ВАШ КОНСУЛЬТАНТ
420021, г. Казань,
ул. Татарстан, д. 22/41, 8 этаж
Телефон: 8(800)700-52-23, 8(843)515-20-20
Email: cons@vkons.ru Сайт: www.vkons.ru

Поправки в сфере персональных данных с 1 сентября 2022 года: что придется изменить компаниям?

В июле 2022 года был принят закон с поправками в №152-ФЗ «О персональных данных». Это самая значимая и масштабная реформа законодательства о персональных данных в России с 2011 года. Большинство поправок вступит в силу уже с 1 сентября 2022 года. Еще часть изменений, касающаяся трансграничной передачи данных, вступит в силу с 1 марта 2023 года. В любом случае к ним нужно подготовиться уже сейчас.

> Какие новые уведомления придется направлять в Роскомнадзор? Как теперь передавать данные за границу, например, при работе с иностранными сервисами? Что поменять в договорах с физлицам? Об этом и многом другом поговорим в предложенном материале.

Содержание материала:

1. Что изменится с 1 сентября 2022 года?
2. Что изменится с 1 марта 2023 года?

Что изменится с 1 сентября 2022 года?

Придется уведомлять Роскомнадзор об «утечке» персональных данных

Если оператор установит факт неправомерной или случайной передачи ПД (предоставления, распространения, доступа), которая повлекла нарушение прав субъектов ПД, то он будет обязан уведомить Роскомнадзор о произошедшем инциденте и результатах внутреннего расследования (ч. 3.1 ст. 21 Закона № 152-ФЗ). Норма касается только тех инцидентов, в которых установлены оператором или иным заинтересованным лицом (не уточняется, кто может быть таким лицом):

1. факт неправомерной или случайной передачи ПД;
2. нарушение прав субъектов ПД;
3. причинно-следственная связь между ними.

Срок уведомления об инциденте нужно считать с момента выявления инцидента (факта или подозрения о нем) оператором, Роскомнадзором или иным заинтересованным лицом, но сама обязанность уведомлять об инциденте лежит только на операторе. В то же время Роскомнадзор и иные заинтересованные лица не обязаны информировать оператора о выявлении ими инцидента.

Оператор должен уведомить Роскомнадзор в течение 24 часов, предоставив сведения:

1. о произошедшем инциденте;
2. о предполагаемых причинах;
3. о предполагаемом вреде, нанесенном правам субъектов ПД;
4. о принятых мерах по устранению последствий инцидента;
5. о лице, уполномоченном оператором на взаимодействие с Роскомнадзором по вопросам, связанным с выявленным инцидентом.

Далее в течение 72 часов нужно сообщить о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

Рекомендации:

1. разработайте локальную процедуру выявления, установления, нейтрализации и уведомления в отношении инцидентов неправомерного раскрытия ПД. Особый фокус

следует уделить выявлению и мониторингу инцидентов в СМИ, интернет-ресурсах и иных открытых источниках. Также можно организовать программу по «охоте» за такого рода сведениями с привлечением всех заинтересованных лиц («Data Breach Bounty») путем выплаты вознаграждения за предоставление достоверных сведений о таких инцидентах;

2. проверьте, соответствуют ли типовые формы договоров об обработке ПД новым требованиям в отношении инцидентов неправомерного раскрытия ПД. Внесите изменения в уже заключенные договоры.

Обратите внимание!

С 1 марта 2023 года Роскомнадзор начнет вести реестр учета инцидентов в области персональных данных. До этой даты он должен определить порядок и условия взаимодействия с операторами в рамках ведения реестра (ч. 10 ст. 23 Закона №152-ФЗ).

Придется передавать сведения о компьютерных инцидентах в госсистему.

Оператор обязан обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) и предоставлять информацию о компьютерных инцидентах, повлекших исключительно неправомерную передачу ПД. А вот случайная передача ПД находится вне регулирования ст. 19 Закона № 152-ФЗ (ч. 12 ст. 19 Закона № 152-ФЗ).

