанной правоприменительной практики, которая только начинает формироваться.

В подобной ситуации существует настоятельная потребность

а также от иных неправомерных действий в отношении персональных данных.

Административная ответственность установлена ст. 23.7 КоАП.

Если субъекту персональных данных причинен вред, в т.ч. моральный, действиями оператора или уполномоченного лица, то он может обратиться с иском к оператору, который, в свою очередь, может требовать привлечения уполномоченного лица к ответственности за нарушение условий договора (ст. 7 Закона № 99-З).

Оператор также несет ответственность за случаи «утечки» персональных данных, допущенные уполномоченным лицом на территории иностранного государства.

В связи с этим операторам следует тщательно подходить к выбору уполномоченных лиц и привлекать к обработке персональных данных только тех из них, которые предоставляют достаточные гарантии принятия ими соответствующих правовых, организационных и технических мер для обеспечения обработки персональных данных в соответствии с требованиями Закона № 99-З.

уполномоченное лицо должно прекратить обработку соответствующих персональных данных (такие данные передаются оператору либо удаляются (блокируются)).

Правовая основа отношений между оператором и уполномоченным лицом

Взаимоотношения оператора и уполномоченного лица основываются:

- на акте законодательства;
- решении государственного органа, являющегося оператором;
- договоре между оператором и уполномоченным лицом.

В Рекомендациях указываются условия, которые целесообразно предусмотреть в договоре:

- о привлечении уполномоченным лицом иных лиц для обработки персональных данных (например, недопустимость привлечения к обработке персональных данных субуполномоченных лиц с территории государств с ненадлежащим уровнем защиты прав субъектов персональных данных);
- механизме участия уполномоченного лица в выполнении оператором обязанностей перед субъектами персональных данных;
- обязанности уполномоченного лица прекратить по окончании договора обработку соответствующих персональных данных и передать такие данные оператору либо удалить (блокировать) их.

В договор также рекомендуется включать иные стандартные положения согласно приложению к Рекомендациям.

Ответственность

Операторы и уполномоченные лица несут 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,

в прояснении критериев отнесения сведений к персональным данным в целях обеспечения единообразных подходов в правоприменении. Важная роль в этом вопросе отводится НЦЗПД, который уполномочен проводить разъяснительную работу о законодательстве о персональных данных.

Признаки персональных данных

В соответствии с Законом персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

Закон не предусматривает ограничений или требований к носителям информации для признания ее персональными данными. Таким образом, форма представления информации значения не имеет. Это может быть текстовая информация на бумажном или электронном носителе, фотоизображение, видеозапись и др.

Прежде всего, для признания информации персональными данными необходимо, чтобы эта информация «относилась» к лицу. Этот признак призван ограничить всеобъемлющий характер определения персональных данных.

Информация относится к лицу, когда эта информация:

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

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

Рассматриваемый признак исключает отнесение к персональным данным информации, когда такая информация является случайной по отношению к цели ее обработки и не может оказать влияния на субъекта персональных данных. Например, случайное изображение на фотографии,

иллюстрирующей открытие нового магазина, транспортных средств с различимыми номерами. В данном случае целью обработки является не оценка владельца транспортного средства или оказание на него определенного влияния. Соответственно, такие данные не должны признаваться персональными данными.

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

При решении вопроса о том, относится ли информация к конкретному лицу, следует учитывать различные обстоятельства, в том числе содержание информации, цель обработки и возможное влияние обработки на конкретного субъекта.

Но не вся информация, которая касается лица или может оказать на него влияние, будет считаться персональными данными, а лишь та, на основании которой лицо ***идентифицировано*** или ***может быть идентифицировано.***

Идентифицированным является лицо, личность которого известна, которое однозначно выделено среди других лиц (мы на него указали, к нему можно обратиться, мы уже контактировали с данным лицом, знаем его и др.).

Наиболее распространенным вариантом такой ситуации является указание ФИО лица в совокупности с другими данными, которые однозначно выделяют лицо среди других лиц. Например, Ковалев Михаил

операторов или уполномоченных лиц! Оператором в данном случае выступает наниматель, у которого работник работает по трудовому договору, а работник, выполняя свою трудовую функцию, действует от имени оператора и является его «частью».

Пример 7

Секретарь директора учреждения образования выдает справки, содержащие персональные данные учащихся. В этом случае работник занимается обработкой персональных данных, но он не является уполномоченным лицом. Оператором персональных данных является организация, в которой он работает.

