Защита персональных данных в ритейле | Алексей Мунтян | *11.08.2023*

Алексей Мунтян, *15 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель Russian Privacy Professionals Association - RPPA.ru

Внешний Data Protection Officer в нескольких транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru

t.me/prv_adv

Telegram-канал

3 Что такое персональные данные?

Персональные данные – любая информация, относящаяся к прямо или косвенно определяемому / определенному физическому лицу

≠ точно **идентифицирующая** конкретного человека

= которую можно **ассоциировать** с человеком

- Идентификационные данные
- Личность и семья
- Образование и профессия
- Трудовая деятельность, воинский учет, госслужба
- Страхование, пенсия, налоги
- Поездки и транспорт
- Деловая (экономическая) деятельность

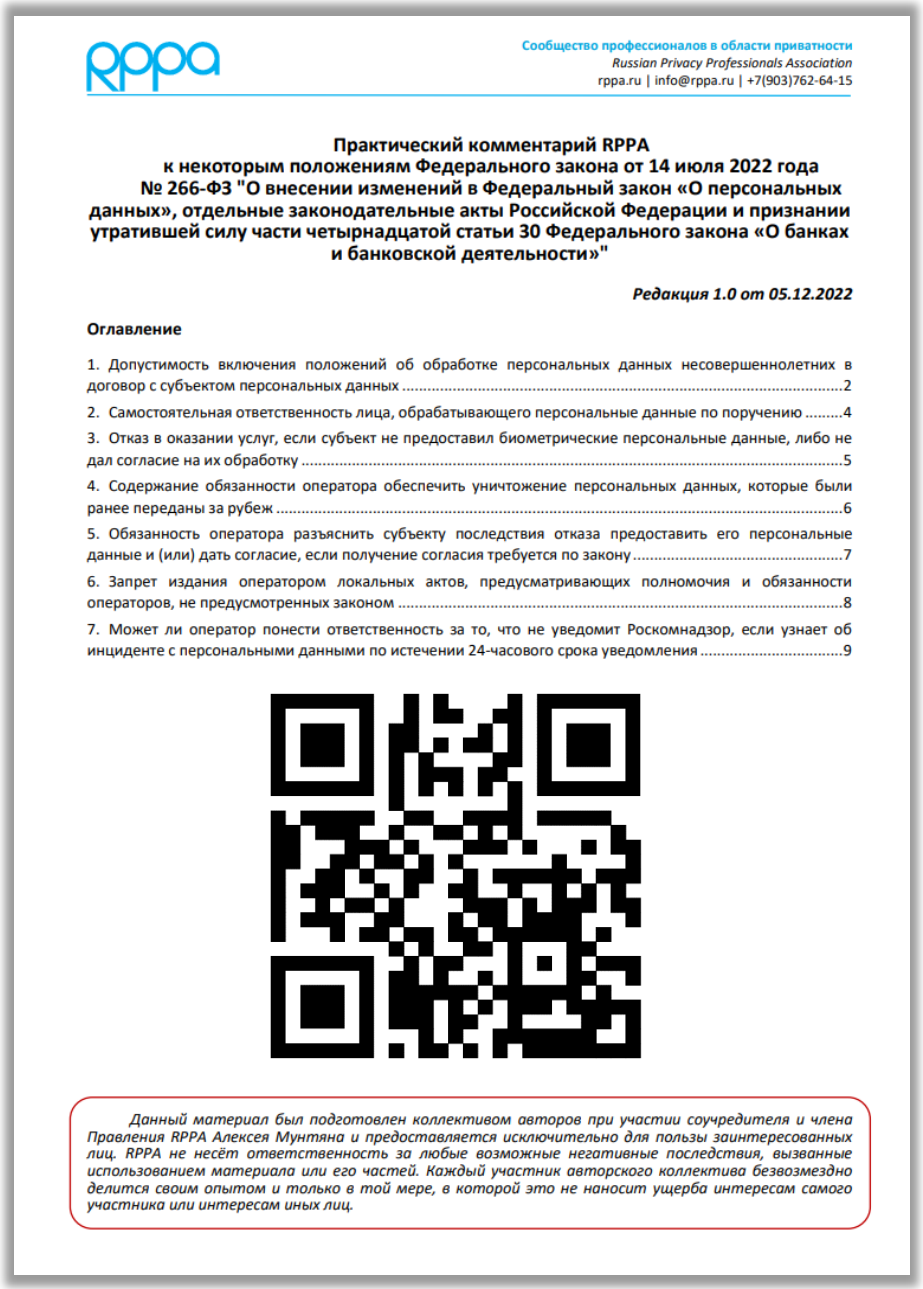
- Договоры и покупки
- Мероприятия, взаимодействия и спорт
- ИТ, связь и Интернет
- Геолокация и навигация
- Диагностика и телеметрия
- Медицинские данные
- Биометрия, геном и антропометрика
- Особо чувствительные данные

