Памятка для операторов персональных данных в связи с изменениями в законодательстве с 1 сентября 2022 г.

август 2022 г.

См. Обзор изменений в законодательстве о персональных данных с 1 сентября 2022 г.

1. Изменения в содержании применяемых вами документов

а) договор, стороной которого является субъект ПД:

До 1 сентября обрабатывать ПД этого субъекта для целей заключения или исполнения договора можно было без согласия субъекта. Теперь же для сохранения возможности обработки ПД без согласия субъекта ПД необходимо проверить, чтобы договор, заключаемый с субъектом ПД, не ограничивал права и свободы субъекта ПД, не допускал обработку ПД несовершеннолетних (иное может быть предусмотрено законодательством РФ), а также не предусматривал бездействие субъекта ПД в качестве условия заключения договора (п. 5 ч. 1 ст. 6 Закона о ПД в новой ред.).

Если подобные условия все же необходимо сохранить в договоре, для обработки ПД субъекта потребуется его согласие, несмотря на то, что обработка будет необходима для заключения / исполнения договора, стороной которого является субъект ПД (п. 5 ч. 1 ст. 6 Закона о ПД). Напомним, что согласие на обработку обычных ПД (не относящихся к биометрическим или специальным ПД) может быть дано субъектом ПД (его представителем) в любой позволяющей подтвердить факт его получения форме (ч. 1 ст. 9 Закона о ПД).

б) договор с лицом, осуществляющим обработку ПД по поручению оператора (обработчиком):

С 1 сентября в круг обязанностей обработчика, которые должны быть предусмотрены его договором с оператором, добавлены требования:

- при сборе ПД по общему правилу использовать базы данных, находящиеся на территории РФ,

- соблюдать предписания ст. 18.1 Закона о ПД,

- предоставлять по запросу оператора ПД (в течение срока действия поручения) документы и иную информацию, подтверждающие принятие мер и соблюдение требований закона,

- уведомлять оператора о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД (ч. 3 ст. 6 Закона о ПД в новой ред.), субъектом ПД наряду с оператором (ч. 6 ст. 6 Закона о ПД в новой ред.).

Данные обязанности следует включать в те договоры, которые будут заключаться начиная с 1 сентября. Ранее заключенные договоры в принудительном порядке не меняются, поскольку переходные положения не устанавливают, что действие изменений распространяется на отношения, возникшие из ранее заключенных договоров (ст. 422 ГК РФ). Изменение содержания таких договоров возможно только по соглашению сторон.

в) согласие на обработку ПД:

Ранее от согласия на обработку ПД требовалось быть конкретным, информированным и сознательным. Теперь оно должно быть еще и предметным, а также однозначным (ч. 1 ст. 9 Закона о ПД в новой ред.).

Пока не сложится практика применения данной нормы, сложно сказать, в чем существенное отличие нового регулирования. Пояснительная записка к законопроекту не освещает это изменение. На наш взгляд, понятие конкретности согласия настолько тесно связано с его предметностью и однозначностью, что и до этого согласие субъекта ПД предполагалось дающимся в отношении определенных видов ПД и определенных видов их обработки (предметность) и не допускающим различного толкования (однозначность).

Пока практической рекомендацией, видимо, должна быть проверка разработанного оператором шаблона согласия на пресловутые предметность и однозначность.

г) локальные акты по вопросам обработки ПД:

С 1 сентября уточняются требования к содержанию документов, определяющих политику оператора в отношении обработки ПД, локальных актов по вопросам обработки ПД:

- в них должны определяться для каждой цели обработки ПД категории и перечень обрабатываемых ПД, категории субъектов, ПД которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПД при достижении целей их обработки или при наступлении иных законных оснований,

- запрещено включать в них положения, ограничивающие права субъектов ПД, а также возлагающие на операторов не предусмотренные законодательством РФ полномочия и обязанности (п. 2 ч. 1 ст. 18.1 Закона о ПД в новой ред.).

Также отметим, что с 1 сентября конкретизировано, где именно в соответствующей информационно-телекоммуникационной сети оператор, осуществляющий сбор ПД с использованием таких сетей, обязан опубликовать документ, определяющий его политику в отношении обработки ПД, и сведения о реализуемых требованиях к защите ПД - а именно, на страницах принадлежащего оператору сайта в интернете, с использованием которых осуществляется сбор ПД (ч. 2 ст. 18.1 Закона о ПД в новой ред.). Однако формулировка "в том числе" указывает, что это не исключительный способ опубликования сведений.