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.

Пример 8

Магазин предоставляет свое помещение для проведения акции по дегустации товаров молочного завода. В процессе дегустации участники заполняют небольшую анкету, где указывают свои ФИО и контактные данные. По договору с магазином молочный завод предоставит ему часть данных, полученных в ходе дегустации. В этой ситуации молочный завод является уполномоченным лицом, осуществляющим обработку персональных данных в интересах оператора.

Важной особенностью взаимоотношений между оператором и уполномоченным лицом является то, что после окончания обработки

Но в большинстве случаев оператором по работе с персональными данными является субъект, который **и организует, и осуществляет обработку персональных данных.** Это означает, что оператор не только организует обработку персональных данных (т.е., 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 6

Медицинская организация ведет учет обслуживаемых физических лиц, формирует, хранит и использует их медицинские карты и иные данные, результаты лабораторных исследований, обследований и т.д. Такая организация является оператором по работе с персональными данными.

Кто является уполномоченным лицом

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 (абзац 16 ст. 1 Закона № 99-З).

Признаками уполномоченного лица, как и оператора, являются статус и характер осуществляемой с персональными данными деятельности.

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

Работники не рассматриваются в качестве самостоятельных

Александрович, который приходил на личный прием 15.02.2022 в 10.30 по вопросу незаконной перепланировки жилого помещения, или Ковалев Михаил, который проживает по адресу: г. Минск, ул. Руссиянова, 3–24.

Но даже если мы не знаем ФИО лица, то информация о нем может относиться к персональным данным как информация о физическом лице, которое может быть идентифицировано.

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

Данная формулировка Закона предусматривает отнесение к персональным данным информации о лице, которое может быть определено прямо или косвенно.

Физическое ***лицо, которое может быть прямо определено,*** **–** это лицо, личность которого можно установить на основании той информации, которую мы рассматриваем, без использования дополнительных сведений.

Например, заведующий кафедрой криминалистики юридического факультета БГУ, менеджер ООО «Астра» и номер его телефона, одинокий пенсионер, проживающий по адресу: ул. Никифорова, д. 18, кв. 47, лучший бомбардир футбольного клуба «Минск» в 2020–2021 г., электрик Сергей Валерьевич из ЖЭС-110 и др.

Физическое ***лицо, которое может быть косвенно определено,*** **–** это лицо, личность которого нельзя установить на основании той информации, которую мы рассматриваем, но это можно сделать путем объединения такой информации 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 (например, фамилию и имя Михаил Ковалев могут носить несколько десятков или даже сотен человек), то для определения

конкретного лица может потребоваться получение дополнительной информации, например, даты и места рождения, информации о месте работы, учебы, месте жительства. И наоборот, знание места работы (например, юрисконсульт такой-то организации) зачастую 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. При этом для признания сведений персональными данными реальная идентификация не требуется. Достаточно самой возможности идентификации. Кроме того, если идентификация лица зависит от объединения нескольких блоков информации, каждый из таких блоков в отдельности должен рассматриваться как персональные данные.

Закон предусматривает ряд идентификаторов, наличие которых может свидетельствовать о возможности прямого или косвенного определения лица: ФИО, дата рождения, идентификационный номер, один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Так, например, к признакам, характерным для физической идентичности, могут относиться пол, рост, вес, цвет волос, состояние здоровья (например, дефект речи, инвалидность, фотографии, звукозаписи голосов и др.). Об экономической идентичности может свидетельствовать владение транспортным средством, объектами недвижимости, уровень заработной платы, номер кредитной карточки и др. Социальная идентичность может характеризоваться посредством ссылок на вероисповедание, национальность, политические взгляды, социальные связи, высказывания и комментарии, сексуальную ориентацию.

Это не полный перечень соответствующих идентификаторов.

организует маркетинговое исследование облика и характеристик потребителя определенной кухонной техники. Само исследование она заказывает у специализированной организации, но результаты исследования и все данные по договору будут переданы ей для использования в коммерческой деятельности. Такая организация-производитель считается оператором.

В Законе об информации используется термин «оператор информационной системы», под которым понимается субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством нее информационные услуги. В связи с этим недопустим механический перенос терминологии Закона об информации на сферу обработки персональных данных, поскольку в большинстве случаев оператор информационной системы не будет являться оператором по смыслу законодательства о персональных данных. Такие лица, как правило, выступают в качестве уполномоченных лиц.