4 Актуальные тренды законодательства

« ...Русь, куда ж несешься ты? »

t.me/prv_adv | muntyan.alexey@gmail.com

5 Комментарий к новым нормам 152-ФЗ



Сообщество профессионалов в области приватности
Russian Privacy Professionals Association
rppa.ru | info@rppa.ru | +7(903)762-64-15

Практический комментарий RPPA
к некоторым положениям Федерального закона от 14 июля 2022 года № 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»"

Редакция 1.0 от 05.12.2022

Оглавление

Практический комментарий RPPA к некоторым положениям 266-ФЗ от 14.07.2022, в котором рассматриваются следующие вопросы:

- ◇ Допустимость включения положений об обработке ПД несовершеннолетних в договор с субъектом ПД
- ◇ Самостоятельная ответственность лица, обрабатывающего ПД по поручению
- ◇ Отказ в оказании услуг, если субъект не предоставил биометрические ПД, либо не дал согласие на их обработку
- ◇ Содержание обязанности оператора обеспечить уничтожение ПД, которые были ранее переданы за рубеж
- ◇ Обязанность оператора разъяснить субъекту последствия отказа предоставить его ПД и (или) дать согласие, если получение согласия требуется по закону
- ◇ Запрет издания оператором локальных актов, предусматривающих полномочия и обязанности операторов, не предусмотренных законом
- ◇ Может ли оператор понести ответственность за то, что не уведомит Роскомнадзор, если узнает об инциденте с ПД по истечении 24-часового срока уведомления

https://rppa.ru/_media/analitika/rppa_comments_266fz.pdf

6 Обработка ПД на основании договора с субъектом ПД

П.5. Ч.1 СТ.6 152-ФЗ «... Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных»

- ✖ БЕЗДЕЙСТВИЕ СУБЪЕКТА КАК ПОДТВЕРЖДЕНИЕ АКЦЕПТА ОФЕРТЫ
- ✖ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ, В ТОМ ЧИСЛЕ ДЛЯ НАПРАВЛЕНИЯ РЕКЛАМЫ
- ✖ ОБРАБОТКА ДАННЫХ В ЦЕЛЯХ, НЕ СВЯЗАННЫХ С ПРЕДМЕТОМ ДОГОВОРА
- ✖ БЕССРОЧНАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

ОБРАБОТКА НА ОСНОВАНИИ ТАКИХ УСЛОВИЙ ДОГОВОРА → СТ.13.11. КОАП РФ

Обновлённая ч.2 ст.16 ЗоЗПП – о недопустимых условиях договора, ущемляющих права потребителя

К недопустимым условиям договора, ущемляющим права потребителя, относятся:

1) условия, которые предоставляют продавцу (изготовителю, исполнителю, уполномоченной организации или уполномоченному индивидуальному предпринимателю, импортеру, владельцу агрегатора) право на односторонний отказ от исполнения обязательства или **одностороннее изменение условий обязательства** (предмета, цены, срока и **иных согласованных с потребителем условий**), за исключением случаев, если законом или иным нормативным правовым актом РФ предусмотрена возможность предоставления договором такого права;

5) условия, которые обусловливают приобретение одних товаров (работ, услуг) обязательным приобретением иных товаров (работ, услуг), в том числе **предусматривают обязательное заключение иных договоров**, если иное не предусмотрено законом;

15) **иные условия, нарушающие правила, установленные** международными договорами РФ, настоящим Законом, **законами и принимаемыми в соответствии с ними иными нормативными правовыми актами РФ**, регулирующими отношения в области защиты прав потребителей.