Рекомендации:

1. проанализируйте требования в отношении порядка взаимодействия операторов с ГосСОПКА, включая порядок информирования ФСБ о компьютерных инцидентах, который утвердит ФСБ (пока не утверждены);

2. разработайте локальную процедуру взаимодействия с ГосСОПКА после утверждения ФСБ соответствующего правового акта.

Запрещено включать в договоры определенные условия

В договоры с физлицами нельзя включать положения:

1. ограничивающие права и свободы субъекта ПД. Например, некоторые операторы пытаются обусловить реализацию права субъектов на доступ к своим ПД требованием предварительно зарегистрироваться в каких-то информационных системах или на цифровых платформах;

2. устанавливающие случаи обработки ПД несовершеннолетних, если иное не предусмотрено в законодательстве;

3. допускающие в качестве условия заключения договора бездействие субъекта ПД (п. 5 ч.1 ст. 6 Закона № 152-ФЗ). Например, будет сомнительной практика одностороннего изменения оператором положений уже заключенного договора с субъектом ПД, в рамках которой бездействие субъекта ПД (в том числе в ответ на уведомление со стороны оператора) квалифицируется в качестве его согласия с измененными положениями договора.

Рекомендации:

1. проанализируйте и при необходимости доработайте типовые формы договоров с потребителями, договоров гражданско-правового характера с подрядчиками (физлицами, ИП) и трудовые договоры согласно новым требованиям. Внесите изменения в уже заключенные договоры;

2. если в договорах есть положения об обработке персональных данных, то особое внимание следует уделить соответствию/совместимости предмета договора и заявленных в нем целей обработки ПД, необходимости и пропорциональности обработки указанной в договоре обработки ПД. Например, многие компании неправомерно включают в договоры с потребителями согласие таких лиц на получение сообщений уведомительного и рекламного характера, не касающихся хода выполнения договора, на номер мобильной связи и адрес электронной почты.

Обратите внимание!

Положение об обработке персональных данных (политику конфиденциальности) нужно опубликовать не просто на любой странице сайта, а на всех страницах, на которых осуществляется сбор ПД (ч. 2 ст. 18.1 Закона №152-ФЗ).

Также проверьте, указаны ли в положении об обработке ПД для каждой цели обработки отдельно категории и перечень ПД, способы, сроки их обработки и хранения, порядок уничтожения ПД (ст. 18.1 Закона №152-ФЗ). Роскомнадзор и раньше требовал это указывать (об этом было сказано в рекомендациях Роскомнадзора), но теперь данное требование закреплено законодательно.С 1 марта 2023 года Роскомнадзор начнет вести реестр учета инцидентов в области персональных данных. До этой даты он должен определить порядок и условия взаимодействия с операторами в рамках ведения реестра (ч. 10 ст. 23 Закона №152-ФЗ).

Изменились требования к обработчикам

Это лица, которым операторы выдают поручение на обработку ПД. Теперь меняются требования к содержанию договора о поручении обработки ПД, а также расширяется объем обязанностей обработчиков. Обработчики должны:

1. локализовать базы с персональными данными;
2. принять меры, предусмотренные ст. 18.1 Закона № 152-ФЗ, и предоставить сведения о них по запросу оператора;
3. уведомлять оператора в отношении инцидентов с ПД (ч. 3 ст. 6 Закона № 152-ФЗ).

Если оператор поручает обработку ПД иностранному лицу, то ответственность перед субъектом персональных данных будет нести не только оператор, но и обработчик (ч. 6 ст. 6 Закона № 152-ФЗ).

Рекомендации:

1. проанализируйте и при необходимости доработайте типовые формы договоров об обработке ПД согласно ч. 3 ст. 6 Закона № 152-ФЗ. Также проанализируйте договоры на предмет распределения ответственности оператора-резидента и обработчика-нерезидента перед субъектом ПД, внесите изменения в уже заключенные договоры;
2. включите в локальные акты оператора положения о порядке взаимодействия с обработчиками в части:

- предоставления документов и сведений, подтверждающих принятие обработчиками мер и соблюдение ими требований ст. 6 Закона № 152-ФЗ в целях исполнения поручения

оператора;

- уведомления оператора об «утечке» ПД;

3. проверьте, указан ли в поручении перечень ПД.

