МАСШТАБНЫЕ ИЗМЕНЕНИЯ В 152-ФЗ. КАК ДЕЙСТВОВАТЬ ОПЕРАТОРАМ?

Илья Романов
CISA, CISM
Руководитель Отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

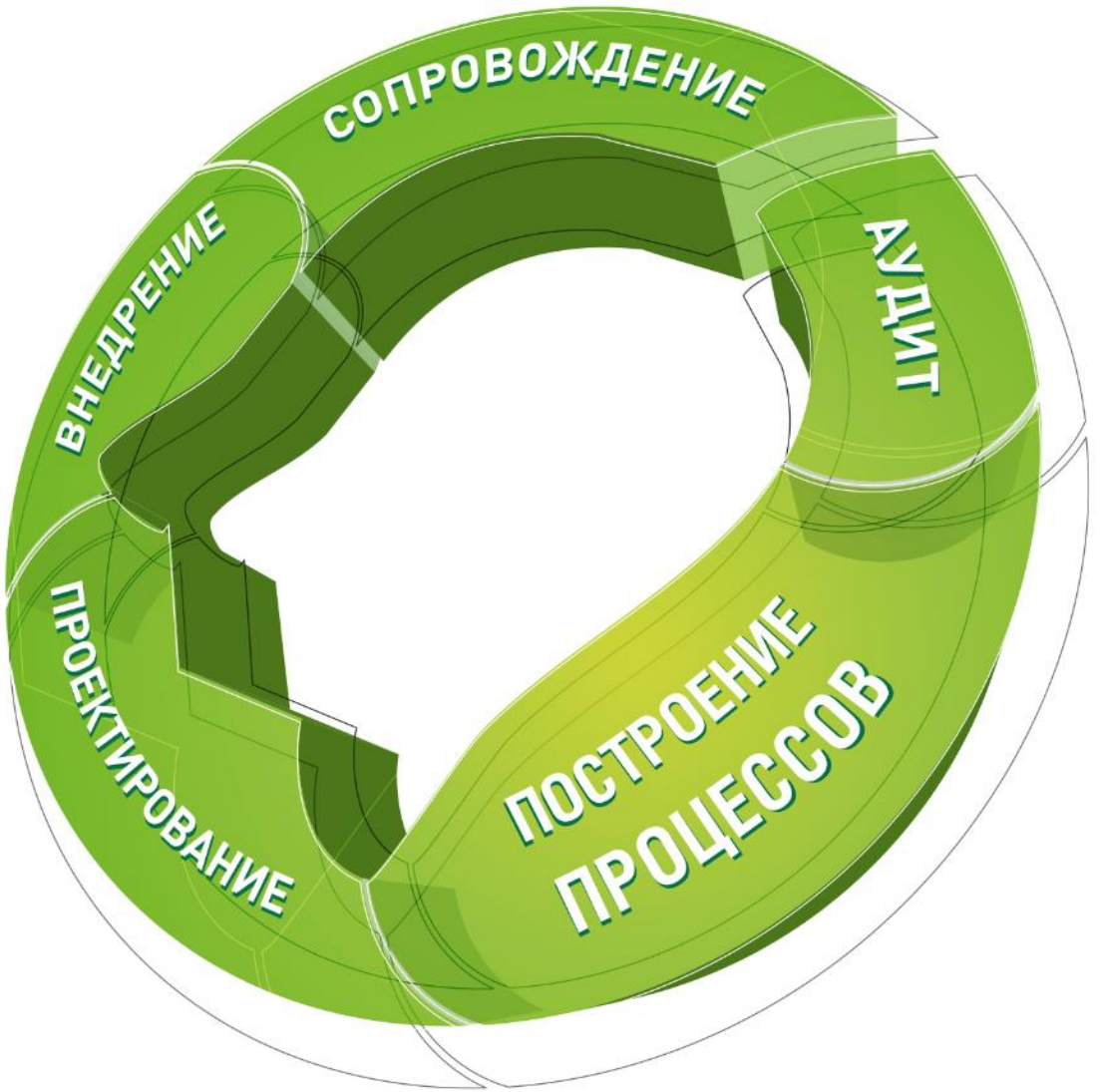
О компании

ДиалогНаука

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН.
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB.
- В настоящее время – системный интегратор в области информационной безопасности.

Направления деятельности

- 152-ФЗ и GDPR
- Объекты КИИ (187-ФЗ)
- PCI DSS
- Положения Банка России
- ГОСТ 57580
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



О компании «ДиалогНаука»: ключевые клиенты

Внесение изменений в 152-ФЗ

Изменения в 152-ФЗ «О персональных данных» внесены Федеральным законом от 14 июля 2022 года № 266-ФЗ

- Основная часть изменений вступила в силу 1 сентября 2022 года
- Оставшаяся часть изменений вступит в силу с 1 марта 2023 года

Принцип экстерриториальности

Ст. 1, ч. 1.1.

