РЕФОРМА 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ». ОПЫТ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ.

Илья Романов
Руководитель Отдела консалтинга
АО «ДиалогНаука»

ДиалОгНаука

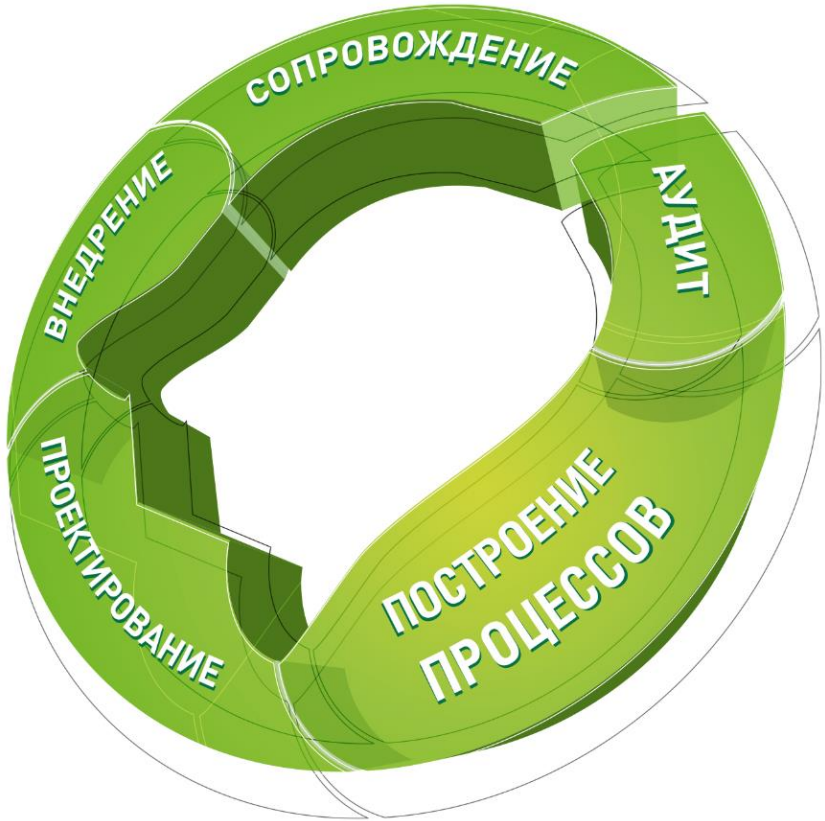
О компании

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)
- Положения Банка России
- ГОСТ 57580
- PCI DSS
- ISO 27001
- АСУ ТП
- Коммерческая тайна
- Сведения ДСП
- Защита ГИС



О компании «ДиалогНаука»: ключевые Заказчики

Внесение изменений в 152-ФЗ

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

- Оценка вреда субъектам ПДн;
- Требования к содержанию политики в отношении обработки ПДн и локальных актов Оператора;
- Требования к поручению обработки ПДн;
- Порядок уничтожения ПДн;
- Уведомление об инцидентах;
- Особенности подачи уведомления об обработке ПДн;
- Трансграничная передача.

Оценка вреда субъектам ПДн

- ✓ Приказ Роскомнадзора от 27 октября 2022 г. № 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона "О персональных данных"

- ✓ Примеры критериев определения степени вреда:
  - обработка биометрии, или спецкатегорий;
  - обработка ПДн несовершеннолетних;
  - обезличивание с целью скоринга и оказания услуг по прогнозированию;
  - поручение обработки иностранному лицу;
  - ведение общедоступных источников;
  - и др. критерии, **касающиеся состава, целей и особенностей обработки ПДн**.

Оценка вреда субъектам ПДн

Пример 1.

Критерий:

- ✓ обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются оператором для установления личности субъекта ПДн, **за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических ПДн.**

Комментарий:

- ✓ В случае обработки ПДн в ЕБС критерий неприменим.

Оценка вреда субъектам ПДн

Пример 2.

Критерии:

- ✓ сбор ПДн с использованием баз данных, находящихся за пределами РФ;
- ✓ обработка ПДн в дополнительных целях, отличных от первоначальной цели сбора

Комментарий:

- ✓ Если эти критерии применимы, то нарушаются требования 152-ФЗ

Оценка вреда субъектам ПДн

Пример 3.

✓ А что, если ни один из критериев не применим?