Сокращены сроки ответов на запросы

Уменьшены сроки исполнения оператором запросов субъектов ПД о получении информации об обработке их ПД. Раньше срок был 30 дней. Теперь нужно будет отвечать в течение 10 рабочих дней. Этот срок может быть продлен, но не более чем на 5 рабочих дней и при условии, что оператор направил мотивированное уведомление с указанием причин продления срока. Кроме того, оператор должен отвечать в той форме, в которой субъект ПД направил свой запрос, если иное не указано в этом запросе (ч. 3 ст. 14 Закона № 152-ФЗ). Отвечать на запросы Роскомнадзора тоже теперь нужно в течение 10 дней (ч. 4 ст. 20 Закона № 152-ФЗ).

Рекомендации:

1. проанализируйте и при необходимости скорректируйте закрепленную в локальных актах практику обработки запросов субъектов ПД о получении информации в отношении обработки их ПД, в том числе в части соответствия новым (сокращенным) срокам реагирования на запросы субъектов ПД;
2. проанализируйте и при необходимости доработайте типовые формы договоров о поручении обработки ПД на предмет их соответствия новым (сокращенным) срокам реагирования на запросы субъектов ПД. Внесите изменения в уже заключенные договоры;
3. нужно учесть новые требования в документах декларативного или информационного характера (политиках, privacy notice и т.п.);
4. проинформируйте сотрудников, которые отвечают на запросы физлиц, о том, что сроки сократились.

Запрещено отказывать в обслуживании из-за непредоставления биометрических данных

Оператор не вправе отказывать в обслуживании в случае отказа субъекта ПД предоставить биометрические ПД (фото, видео, отпечатки пальцев) или дать согласие на обработку биометрических ПД, если получение оператором такого согласия не является обязательным (ч. 3 ст. 11 Закона № 152-ФЗ).

Рекомендации:

1. проанализируйте договоры с потребителями и локальные документы, проверьте, чтобы в них не было положений о праве отказать потребителю в обслуживании из-за непередачи биометрических данных.

Сократится перечень случаев, когда не нужно уведомлять Роскомнадзор о начале обработке персональных данных

В прежней редакции содержался список случаев, когда можно было не отправлять уведомление в Роскомнадзор. Например, если компания обрабатывает только ПД сотрудников или ПД, которые нужны для однократного пропуска на территорию. Теперь этот перечень существенно сократился. Можно не отправлять уведомление только в следующих случаях:

1. если ПД включены в государственные информационные системы ПД, созданные в целях защиты безопасности государства и общественного порядка;

2. если оператор осуществляет деятельность по обработке данных исключительно без использования средств автоматизации, то есть только в бумажном виде;

3. если ПД обрабатываются в случаях, предусмотренных законодательством о транспортной безопасности (ч. 2 ст. 22 Закона № 152-ФЗ).

Кроме того, в уведомлении нужно будет указывать отдельно для каждой цели обработки ПД категории ПД, категории субъектов ПД, правовое основание обработки ПД, перечень действий с ПД, способы обработки ПД (п. 3-6 ч. 3 ст. 22 Закона № 152-ФЗ исключены, ч. 3.1 ст. 22 Закона № 152-ФЗ).

Если сведения, указанные в уведомлении изменились, то оператор должен не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения, уведомить Роскомнадзор обо всех изменениях, произошедших за этот период. Раньше об

этом нужно было сообщать в течение 10 рабочих дней после появления изменений (ч. 7 ст. 22 Закона № 152-ФЗ).

Рекомендации:

1. если раньше компания не обязана была уведомлять Роскомнадзор (например, если она обрабатывала только ПД сотрудников), а теперь она должна это делать, то нужно отправить уведомление о начале обработки ПД. Дата начала обработки ПД, указываемая в уведомлении, должна соответствовать моменту фактического начала обработки ПД.

Обратите внимание!