152-ФЗ распространяется на иностранных ЮЛ и ФЛ, если они обрабатывают ПДн граждан РФ (принцип экстерриториальности)

В КоАП появляется ст. 19.5.2, согласно которой иностранных лиц, осуществляющих деятельность в сети «Интернет» на территории РФ, будут штрафовать за нарушение запрета на сбор ПД граждан РФ (до 18 млн. рублей при повторном нарушении).

Что делать: если есть контрагенты – иностранные ЮЛ или ФЛ, которые обрабатывают ПДн граждан РФ – рекомендуем предупредить их о появлении новых требований.

Требования к договорам с субъектами ПДн

Ст. 6, ч. 1, п. 5

Заключаемый с субъектом ПДн договор не может содержать положения, ограничивающие права и свободы субъекта ПДн, а также положения, допускающие в качестве условия заключения договора бездействие субъекта ПДн.

Аналогичные положения в ст. 16 ФЗ «О защите прав потребителей» – запрещается

1) необоснованный сбор ПДн потребителей,

2) включение в договоры условий, навязывающих доп. товары и услуги

Что делать: проанализировать содержание договоров, при необходимости скорректировать разделы об обработке ПДн в них, уделив внимание соответствию предмета договора и заявленных в нем целей обработки ПДн, необходимости и пропорциональности обработки указанных в договоре ПДн.

Поручение обработки ПДн

Ст. 6, ч. 3, 6

Расширены требования к составу поручения обработки ПДн. Обработчик должен по запросу Оператора предоставлять свидетельства выполнения поручения (в том числе мер по защите). Обработчик должен уведомлять Оператора об инцидентах.

Если оператор поручает обработку ПДн иностранному ФЛ или иностранному ЮЛ, ответственность за действия указанных лиц несет оператор и лицо, осуществляющее обработку по поручению

Что делать: обновить типовую форму поручения обработки ПДн и обеспечить подписание поручений обработки ПДн по новой форме.

Дополнительные требования к согласию

Ст. 9, ч. 1

Дополнительные требования к согласию – должно быть **предметным** и **однозначным**

Критерии предметности и однозначности?

Что делать: проанализировать согласия на обработку данных и скорректировать их при необходимости

Обработка биометрических ПДн

Ст. 11

Предоставление биометрических ПДн не может быть обязательным. Оператор не вправе отказывать в обслуживании в случае отказа субъекта ПДн предоставить биометрические ПДн, если это не предусмотрено законом.

Что делать: проанализировать существующую практику обработки биометрических ПДн, внести корректировки в процессы, при необходимости.

Сроки взаимодействия с субъектами

Ст. 14, ч. 3, 7

Срок ответа на запрос субъекта об обрабатываемых ПДн – 10 рабочих дней. Срок может быть продлен не более чем на 5 рабочих дней в случае мотивированного уведомления субъекта с указанием причин продления.

Субъект вправе запросить в том числе информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 (Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных 152-ФЗ)

Что делать: Скорректировать формы локальных актов в соответствии с новыми требованиями, в т.ч. относительно новых сроков реагирования на запросы. Быть готовым при получении запроса от субъекта об обрабатываемых Оператором ПДн предоставлять ответ в течение 10 рабочих дней.

Требования к локальным актам

Ст. 18.1

Политика и иные локальные акты по вопросам обработки ПДн должны включать в себя детальный состав данных, перечисленный в ч.2 ст.18.1 (для каждой цели – субъекты, состав данных, сроки, порядок уничтожения)

Предусмотрена разработка и утверждение Роскомнадзором требований (методики) в отношении оценки вреда субъектам ПД (норма вступает в силу с 01.03.2023)

Что делать: дополнить локальные акты, проанализировать реализуемые процессы на предмет возможности их обоснования соответствующими положениями законодательства РФ.

Требования к локальным актам

Ст. 18, ч. 2

Политика оператора в отношении обработки ПДн должна быть доступна на тех страницах Интернет-сайтов, которые используются для сбора ПДн.

Что делать: проверить наличие текста/ссылки на политику оператора в отношении обработки ПДн на страницах/разделах Интернет-ресурсов (сайтов и мобильных приложений), используемых для сбора ПДн.

Взаимодействие с ГосСОПКА

Ст. 19

Все операторы ПДн должны обеспечить взаимодействие с ГосСОПКА. Вся информация, передаваемая в ГосСОПКА, будет передаваться в Роскомнадзор. Предусмотрена разработка и утверждение ФСБ требований в отношении порядка взаимодействия операторов с ГосСОПКА.