Практические рекомендации:

- предусмотреть в потребительском договоре специализированный раздел с исчерпывающим описанием условий обработки ПД
- не закладывать в договор «лазейки» или «резиновые формулировки», позволяющие в одностороннем порядке менять существенные элементы условий обработки ПД (например, состав операторов ПД и привлекаемых к обработке ПД лиц)

- не навязывать потребителю обработку его ПД со стороны компаний, входящих в одну группу с продавцом или являющихся участниками общей цифровой экосистемы/платформы

- не включать в потребительский договор элементы согласия потребителя на обработку ПД в целях, отличных от исполнения договора

Добавленная ч.4 ст.16 ЗоЗПП – о недопустимости избыточного сбора ПД потребителя

Продавец не вправе отказывать потребителю в заключении, исполнении, изменении или расторжении договора с потребителем в связи с отказом потребителя предоставить ПД, за исключением случаев, если **обязанность** предоставления таких данных **предусмотрена законодательством РФ** или непосредственно **связана с исполнением договора** с потребителем.

При предъявлении потребителем **требования о предоставлении информации о конкретных причинах и правовых основаниях**, определяющих невозможность заключения, исполнения, изменения или расторжения договора без **предоставления ПД**, в письменной форме (в том числе в форме электронного документа) продавец должен предоставить такую информацию в течение семи дней со дня предъявления указанного требования.

Продавец предоставляет информацию потребителю **в той форме, в которой предъявлено требование потребителя** о предоставлении информации о конкретных причинах и правовых основаниях, определяющих невозможность заключения, исполнения, изменения или расторжения договора без предоставления ПД, **если иное не указано в этом требовании**.

При предъявлении потребителем требования о предоставлении информации о конкретных причинах и правовых основаниях, определяющих невозможность заключения, исполнения, изменения или расторжения договора без предоставления ПД, **в устной форме такая информация должна быть предоставлена незамедлительно**.

Практические рекомендации:

- проанализировать состав получаемых у потребителя ПД на предмет возможности его минимизации и последующего обоснования с опорой на нормы законодательства РФ и предмета потребительского договора

- предусмотреть в локальных актах организации процедуру предоставления потребителю информации о конкретных причинах и правовых основаниях необходимости предоставления ПД, а также об альтернативной возможности приобретения продукции без предоставления ПД

- идентифицировать все возможные формы получения требования потребителя о предоставлении ему информации и учесть их в локальной процедуре организации

- подготовить для персонала, непосредственно взаимодействующего с потребителем, соответствующую инструкцию, а также провести сопутствующий тренинг персонала

9 Вредные советы

🧐 **Собирайте как можно больше данных - вдруг они пригодятся?**
Не становитесь «складом» или «кладбищем» данных. Когда от каких-то данных нет практической пользы... избавьтесь от них. И помните, что утечка данных - это не "если", а "когда".

🧐 **Молчание - знак согласия. Если "физик" не возражает против обработки его данных, то все отлично.**
Всегда получайте явное разрешение от субъекта на обработку данных в форме, позволяющей подтвердить факт его получения. Федеральный закон "Об электронной подписи" вам в помощь.

🧐 **Включайте положения о разрешении direct-marketing в договоры с "физиками" - они потерпят, а вам профит ;-)**
Рекламная рассылка или иной direct-marketing легализуются только с явного согласия субъекта. См. информационное письмо Банка России № ИН-06-59/70, ФАС России № АК/75514/21 от 06.09.2021 «О согласии на получение рекламы».

🧐 **Курица - не птица, а использование иностранных сервисов или зарубежная переписка - не трансграница.**
Почти любое взаимодействие с иностранными сервисами/контрагентами может быть квалифицировано как трансграничная передача персональных данных. С 01.03.2023 такая передача возможна только при уведомлении Роскомнадзора и отсутствии возражений с его стороны.