Комментарий:
~~Вариант 1 – Субъектам не может быть причинен вред~~
Вариант 2 – Не может быть причинена ни одна из степеней вреда, согласно Приказу РКН

Оценка вреда субъектам ПДн

- ✓ Степень вреда субъектам ПДн не определяется:
  - объемом обрабатываемых сведений;
  - оценкой последствий в случае возможных инцидентов с ПДн;
  - реализуемыми мерами по защите.

- ✓ Согласно ПП-1119 определение типа угроз безопасности ПДн производится **с учетом оценки возможного вреда**, но каким образом учитывать такую оценку нормативные документы не поясняют.

Требования к локальным актам

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

Требования к локальным актам

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

Должны определять для каждой цели обработки ПДн:
- ✓категории и перечень ПДн;
- ✓категории субъектов ПДн;
- ✓способы обработки;
- ✓сроки обработки и хранения;
- ✓порядок уничтожения.

Требования к локальным актам

Оператор обязан издать:

- ✓ политику в отношении обработки ПДн;
- ✓ локальные акты по вопросам обработки ПДн,
- ✓ локальные акты, направленные на предотвращение, выявление и устранение последствий нарушений законодательства РФ

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

Поручение обработки ПДн

Расширены требования к составу поручения обработки ПДн:

- ✓ перечень ПДн, цели их обработки;
- ✓ требования, предусмотренные ч.5 ст.18 и ст.18.1 ФЗ-152 (обязанности при сборе и обработке ПДн);
- ✓ обязанность по запросу оператора ПДн предоставлять свидетельства принятия мер и соблюдения требований, установленных поручением и Законом о ПДн;
- ✓ требования к защите ПДн в соответствии со ст.19 ФЗ-152, включая требование уведомления оператора об инцидентах с ПДн*

* фактах неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн

Поручение обработки ПДн

Обработчик (лицо, осуществляющее обработку ПДн по поручению оператора)	**Ответственность перед субъектом ПДн**
Российское лицо	✓ Оператор ПДн
Иностранное лицо	✓ Оператор ПДн ✓ Обработчик

Уничтожение ПДн

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179 «Об утверждении Требований к **подтверждению уничтожения** персональных данных»

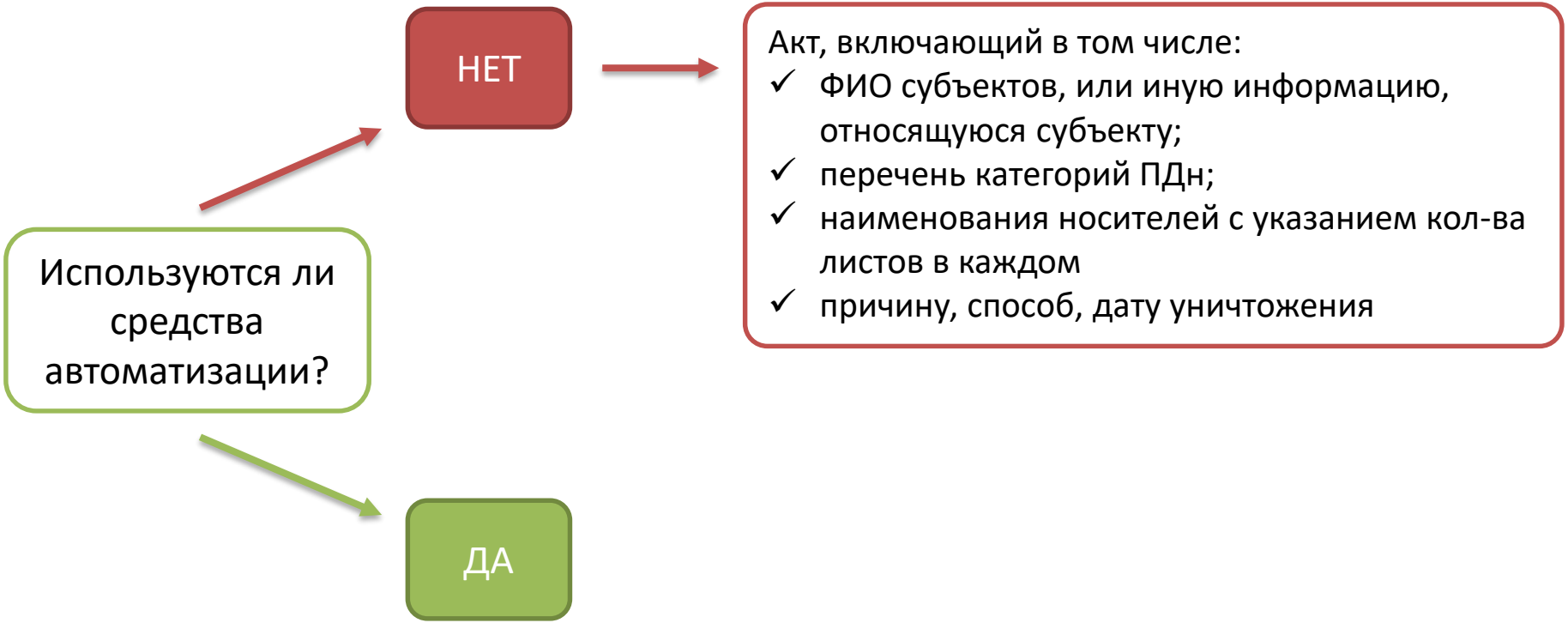
Требования применяются в случаях :