д) уведомление Роскомнадзора о начале обработки ПД

В нем дополнительно следует указать ФИО физического лица или наименование юридического лица, имеющих доступ и (или) осуществляющих на основании договора обработку ПД, содержащихся в государственных и муниципальных информационных системах (п. 10.2 ч. 3 ст. 22 Закона о ПД в новой ред.).

А категории ПД, категории субъектов, ПД которых обрабатываются, правовое основание обработки ПД, перечень действий с ПД, способы обработки ПД отныне следует указывать для каждой цели обработки ПД отдельно (ч. 3.1 ст. 22 Закона о ПД в новой ред.).

Обращаем внимание: изменениями закреплена обязательность форм уведомлений о начале и прекращении обработки ПД, а также об изменении ранее представленных сведений, которые устанавливаются Роскомнадзором (ч. 8 ст. 22 Закона о ПД в новой ред.). Таким образом, соответствующие формы, приведенные в приложении к методическим рекомендациям, утв. приказом Роскомнадзора от 30 мая 2017 г. N 94, переходят из статуса рекомендуемых в статус обязательных, если ведомством не будут разработаны новые формы.

Работа по утверждению новых форм уже ведется. Если эти формы не будут приняты к 1 сентября, необходимо подать уведомления о намерении осуществлять обработку ПД (если ранее не уведомляли Роскомнадзор об обработке) или о внесении изменений в ранее представленные сведения (если уведомляли, но по старой редакции ст. 22 Закона о ПД) по старым формам, а при появлении новых подать недостающие сведения через форму уведомления о внесении изменений в ранее представленные сведения. Такие разъяснения дает и Роскомнадзор.

2. Изменения в вашем взаимодействии с субъектами ПД

а) в части биометрических ПД:

С 1 сентября предоставление биометрических ПД не может быть обязательным, за исключением случаев, когда обработка биометрических ПД может осуществляться без согласия субъекта. Оператор также не вправе отказывать в обслуживании в случае отказа субъекта ПД предоставить биометрические ПД и (или) дать согласие на их обработку, если в соответствии с федеральным законом получение оператором согласия на обработку ПД не является обязательным (ч. 3 ст. 11 Закона о ПД в новой ред.).

б) при запросе субъектом ПД информации, касающейся обработки его ПД:

В перечень сведений, которые субъект ПД может запросить у оператора, включена информация о способах исполнения оператором обязанностей, установленных ст. 18.1 Закона о ПД (п. 9.1 ч. 7 ст. 14 Закона о ПД в новой ред.).

Также с 1 сентября будет определен срок и порядок ответа оператора на запрос субъекта ПД: сведения должны быть предоставлены субъекту ПД (его представителю) в течение десяти рабочих дней с момента обращения (получения оператором соответствующего запроса). Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД. Сведения предоставляются в той форме, в которой направлено соответствующее обращение (запрос), если в нем не указано иное (ч. 3 ст. 14 Закона о ПД в новой ред.).

3) при сборе ПД:

Оператор обязан разъяснить субъекту ПД юридические последствия не только отказа предоставить его ПД (ныне действующая норма), но и отказа дать согласие на их обработку, если в соответствии с федеральным законом получение оператором согласия на обработку ПД является обязательным (ч. 2 ст. 18 Закона о ПД в новой ред.).

В круг сведений, которые оператор обязан предоставить субъекту ПД до начала обработки, если ПД получены от третьих лиц, включен сам перечень полученных ПД (п. 2.1 ч. 3 ст. 18 Закона о ПД в новой ред.).

4) по поводу устранения нарушений законодательства, допущенных при обработке ПД:

В случае обращения субъекта ПД к оператору с требованием о прекращении обработки ПД оператор обязан по общему правилу прекратить их обработку или обеспечить прекращение такой обработки (если за оператора действует обработчик) за исключением случаев, когда обработка возможна без согласия субъекта ПД, в течение десяти рабочих дней с даты получения требования. Указанный срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор должен направить в адрес субъекта ПД (ч. 5.1 ст. 21 Закона о ПД в новой ред.).

3. Изменения в вашем взаимодействии с Роскомнадзором

а) по уведомлению о начале обработки ПД:

Перечень случаев, когда обработка ПД возможна без уведомления Роскомнадзора, с 1 сентября урезан до обработки ПД:

- включенных в государственные информационные системы ПД, созданные в целях защиты безопасности государства и общественного порядка;

- обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства,

- в случае, если оператор осуществляет деятельность по обработке ПД исключительно без использования средств автоматизации (ч. 2 ст. 22 Закона о ПД в новой ред.).