Что делать: разработать процедуру взаимодействия с ГосСОПКА в шаблонах локальных актов после утверждения ФСБ соответствующего правового акта.

Взаимодействие с РКН

Ст. 20

С 30 календарных до 10 рабочих дней сокращаются сроки исполнения оператором запросов надзорных органов и субъектов ПДн по вопросам, связанным получением информации об обработке ПДн.

Срок можно продлить на 5 рабочих дней, если оператор мотивирует причины продления срока.

Что делать: скорректировать формы локальных актов в соответствии с новыми требованиями, в т.ч. относительно новых сроков реагирования на запросы, при получении соответствующего запроса предоставлять ответ в течение 10 рабочих дней.

Уведомление РКН об инцидентах

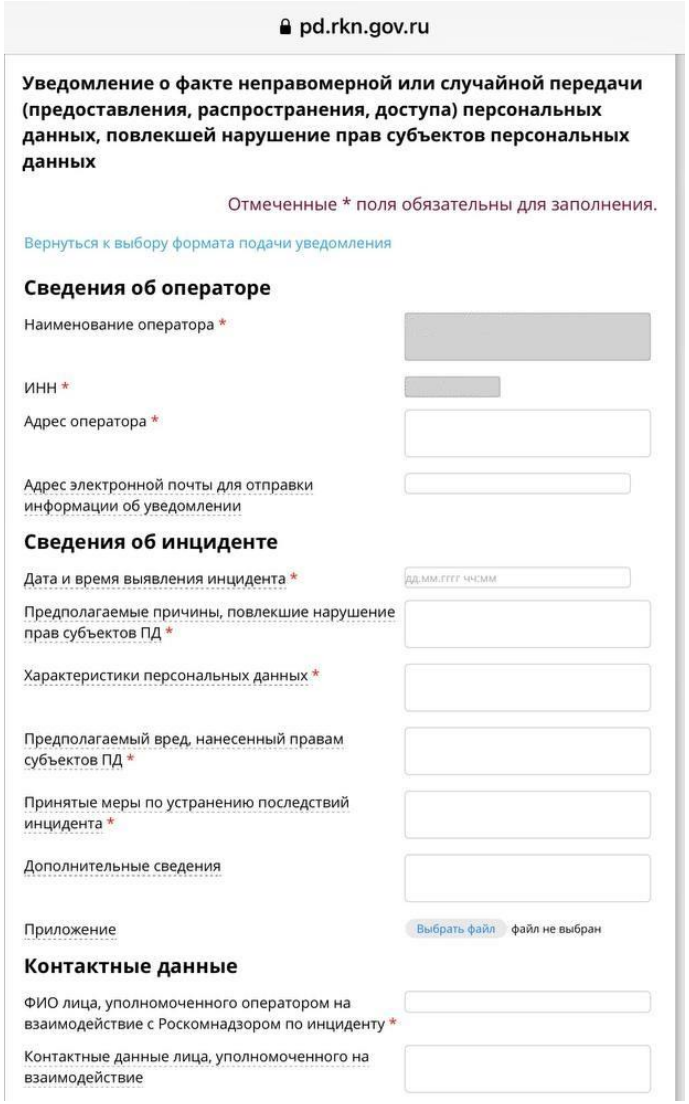
Ст. 21, ч. 3(1)

Оператор обязан информировать об инцидентах безопасности Роскомнадзор в течение 24 часов с момента обнаружения инцидента. И в течение 72 часов – о результатах внутреннего расследования выявленного инцидента.

Инцидент в данном контексте – «факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных».

Что делать: разработать и внедрить процедуру выявления, установления, нейтрализации и уведомления в отношении инцидентов.

Уведомление РКН об инцидентах - форма



- Дата и время выявления инцидента
- Причины, повлекшие нарушение прав субъектов ПДн
- Характеристики ПДн
- Предполагаемый вред правам субъектов ПДн
- Принятые меры по устранению последствий

Требование о прекращении обработки ПДн

Ст. 21, ч. 5(1)

Если субъект просит оператора прекратить обработку ПДн – оператор должен в течение 10 рабочих дней прекратить обработку. Срок можно продлить на 5 рабочих дней с предоставлением обоснования продления срока субъекту.

Что делать: при получении от субъекта запроса с просьбой прекратить обработку необходимо прекращать обработку в течение 10 рабочих дней (разработать и внедрить соответствующую процедуру)

Уничтожение ПДн

Ст. 21, ч. 7

Предусмотрена разработка и утверждение Роскомнадзором требований в отношении подтверждения факта уничтожения ПДн (возможно, будет представлена форма акта об уничтожении).