- ✓ выявления неправомерной обработки ПДн;
- ✓ достижения цели обработки ПДн;
- ✓ отзыва субъектом ПДн согласия на обработку ПДн.

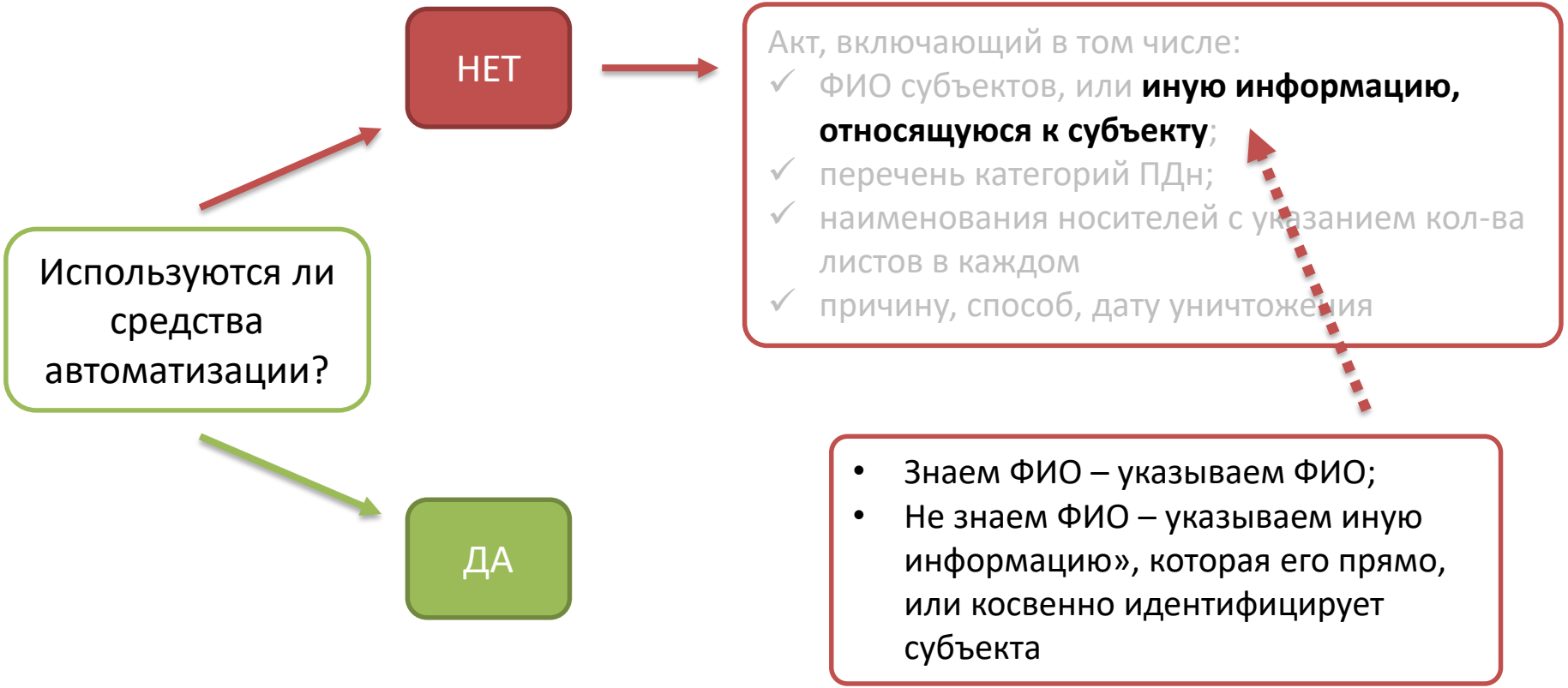
при отсутствии иных правовых оснований для продолжения обработки.