🧐 **Используйте биометрию как раньше: подключение к ЕБС - это для "госов".**
С 01.06.2023 у государства возникла квазимонополия на обработку биометрии, реализуемая через обязательное подключение всех обработчиков биометрии к Единой биометрической системе. Подумайте дважды, насколько биометрия критична для вашей деятельности.

Уведомление Роскомнадзора об инциденте (утечке) с ПД

Ч.3.1 СТ.21 152-ФЗ «В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, оператор обязан с момента выявления такого инцидента оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных»

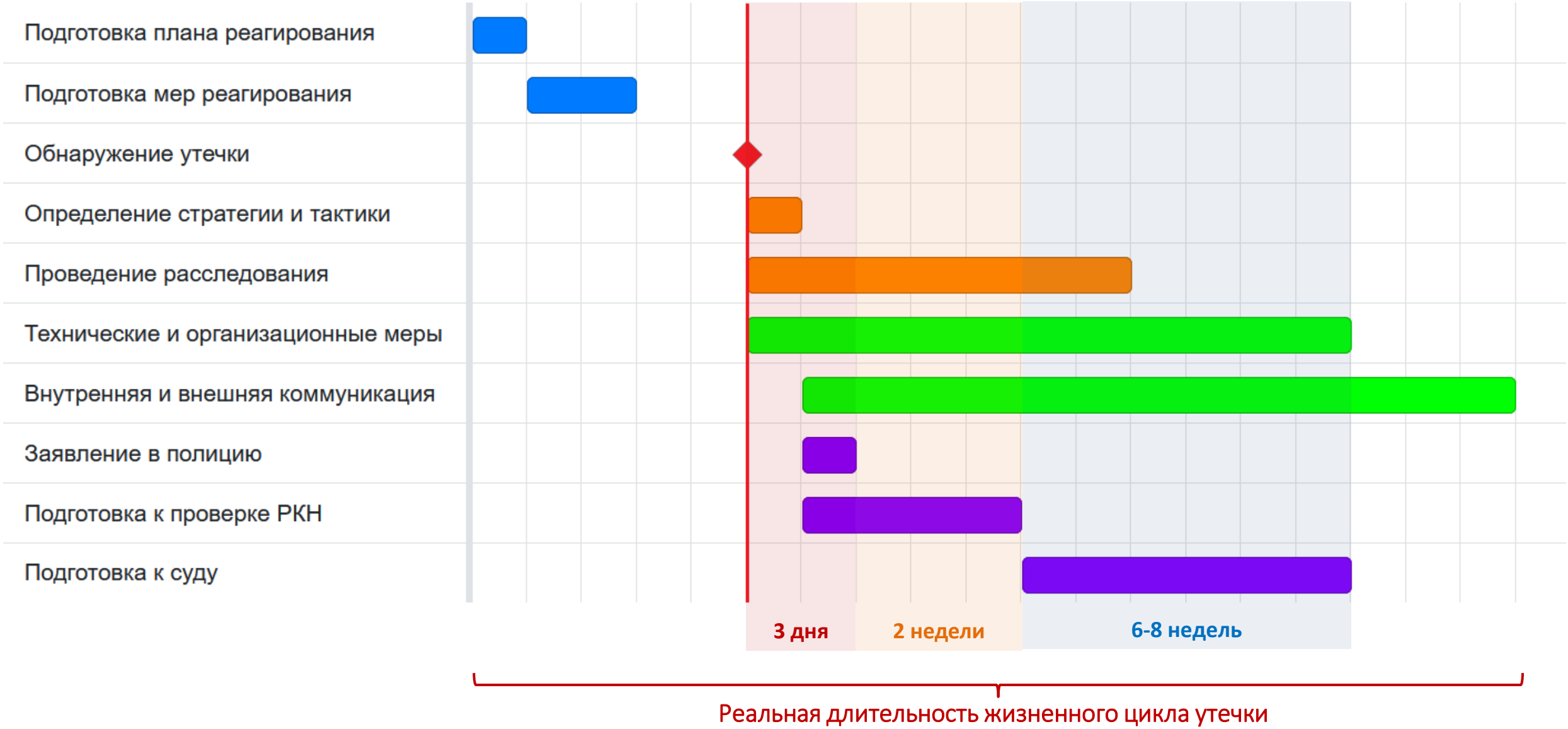
- ✓ ВЫЯВИЛИ НЕПРАВОМЕРНОЕ КОПИРОВАНИЕ БАЗЫ ДАННЫХ
- ✓ КОПИЯ БАЗЫ ДАННЫХ ДОСТУПНА В ИНТЕРНЕТ
- ✓ ПОЛУЧЕНО СООБЩЕНИЕ С УГРОЗОЙ РАСКРЫТЬ БАЗУ ДАННЫХ
- ✗ НСД ВНУТРЕННЕГО ПОЛЬЗОВАТЕЛЯ К БАЗЕ БЕЗ КОПИРОВАНИЯ
- ✗ СЛУЧАЙНОЕ УНИЧТОЖЕНИЕ БАЗЫ ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЕМ
- ✗ ПОДОЗРИТЕЛЬНАЯ АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЯ СИСТЕМЫ