С 1 сентября 2022 года начнут действовать поправки согласно которым согласие на обработку персональных данных должно быть «предметным» и «однозначным» (ч. 1 ст. 9 Закона №152-ФЗ). Это указано в дополнение к тому, что согласие должно быть конкретным, информированным и сознательным.

Что изменится с 1 марта 2023 года?

Операторы, которые ранее осуществляли трансграничную передачу ПД и продолжают это делать, обязаны направить в Роскомнадзор уведомление о намерении осуществлять трансграничную передачу ПД (ст. 12 Закона № 152-ФЗ). То есть придется отправлять в Роскомнадзор не только уведомление о намерении начать обрабатывать ПД, но и отдельное уведомление о намерении осуществлять трансграничную передачу данных. При этом Роскомнадзор может принять решение о запрете передачи ПД иностранному лицу. Такое решение принимается в течение 10 дней. В таком случае оператор должен обеспечить уничтожение полученных иностранным лицом ПД.

Рекомендации:

1. включите в локальные акты положения о порядке получения и документирования оператором от органов иностранного государства, иностранных физлиц или юрлиц, которым планируется трансграничная передача ПД, сведений, предусмотренных ч. 5 ст. 12 Закона № 152-ФЗ. Это сведения:

- о мерах по защите передаваемых ПД и об условиях прекращения их обработки, принимаемых иностранными лицами, которым планируется трансграничная передача ПД;
- о правовом регулировании в области ПД иностранного государства, под юрисдикцией которого находятся иностранные лица, которым планируется трансграничная передача ПД (если предполагается передача ПД иностранным лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД);
- об иностранных лицах, которым планируется трансграничная передача ПД (наименование либо ФИО, а также номера контактных телефонов, почтовые адреса и адреса электронной почты);

2. включите в локальные акты положения о проведении оператором оценки соблюдения иностранными лицами, которым планируется трансграничная передача ПД,

конфиденциальности ПД и обеспечения безопасности ПД при их обработке;

3. проанализируйте и при необходимости скорректируйте существующую практику трансграничной передачи ПД и получения согласия на предмет ее оптимизации (то есть для сокращения количества случаев трансграничной передачи ПД и уменьшения числа получателей ПД в «неадекватных» юрисдикциях);

4. после анализа запросите у оставшихся актуальными зарубежных получателей ПД сведения, предусмотренные ч. 5 ст. 12 Закона № 152-ФЗ;

5. после запроса сведений у иностранных лиц уведомите Роскомнадзор о намерении осуществлять трансграничную передачу ПД;

6. проанализируйте и доработайте типовые формы договоров об обработке ПД и зарепите в них механизм уничтожения ПД их зарубежными получателями в случае принятия Роскомнадзором соответствующего решения. Внесите изменения в уже заключенные договоры;

7. отслеживайте процесс принятия проекта нового приказа Роскомнадзора «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

Правила трансграничной передачи ПД

Если ПД передаются в страну, которая обеспечивает адекватную защиту прав субъектов ПД, то нужно получить от иностранных лиц информацию о принимаемых ими мерах и условиях прекращения обработки ПД. Это государства — стороны Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также государства, обеспечивающие адекватную защиту прав субъектов персональных данных (утверждены Приказом Роскомнадзора от 15.03.2013 № 274). В этом случае достаточно отправить уведомление в Роскомнадзор о намерении осуществлять трансграничную передачу данных в эти страны.

Если ПД передаются в страну, которая не обеспечивает адекватную защиту прав субъектов ПД (например, в США, Китай), то нужно еще получить информацию о правовом регулировании ПД в этой стране. Кроме того, в таком случае передавать данные за границу можно будет только через 10 дней после уведомления Роскомнадзора (ст. 12 Закона № 152-ФЗ).

Дополнительные полезные материалы из СПС «КонсультантПлюс»:

- *Федеральный закон от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" {КонсультантПлюс}*
- *"Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" {КонсультантПлюс}*
- *Проект Приказа Роскомнадзора "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" (по состоянию на 19.07.2022) (подготовлен Роскомнадзором, ID проекта 01/02/07-22/00129709) {КонсультантПлюс}*