Оператором является и такой субъект, который 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, а цели и порядок такой обработки определяются законодательством. При этом для признания организации оператором в понимании законодательства о персональных данных не требуется, чтобы в нормативном правовом акте это было прямо предусмотрено.

Пример 5

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.

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

Важно учитывать, что вопрос об отнесении сведений к персональным данным должен решаться лишь в отношении конкретной ситуации. Информация, которая позволяет идентифицировать человека в одном контексте, может не идентифицировать человека в другом контексте. Так, например, имя Михаил Ковалев является весьма распространенным. Таких данных вполне достаточно для идентификации лица в небольшом коллективе, например, классе или даже в школе, но явно недостаточно для идентификации лица среди всего населения города или страны.

На то, можно ли идентифицировать человека с помощью конкретной информации, в значительной степени будет влиять то, кто владеет информацией и имеет к ней доступ. Когда информация публикуется публично, доступ к ней может получить кто угодно в мире. Это может затруднить определение того, к какой дополнительной информации люди могут иметь доступ и какие у них могут быть мотивы для идентификации человека.

Примеры отнесения сведений к персональным данным

В поступающих в НЦЗПД запросах часто поднимается вопрос о том, является ли определенный идентификатор сам по себе персональными данными. Как уже отмечалось, подобные вопросы, как правило, не могут быть решены абстрактно и требуют анализа конкретной ситуации.

Для примера, рассмотрим вопрос об отнесении к персональным данным номера мобильного телефона, e-mail субъекта и VIN-номера транспортного средства.

1. Адрес электронной почты

Адреса электронной почты может быть достаточно, чтобы идентифицировать кого-то, когда в электронном адресе отражаются

или предпринимательской деятельностью, **не являются операторами,** поскольку в соответствии с абзацем вторым п. 2 ст. 2 Закона № 99-З на такие отношения его действие не распространяется.

Пример 2

Профессиональный фотограф оказывает услуги по проведению семейной фотосессии. Несмотря на то что лица, заказавшие такую услугу, будут использовать фотографии исключительно для личных целей, для фотографа такая деятельность является профессиональной. Следовательно, фотограф в данном случае будет являться оператором и иметь обязанности в соответствии с Законом № 99-З.

Пример 3

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. Такая деятельность не является профессиональной или предпринимательской деятельностью, соответственно такое лицо не несет обязанности оператора.

Вторым признаком оператора является деятельность по **организации обработки и (или) непосредственно обработка им персональных данных.**

Субъект может только организовывать обработку персональных данных, но не заниматься ею непосредственно, например, определять ключевые параметры обработки персональных данных (цели и сроки, объем обрабатываемых данных, круг лиц, которым предоставляются персональные данные), а саму обработку поручать уполномоченному лицу. Такая деятельность относится к деятельности оператора.

Пример 4

Организация, занимающаяся производством бытовой техники,

данные о лице (ФИО, дата рождения, место работы и др.) (например, *Kovalev12.10.1983@cpd.by).* В этом случае обработка такой информации, когда она «привязана» к лицу, является обработкой персональных данных.

В других ситуациях информация в электронном адресе лишь теоретически может быть связана с лицом и у субъекта может не быть реальных законных рычагов получения информации с целью идентификации лица. В таком случае данные не могут признаваться персональными. Например, *info@cpd.by, 1237@gmail.com.*

2. Номер мобильного телефона

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. Такая 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), рассылки рекламных или иных нежелательных сообщений). Это может причинять беспокойство, вызывать раздражение, недовольство попытками завладеть вниманием лица.

Как следствие, даже не зная конкретного лица (например, не владея информацией о ФИО лица и его местоположении), которому принадлежит номер телефона, оператор может стремиться использовать данные способы связи для оказания влияния на него. Это может заставить субъекта изменить контактные данные или поменять оператора, по вине которого произошло нарушение его прав. Кроме того, неправомерное использование контактных данных может нарушить интересы третьих лиц, например, семьи субъекта.

В связи с этим, 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.

− юридическое лицо (государственная или негосударственная организация, в т.ч. государственный орган);

− физическое лицо (как имеющее, так и не имеющее статуса индивидуального предпринимателя).

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

Пример 1

Организация имеет в штате 6 сотрудников и занимается техническим дизайном компьютерных игр. Несмотря на то что данная организация не имеет клиентов – физических лиц и не работает непосредственно с их данными, она все равно имеет штатных сотрудников, данные которых собираются и хранятся этой организацией. Таким образом, она является оператором по работе с персональными данными.