Уничтожение ПДн

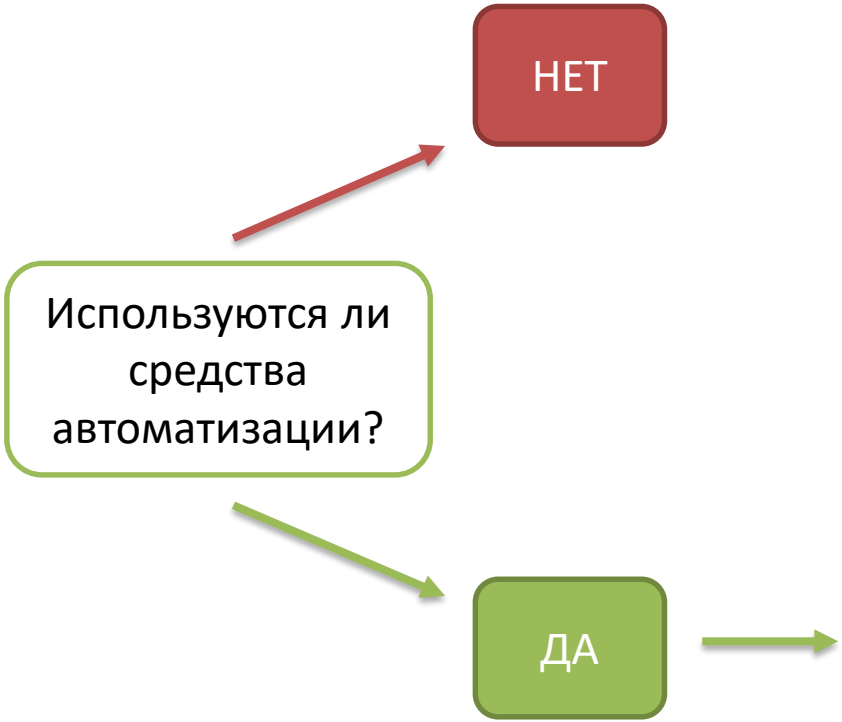
Уничтожение ПДн



Уничтожение ПДн



Уничтожение ПДн



Акт, включающий в том числе:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименования носителей с указанием кол-ва листов в каждом
- ✓ причину, способ, дату уничтожения

Выгрузка из журнала ИСПДн, включающая:

- ✓ ФИО субъектов, или иную информацию, относящуюся субъекту);
- ✓ перечень категорий ПДн;
- ✓ наименование ИСПДн;
- ✓ причину и дату уничтожения

Уничтожение ПДн

- ✓ Если выгрузка из журнала не позволяет указать отдельные сведения, недостающие сведения вносятся в акт.
  - Вопрос: А можно ли вообще не делать выгрузку?

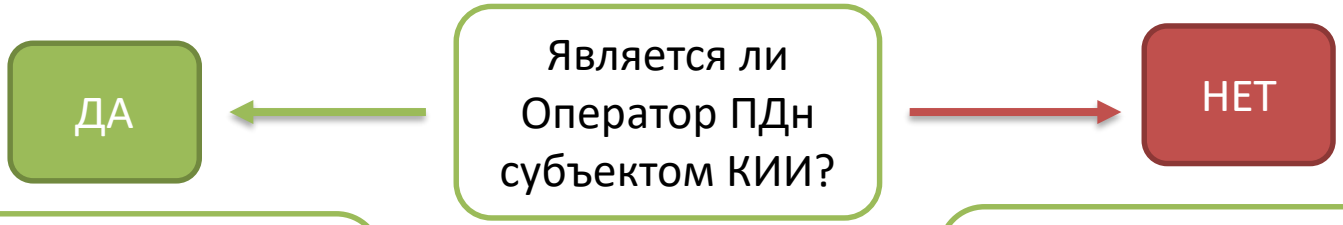
- ✓ Акт и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения ПДн.

Уведомление об инцидентах

Ст. 19 – Обязанность обеспечения взаимодействия с ГосСОПКА, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.

Ст. 21 – Обязанность информирования о факте неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, **повлекшей нарушение прав субъектов ПДн**, а также о результатах внутреннего расследования.