Отметим, что в последнем случае речь идет о возможности обработки ПД без уведомления Роскомнадзора только тогда, когда оператор вообще осуществляет деятельность по обработке ПД исключительно без использования средств автоматизации, т.е. абсолютно все ПД им обрабатываются таким способом.

Несмотря на то, что законодатель значительно увеличил число случаев, в которых уведомление Роскомнадзора необходимо, он не предусмотрел никаких переходных положений по срокам направления уведомления для тех операторов, которые ранее не обязаны были направлять такое уведомление. Официальных разъяснений на этот счет тоже пока нет. Мы полагаем наименее рискованным направление уведомления в первый день действия новой редакции Закона о ПД - 1 сентября.

б) при запросе информации Роскомнадзором:

Срок ответа оператора при получении запроса Роскомнадзора сокращен с тридцати календарных дней до десяти рабочих дней со дня обращения (получения запроса). Но этот срок может быть продлен не более чем на пять рабочих дней по мотивированному уведомлению, которое оператор обязан направить в Роскомнадзор (ч. 4 ст. 20 Закона о ПД в новой ред.).

в) по поводу устранения нарушений законодательства, допущенных при обработке ПД:

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД, оператор обязан уведомить Роскомнадзор о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПД, и предполагаемом вреде, нанесенном правам субъектов ПД, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о контактном лице - в течение суток с момента выявления такого инцидента оператором, самим Роскомнадзором или иным заинтересованным лицом, а о результатах внутреннего расследования выявленного инцидента и о лицах, действия которых стали причиной выявленного инцидента (при наличии) - в течение трех суток (ч. 3.1 ст. 21 Закона о ПД в новой ред.).

Внимание

В случае возникновения инцидента оператор обязан направить в Роскомнадзор два уведомления!

4. Абсолютно новая обязанность оператора по взаимодействию с ГосСОПКА

Такое название носит Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории РФ, в дипломатических представительствах и (или) консульских учреждениях РФ), созданная в соответствии с Федеральным законом от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

С 1 сентября оператор обязан в порядке, определенном ФСБ, обеспечивать взаимодействие с ГосСОПКА, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПД. Поступившая от оператора информация передается органами ФСБ в Роскомнадзор в согласованном ими порядке (ч. 12-14 ст. 19 Закона о ПД в новой ред.).

В отсутствие новых нормативных актов, по всей видимости, встает вопрос о применимости Перечня информации, представляемой в ГосСОПКА, и Порядка представления информации в ГосСОПКА, утв. приказом ФСБ России от 24.07.2018 N 367, а также Порядка информирования ФСБ России о компьютерных инцидентах..., утв. приказом ФСБ России от 19.06.2019 N 282. При этом следует обратить внимание на понятие субъектов критической информационной инфраструктуры, на которых распространяются данные приказы ФСБ: это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. Очевидно, что это понятие уже, чем понятие оператора ПД, в деятельности которого произошел компьютерный инцидент, повлекший неправомерную передачу (предоставление, распространение, доступ) ПД, которое использует Закон о ПД в новой ред. Поэтому мы полагаем, что должны последовать официальные разъяснения о том, что именно включает в себя обязанность оператора ПД обеспечивать взаимодействие с ГосСОПКА, применим ли при этом приказ N 367, должно ли происходить информирование ФСБ согласно приказу N 282, действуют ли два этих порядка одновременно или только один из них. До таких разъяснений применимость этих приказов вызывает сомнения.

5. Отдельные напоминания

а) организациям, подведомственным государственным и муниципальным органам:

Особенности обработки ПД, разрешенных субъектом ПД для распространения, установленные ст. 10.1 Закона о ПД, не распространяются на обработку вами ПД при исполнении возложенных на вас законодательством РФ функций, полномочий и обязанностей (ч. 15 ст. 10.1 Закона о ПД в новой ред.).

б) иностранным юридическим или физическим лицам:

Если вы осуществляете обработку ПД российских граждан на основании договоров с ними либо на основании их согласия на обработку их ПД, тогда с 1 сентября положения Закона о ПД являются для вас обязательными (ч. 1.1 ст. 1 Закона о ПД в новой ред.).

Для эффективного погружения в новое для вас законодательство рекомендуем ознакомиться с материалами Энциклопедии решений "Персональные данные"