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, лицо, осуществляющее деятельность по оказанию услуг в сфере агроэкотуризма или иные виды деятельности, не являющиеся предпринимательской в соответствии с частью четвертой п. 1 ст. 1 ГК). В частности, это репетиторство, фотосъемка, изготовление фотографий; видеосъемка событий, аренда, прокат развлекательного и спортивного оборудования и т.п.

Физические лица, осуществляющие обработку персональных данных в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной

ОПЕРАТОР И УПОЛНОМОЧЕННЫЙ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: ОПРЕДЕЛЯЕМ ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ

Кто является оператором по обработке персональных данных

Организация, занимающаяся обработкой персональных данных, является оператором. К операторам относятся не только государственные организации, но и любое иное юридическое лицо, а также индивидуальный предприниматель или физическое лицо, если последние самостоятельно или совместно с иными лицами организуют и (или) осуществляют обработку персональных данных (абзац восьмой ст. 1 Закона № 99-З).

В Рекомендациях выделены следующие **признаки оператора**:

1) статус;

2) осуществление обработки персональных данных.

Статус определяется организационно-правовой формой субъекта. Это:

3. VIN-номер транспортного средства

Много вопросов вызывает на практике и отнесение к персональным данным VIN-номера. Сейчас довольно распространена практика использования VIN-номера транспортного средства для проверки его истории (наличие аварий и др.). Использование такой информации имеет прямое влияние на владельца транспортного средства, когда покупатель откажется от сделки после проверки истории машины, то есть эта информация «относится» к лицу. При этом во многих случаях существуют легальные возможности «связать» транспортное средство с его владельцем. Подобные сведения содержатся в реестре движимого имущества, обремененного залогом, доступ к которому может получить любой желающий при условии внесения платы. Кроме того, широко распространена практика указания VIN-номера в объявлениях о продаже транспортных средств, где наряду с VIN-номером отражаются информация о продавце и его контактные данные – номер телефона и (или) электронной почты. Таким образом, обработка VIN-номера в подобном случае должна рассматриваться как обработка персональных данных.

Отдельно следует остановиться на вопросах обработки персональных данных в целях прямого маркетинга. Хотя, на первый взгляд, данный вопрос не является критически важным для граждан и многие спокойно относятся к подобной обработке, тем не менее он поднимается фактически в каждой второй жалобе, поступающей в НЦЗПД.

Особенность интернет-рекламы на современном этапе заключается в персонализации рекламных моделей, которые стремятся предложить каждому индивидуально подобранную для него рекламу. Однако эта практика требует сбора больших объемов личных данных (например, анализ информации, которую вы просматриваете на сайтах, может много сказать о ваших привычках, интересах, образе жизни и др.).

Проснувшись с утра, вы просмотрели новости, ответили на сообщения в социальных сетях, заказали определенные товары в интернете. В течение дня вы продолжаете активно использовать

преимущества глобальной сети, например, выяснив, где можно в определенном районе перекусить в кафе, в последующем оценив качество обслуживания в нем, записались в парикмахерскую, заказали билеты в кино и др. На первый взгляд персональные данные нигде не оставлялись. Но в тот же день вы можете увидеть сообщения на своей страничке в социальной сети о предложениях новых кафе, о просмотре фильмов и др. Это не совпадения, а результат сбора ваших данных навигации в сети интернет и геолокации.

В соответствии с одним из последних исследований наша личная информация, включая геолокацию, распространяется среди тысяч компаний в среднем почти 400 раз в день.

В целом, можно отметить, что универсального перечня сведений, которые должны признаваться персональными данными, нет и, наверное, не может быть. Вместо этого в Законе содержится своеобразный «тест» с признаками относимости к лицу информации и возможностью его идентификации на основе такой информации. Как следствие, вопрос об отнесении сведений к персональным данным должен рассматриваться в каждом конкретном случае с учетом всех обстоятельств.

административное правонарушение, малолетнего.

Решение суда по делу

К. была подвергнута административному взысканию в виде штрафа в размере 85 БВ на сумму 3145 руб.

2 Содержание административного правонарушения

По ч. 4 ст. 23.7 КоАП **Л**., являясь директором ООО «Т», не принял меры:

1) по ознакомлению работников, непосредственно осуществляющих обработку персональных данных, в частности:

– с требованиями по защите персональных данных;

– документами, определяющими политику организации в отношении обработки персональных данных;

2) обучению указанных работников и иных лиц в порядке, установленном законодательством;

3) установлению порядка доступа к персональным данным, в том числе обрабатываемым в информационном ресурсе;

4) осуществлению технической и криптографической защиты персональных данных в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов, содержащих персональные данные.