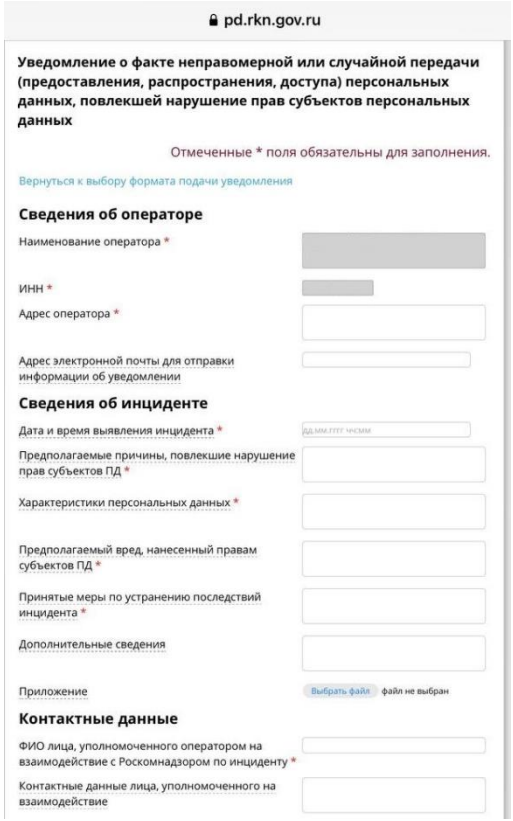
Уведомление об инцидентах



- ✓ В течение 24 часов – подача информации в ГосСОПКА

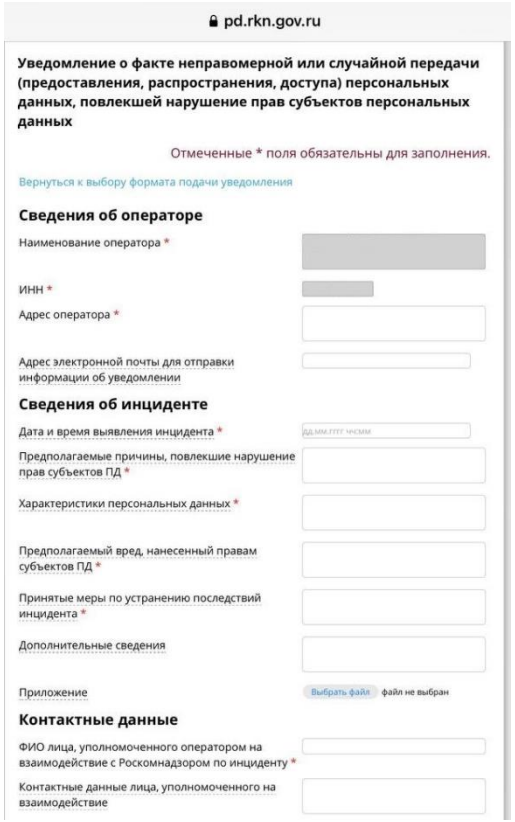
- ✓ В течение 24 часов – уведомление РКН об инциденте
- ✓ В течение 72 часов – уведомление РКН о результатах расследования

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

Уведомление РКН об инцидентах - форма



pd.rkn.gov.ru

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *

ИНН *

Адрес оператора *

Адрес электронной почты для отправки информации об уведомлении

Сведения об инциденте

Дата и время выявления инцидента *

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *

Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение

Выбрать файл файл не выбран

Контактные данные

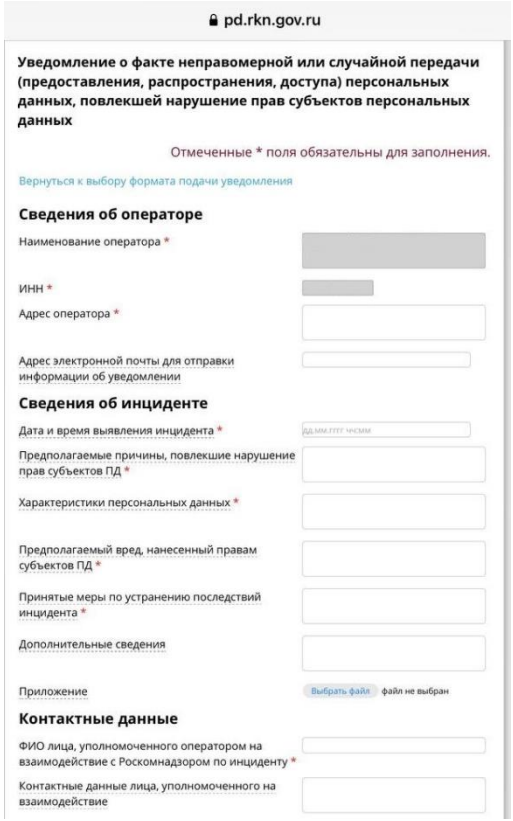
ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

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

- ✓категории субъектов
- ✓кол-во записей
- ✓перечень категорий
- ✓актуальность БД
- ✓период сбора ПДн

Уведомление РКН об инцидентах - форма



pd.rkn.gov.ru

Уведомление о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

Отмеченные * поля обязательны для заполнения.