24 ЧАСА — СООБЩЕНИЕ ОБ УТЕЧКЕ
ХАРАКТЕРИСТИКИ ДАННЫХ, ОБСТОЯТЕЛЬСТВА ИНЦИДЕНТА, ОТВЕТСТВЕННЫЙ ЗА ВЗАИМОДЕЙСТВИЕ

72 ЧАСА — РЕЗУЛЬТАТ РАССЛЕДОВАНИЯ
ПРИЧИНЫ УТЕЧКИ, ВИНОВНЫЕ ЛИЦА

11 **Формируем рабочую группу по реагированию на утечку**

Управляем утечкой: думаем медленно, решаем быстро



13 Перспективы усиления административной ответственности в 2023г.

Проект изменений в ст.13.11 КоАП РФ (*на 26.07.2023 - https://www.rbc.ru/technology_and_media/27/07/2023/64c15e069a79474102dac8b0*)		
Часть	**Состав правонарушения**	**Санкция (штраф)**
10	Неуведомление и (или) несвоевременное уведомление Роскомнадзора об обработке ПД	ФЛ: 5-10 тыс. ₽ ДЛ[1]: 15-50 тыс. ₽ ИП/ЮЛ: 100-300 млн. ₽
11	Неуведомление и (или) несвоевременное уведомление Роскомнадзора и **субъектов ПД** об утечке ПД[2], **повлекшей нарушение прав субъектов ПД**	ФЛ: 50-100 тыс. ₽ ДЛ: 400-800 тыс. ₽ ИП/ЮЛ: 1-3 млн. ₽
12	Действия (бездействия) оператора, повлекшие утечку ПД 1-10 тыс. субъектов и/или 10-100 тыс. идентификаторов[3]	ФЛ: 100-200 тыс. ₽ ДЛ: 800-1000 тыс. ₽ ИП/ЮЛ: 3-5 млн. ₽
13	Действия (бездействия) оператора, повлекшие утечку ПД 10-100 тыс. субъектов и/или 100-1000 тыс. идентификаторов	ФЛ: 200-300 тыс. ₽ ДЛ: 1-1,5 млн. ₽ ИП/ЮЛ: 5-10 млн. ₽
14	Действия (бездействия) оператора, повлекшие утечку ПД >100 тыс. субъектов и/или >1000 тыс. идентификаторов	ФЛ: 300-400 тыс. ₽ ДЛ: 1,5-2 млн. ₽ ИП/ЮЛ: 10-15 млн. ₽
15	Рецидив утечки ПД, предусмотренной ч.ч.12-14 ст.13.11 КоАП	ФЛ: 400-600 тыс. ₽ ДЛ: 2-4 млн. ₽ ИП/ЮЛ: 0,1-3% от годового оборота (мин. 15 млн. ₽ и макс. 500 млн. ₽)
16	Действия (бездействия) оператора, повлекшие утечку специальных категорий и/или биометрических ПД	ФЛ: 400-500 тыс. ₽ ДЛ: 2-3 млн. ₽ ИП/ЮЛ: 15-20 млн. ₽
17	Рецидив утечки специальных категорий и/или биометрических ПД оператором, который ранее наказывался по ч.ч.12-14, 16 ст.13.11 КоАП	ФЛ: 500-800 тыс. ₽ ДЛ: 3-5 млн. ₽ ИП/ЮЛ: 0,1-3% от годового оборота (мин. 20 млн. ₽ и макс. 500 млн. ₽)
Также предложено добавить **ст.13.11[4]** «Нарушение требований в области обработки биометрических ПД».		