Следовательно, **Л**. допустил несоблюдение мер обеспечения защиты персональных данных физических лиц, нарушив требования п. 3, 4 ст. 17 Закона № 99-З.

В судебном заседании лицо, в отношении которого ведется административный процесс, вину в совершении правонарушения признало, отметив частичное устранение выявленных нарушений.

Решение суда по делу

Директор **Л**. на основании ч. 4 ст. 23.7 КоАП был подвергнут административному взысканию в виде штрафа в размере 4 БВ на сумму 128 руб.

		(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	

Примеры судебных споров

1 Содержание административного правонарушения

К., являясь старшим инспектором Дворца гражданских обрядов главного управления юстиции Мингорисполкома, умышленно путем отправления смс-сообщения с абонентского номера *** на абонентский номер *** в мессенджере, незаконно предоставила гражданке **А**. персональные данные гражданки **М**. без согласия последней, которые ей стали известны в связи с ее служебной деятельностью. Данные были о том, что **М.** состоит в браке с 2002 г. с гражданином **С**., расторжения брака не было.

В судебном заседании **К.** вину во вмененном ей правонарушении признала полностью. Суд, заслушав лицо, в отношении которого ведется административный процесс, исследовав материалы дела, пришел к выводу о доказанности виновности **К.** в умышленном незаконном предоставлении персональных данных физического лица, совершенном лицом, которому персональные данные известны в связи с его служебной деятельностью, и квалифицировал ее действия по ч. 2 ст. 23.7 КоАП. Обстоятельством, смягчающим административную ответственность, является чистосердечное раскаяние в совершении правонарушения, наличие на иждивении у физического лица, совершившего

ОБ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

В таблице для лучшего понимания разберем, когда применяется ст. 23.7 КоАП, приведем ее краткую характеристику.

Часть ст. 23.7 КоАП	**Описание нарушения**	**Примеры нарушения (согласно Постатейному комментарию)**	**Примечание**
Ч. 1	Умышленные незаконные сбор, обработка, хранение или предоставление персональных данных физического лица либо нарушение его прав, связанных с обработкой персональных данных. Санкция: штраф до 50 БВ	Нарушение прав субъекта, связанных с обработкой персональных данных, может иметь различные формы: • **отсутствие ответа на заявления,** поданные в соответствии со ст. 14 Закона № 99-З; • **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 № 99-З субъекту вместо конкретных персональных данных предоставляется общая характеристика таких данных; при подаче заявления в соответствии с ст. 12 Закона № 99-З указывается лишь то, 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

Ч. 2	Деяния, предусмотренные ч. 1 настоящей статьи, совершенные **лицом, которому персональные данные известны в связи с его профессиональной или служебной деятельностью.** Санкция: штраф от 4 до 100 БВ	При привлечении лица к административной ответственности в данном случае следует установить, что соответствующие действия по обработке персональных данных, охватывались трудовой функцией работника, отражены в его должностной инструкции. Например, в *качестве подобного нарушения можно рассматривать неофициальную практику «пробивания» по базам по просьбе знакомых и др.*	Данная часть применяется также в случае нарушения законодательства о защите персональных данных, но когда такое нарушение допустило (совершил) должностное лицо (работник), который получил к таким персональным данным доступ для выполнения трудовых обязанностей
Ч. 3	Умышленное незаконное распространение персональных данных физических лиц. Санкция: штраф до 200 БВ	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). Например, *распространением является размещение чужих персональных данных без согласия субъекта персональных данных*	То есть ч. 3 применяется только по отношению к такой незаконной обработке персональных данных, как незаконное распространение (когда персональные данные становятся общедоступными, публичными без законного основания)

		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.	
Ч. 4.	Несоблюдение мер обеспечения защиты персональных данных физических лиц. Санкция: штраф от 2 до 10 БВ (на ИП – от 10 до 25 БВ; на юридическое лицо – от 20 до 50 БВ)	Соответствующие меры вытекают из требований ст. 17 Закона № 99-З. 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: **1)** перечня информационных ресурсов (систем), содержащих персональные данные, собственниками (владельцами) которых они являются; **2)** 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	Особенностью данной части является дифференцированный подход к санкциям ст. 23.7 КоАП