Что делать: внедрить форму/процедуру подтверждения уничтожения ПДн, предложенную Роскомнадзором, в локальные акты.

Уведомление об обработке ПДн

Ст. 22, ч. 2

Существенно сокращается количество случаев, освобождающих операторов от необходимости уведомлять Роскомнадзор об обработке ПДн.

Уведомление не требуется:

- Обработка в ГИС, созданных в целях защиты безопасности государства и общественного порядка;
- Обработка исключительно без использования средств автоматизации;
- Обработка в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности…

Что делать: подать уведомление об обработке ПДн.

Состав уведомления об обработке ПДн

Ст. 22, ч. 2

Состав уведомления теперь будет включать в себя расширенную информацию об обработке ПДн для каждой цели:

оператор для каждой цели обработки ПДн указывает категории ПДн, категории субъектов, ПДн которых обрабатываются, правовое основание обработки ПДн, перечень действий с ПДн, способы обработки ПДн

Что делать: подать уведомление об обработке ПДн, когда появится обновленная Роскомнадзором форма уведомления.

Состав уведомления об обработке ПДн

Формы уведомлений будут утверждены приказом Роскомнадзора. До этого оператор вправе заполнить форму уведомления об обработке персональных данных на Портале персональных данных Роскомнадзора или направить такое уведомление в адрес территориального управления ведомства по месту регистрации оператора на бумажном носителе по форме, утвержденной Приказом от 30.05.2017 № 94.

После вступления в силу приказа Роскомнадзора, устанавливающего новую форму уведомления, оператор может направить уведомление о внесении изменений в ранее представленные сведения в Реестр операторов, осуществляющих обработку персональных данных.

Предельный срок уведомления Роскомнадзора об обработке персональных данных не определен. Таким образом, 1 сентября 2022 не является крайним сроком подачи уведомления об обработке персональных данных.

Трансграничная передача

Ст. 12 (норма вступает в силу с **01.03.2023**)

В отношении трансграничной передачи ПДн вводится два режима ее осуществления:

1) уведомительный (при передаче ПДн в «адекватные» страны) и

2) разрешительный (при передаче ПДн в «неадекватные» страны).

Что делать: В случае наличия случаев передачи ПДн в «неадекватные» страны провести оценки соблюдения органами власти иностранных государств, иностранными физическими лицами, иностранными юридическими лицами, которым планируется трансграничная передача ПДн, конфиденциальности ПДн и обеспечения безопасности ПДн при их обработке. Подготовить и подать уведомление(я) о трансграничной передаче по форме Роскомнадзора (для всех стран).

Трансграничная передача

Оператор до подачи уведомления обязан получить следующие сведения:

1) сведения о принимаемых мерах по защите передаваемых ПДн и об условиях прекращения их обработки;

2) информация о правовом регулировании в области ПДн иностранного государства (в случае, если осуществляется передача в «неадекватные» страны);

3) сведения о получателях ПДн (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

Указанные сведения может запросить РКН при рассмотрении уведомления.

Трансграничная передача - уведомление

УВЕДОМЛЕНИЕ
об осуществлении трансграничной передачи персональных данных

Наименование оператора: ООО «Организация»

ИНН: 771234567890

Наличие в РОПД: да

Регион регистрации: г. Москва

Адрес электронной почты: pochta@mail.ru

ФИО лица, ответственного за организацию обработки персональных данных: Иванов Иван Иванович

Номер контактного телефона, почтовые адреса и адреса электронной почты: +79991234567, 123456, г. Москва, ул. Комсомольская, д. 1, оф. 1, pochta1@mail.ru

Цели трансграничной передачи:

1:Организация командирования работников Организации

Правовое основание трансграничной передачи:

наличие согласия субъекта персональных данных на обработку его персональных данных;

Категории передаваемых персональных данных:

Персональные данные: фамилия, имя, отчество; дата рождения; год рождения; месяц рождения; место рождения; пол; адрес электронной почты; гражданство, данные документа, удостоверяющего личность за пределами Российской Федерации

Специальные категории персональных данных: -

Биометрические персональные данные: -

Категории субъектов ПД, персональные данные которых передаются: Работники

Иностранные государства, на территории которых осуществляется передача: Армения, Греция, Грузия, Франция, Италия, Испания, Китай

Дата окончания проведения оценки: 01.08.2022

Состав уведомления:

- Цели передачи
- Правовое основание передачи
- Категории передаваемых ПДн
- Категории субъектов ПДн
- Перечень иностранных государств
- Дата оценки

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: info@DialogNauka.ru