[1] **Должностное лицо** – должностное лицо государственного или муниципального органа, сотрудник государственного или муниципального учреждения.

[2] **Юридическое лицо** – юридическое лицо, не являющееся государственным или муниципальным органом, государственным или муниципальным учреждением.

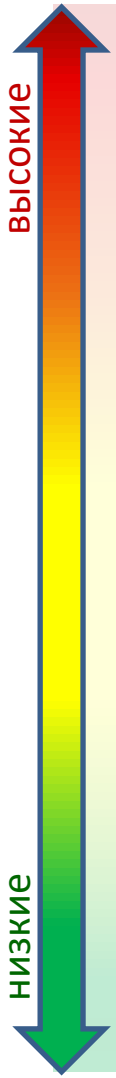
[3] **Утечка ПД** – факт неправомерной передачи (предоставления, распространения, доступа) ПД.

[4] **Идентификатор** – уникальные обозначения сведений о физическом лице, необходимые для определения такого лица.

Чек-лист для проверки Интернет-ресурса

Риски

Ранжирование возможных нарушений, определяемых исходя из позиции и практики Роскомнадзора



- → сбор ПД граждан РФ при нахождении БД Интернет-ресурса (хостинг-провайдера) за пределами РФ
- → сбор ПД в зарубежные БД посредством иностранных метрических программ *(например, Google Analytics)*
- → сбор ПД в зарубежные БД посредством сторонних веб-форм или сервисов
- → нет документа, определяющего политику в отношении обработки ПД (далее – «Политика»)
- → отсутствие ссылки на Политику на страницах, где предполагается сбор ПД
- → нет согласия на предоставление ПД неограниченному кругу лиц с использованием Интернет-ресурса
- → нет согласия на обработку ПД, когда такое согласие необходимо *(например, при использовании аналитических и рекламных файлов cookie, а также для целей прямого маркетинга)*
- → согласие на обработку ПД есть, но нет ссылки на его текст или вместо согласия дается ссылка на Политику, из которой нельзя однозначно установить содержание согласия *(цель и иные условия обработки ПД)*
- → отсутствие в Политике сведений о трансграничной передаче ПД при нахождении Интернет-ресурса за пределами РФ и/или при использовании иностранных метрических программ и сервисов *(например, Google Fonts)*
- → несоответствие объема ПД, собираемого веб-формой, положениям Политики
- → наличие ссылок на сторонние веб-формы сбора ПД (в т.ч. иностранные) без указания на это в Политике
- → мониторинг поведения пользователей без указания на это в Политике
- → отсутствие в Политике детального описания обработки ПД для каждой цели
- → отсутствие в Политике описания порядка прекращения обработки (уничтожения) ПД
- → избыточность объема собираемых ПД по отношению к заявленным целям их обработки
- → условием заключения пользовательского соглашения на Интернет-ресурсе является бездействие пользователя
- → обработка и трансграничная передача ПД на Интернет-ресурсе без подачи в Роскомнадзор уведомления

Дополнительно см. t.me/prv_adv

Благодарю за ваше внимание

t.me/prv_adv

Telegram-канал

Алексей Мунтян, *15 лет в Data Privacy*

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

Внешний Data Protection Officer в четырех транснациональных холдингах

+7 (903) 762-64-15

alexey.muntyan@privacy-advocates.ru