Вернуться к выбору формата подачи уведомления

Сведения об операторе

Наименование оператора *

ИНН *

Адрес оператора *

Адрес электронной почты для отправки информации об уведомлении

Сведения об инциденте

Дата и время выявления инцидента *

Предполагаемые причины, повлекшие нарушение прав субъектов ПД *

Характеристики персональных данных *

Предполагаемый вред, нанесенный правам субъектов ПД *

Принятые меры по устранению последствий инцидента *

Дополнительные сведения

Приложение

Выбрать файл файл не выбран

Контактные данные

ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту *

Контактные данные лица, уполномоченного на взаимодействие

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

В соответствии со статьями 18.1 и 19

Уведомление РКН о расследовании - форма

- ✓ Результаты расследования, в том числе информация о
  - причинах инцидента;
  - вреде, нанесенном правам субъектов;
  - информационной системе;
  - мерах, принятых по результатам расследования.

- ✓ Сведения о лицах, действия которых стали причиной инцидента:
  - ФИО, должность (в отношении работника);
  - ФИО, наименование, IP-адрес, предполагаемое местонахождение и иные сведения (в отношении посторонних лиц)

Уведомление об обработке ПДн

Ст. 22, ч. 2 – Сокращено количество случаев, освобождающих от необходимости уведомлять Роскомнадзор об обработке ПДн.

Больше **не являются** исключением случаи:

- ✓ Обработки ПДн в соответствии с трудовым законодательством;
- ✓ Обработки ПДн для исполнения договора.

Уведомление **не требуется** в случаях:

- ✓ Обработки в ГИС, созданных в целях защиты безопасности государства и общественного порядка;
- ✓ Обработки исключительно без использования средств автоматизации;
- ✓ Обработки, согласно законодательству о транспортной безопасности.

Состав уведомления об обработке ПДн

Ст. 22, ч. 2

Оператор **для каждой цели обработки ПДн** указывает

- ✓ категории ПДн;
- ✓ категории субъектов ПДн;
- ✓ правовое основание обработки ПДн;
- ✓ перечень действий с ПДн;
- ✓ способы обработки ПДн.

Трансграничная передача - уведомление

- ✓ Больше нельзя подать уведомление **об осуществляемой** трансграничной передаче ПДн.
- ✓ Перед началом трансграничной передачи ПДн – нужно подать уведомление о таком намерении.
- ✓ Если поданные ранее сведения о трансграничной передаче изменились – нужно также подать уведомление.
- ✓ Роскомнадзор по результатам рассмотрения уведомления о намерении осуществлять трансграничную передачу ПДн может ограничить или запретить такую передачу (Постановление Правительства № 24 от 16 января 2023).

Трансграничная передача - уведомление

Постановление Правительства РФ от 29 декабря 2022 г. N 2526

Содержит перечень случаев, при которых:

- ✓ **Уведомление о ТГП можно не подавать**, например:
  - воздушные и морские перевозки, железнодорожное и автомобильное сообщения;
  - обеспечение транспортной безопасности;
  - оказание услуг почтовой связи;
  - осуществление международного автоматического обмена финансовой информацией;
- ✓ Уведомление о ТГП подавать нужно, но **Роскомнадзор не сможет запретить такую передачу**, например:
  - обеспечение платежей с использованием платежных систем и платежной инфраструктуры;
  - оказание услуг связи.

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

Состав уведомления о намерении осуществлять трансграничную передачу ПДн

- ✓ Цель передачи;
- ✓ Правовое основание;
- ✓ Категории передаваемых ПДн;
- ✓ Категории субъектов ПДн;
- ✓ Иностранные государства, на территории которых осуществляется передача.

Трансграничная передача

Важно помнить и про «базовые» принципы ФЗ-152 при осуществлении трансграничной передачи ПДн. Во многих случаях такая передача требует:

- ✓ Согласия субъекта ПДн на передачу.
- ✓ Поручения обработки ПДн иностранному лицу.

Вопросы?

115230 Москва,
1-й Нагатинский проезд, д. 10, стр. 1

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

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