АДВОКАТСКОЕ БЮРО | ЕГОРОВ ПУГИНСКИЙ АФАНАСЬЕВ И ПАРТНЕРЫ

Существенные изменения правил обработки персональных данных

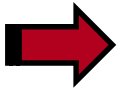
Елена Агаева – руководитель практики M&A и корпоративного права в Санкт-Петербурге
руководитель практики защиты персональных данных

С 1 сентября 2022 года - ужесточение правил обработки персональных данных

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"*

1 Расширена сфера применения Закона № 152-ФЗ

Установили **экстерриториальное действие** Закона № 152-ФЗ. Теперь закон применяется и к иностранным лицам, если они обрабатывают ПДн граждан РФ на основании договоров и соглашений, стороной которых являются россияне, либо на основании согласия на обработку ПДн.



С 1 сентября иностранные компании, получающие личные данные работников российских дочерних обществ, обязаны соблюдать все требования Закона № 152-ФЗ, в том числе о локализации ПДн граждан РФ.

2 Сокращен перечень случаев, когда оператор вправе обрабатывать ПДн без уведомления Роскомнадзора

С 1 сентября 2022 г. компании обязаны уведомить Роскомнадзор о намерении обрабатывать ПДн **в соответствии с трудовым законодательством** (*раньше такое основание подпадало под исключения*)**.** Разрабатывается новая форма уведомления.

NB: По-прежнему не направлять уведомление могут работодатели, которые обрабатывают персональные данные работников исключительно *без использования средств автоматизации*. При условии, что иные случаи обработки ПДн в компании не требуют направления уведомления.

3 Новые требования к согласию на обработку персональных данных

Теперь согласие должно быть конкретным, информированным, сознательным, **предметным и однозначным**.
Какое согласие считается предметным и однозначным, закон не расшифровывает.

4 Новые требования к содержанию локальных актов по вопросам обработки персональных данных

Теперь в ЛНА о ПДн для каждой цели обработки обязательно должны быть указаны:

- Категории и перечень обрабатываемых ПДн;
- Категории субъектов, данные которых обрабатываются;
- Способы, сроки обработки и хранения ПДн;
- Порядок уничтожения ПДн.

Необходимо также указать, какие действия компания предпринимает для предотвращения и выявления нарушений законодательства о ПДн и как будет устранять последствия нарушений.

Установлен запрет на наличие в ЛНА положений, которые ограничивают права субъектов ПДн или возлагают на них полномочия и обязанности, которых нет в законе.

Новые правила: к чему и как готовиться бизнесу

5 Расширены требования к содержанию поручения оператора на обработку персональных данных

В документе, которым оператор поручает обработку ПДн другому лицу, нужно указывать новую информацию: должны быть определены перечень ПДн, требования, предусмотренные ч. 5 ст. 18 (локализация ПДн) и ст. 18.1 Закона № 152-ФЗ (меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Законом № 152-ФЗ), обязанность по запросу оператора предоставлять документы и информацию, подтверждающие принятие мер и соблюдение требований, установленных в соответствии со ст. 6 Закона № 152-ФЗ, обязанность уведомлять оператора о случаях неправомерной или случайной передачи персональных данных и иные сведения.

6 Сокращен срок ответов на запросы

Уменьшен срок, в который нужно отвечать на запросы Роскомнадзора, работника или другого субъекта ПДн. С 1 сентября он составляет **10 рабочих дней** (ранее был 30 дней). При необходимости срок можно продлить на 5 рабочих дней.

NB: Теперь компания обязана раскрывать субъекту ПДн по его запросу информацию о правовых, организационных и технических мерах, которые компания принимает для обеспечения безопасности персональных данных.

7 Биометрические персональные данные

Теперь предоставление биометрических ПДн не может быть обязательным, за некоторыми исключениями. Отказать в обслуживании, если субъект не хочет предоставить такие данные или не дает согласие на их обработку, когда оно нужно, нельзя.

8 Ужесточение правил трансграничной передачи персональных данных

Введена обязанность уведомлять Роскомнадзор о намерении осуществить трансграничную передачу ПДн до начала осуществления деятельности по трансграничной передаче

С 1 марта 2023 г. операторы, которые осуществляют трансграничную передачу ПДн, обязаны направлять отдельное уведомление об этом в Роскомнадзор. Операторы, которые осуществляли трансграничную передачу до дня вступления в силу ФЗ № 266-ФЗ и продолжают осуществлять такую передачу после дня вступления его в силу, обязаны направить уведомление не позднее 1 марта 2023 г.

Срок рассмотрения уведомления Роскомнадзором - **10 рабочих дней** (в случае направления Роскомнадзором запроса оператору для оценки достоверности сведений в уведомлении рассмотрение уведомления приостанавливается до даты предоставления оператором запрошенной информации (срок ответа на запрос – **10 рабочих дней + 5 рабочих дней** при продлении).

В период рассмотрения уведомления передача персональных данных возможна **только в юрисдикцию**, **обеспечивающую адекватную защиту** прав субъектов персональных данных и **включенную в специальный перечень** Роскомнадзора. **Для передачи в юрисдикцию, не обеспечивающую соответствующую защиту**, необходимо будет ждать окончания срока рассмотрения уведомления Роскомнадзором.

NB: **Роскомнадзор актуализировал перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн** (Приказ Роскомнадзора от 05.08.2022 № 128). *В частности, в перечень добавлены КНР, Киргизия, Таиланд и др. Изменения вступают с силу с 1 марта 2023.*

Роскомнадзор **сможет запретить или ограничить** трансграничную передачу в целях:
- защиты основ конституционного строя РФ, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства, защиты экономических и финансовых интересов России, обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан РФ, суверенитета, безопасности, территориальной целостности и других интересов России на международной арене.

Трансграничная передача персональных данных

До подачи уведомления оператор должен провести оценку соответствия мер по защите персональных данных, принимаемых в иностранных государствах

Оператор обязан получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача ПДн, следующие сведения:

- сведения о принимаемых ими мерах по защите передаваемых ПДн и об условиях прекращения их обработки;
- информация о правовом регулировании в области ПДн иностранного государства, под юрисдикцией которого находятся указанные субъекты (за исключением определенных случаев)
- сведения об субъектам, которым планируется трансграничная передача ПДн (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

- Каким образом должна проводиться оценка?
- Какими документами должны подтверждаться выводы по результатам оценки?

9

Компании обязали сообщать в Роскомнадзор о неправомерной или случайной передаче ПДн

Сообщать нужно об утечке, которая произошла как по недосмотру ответственных работников, так и в результате хакерской атаки. Уведомление об утечке необходимо направить в течение **24 часов** с момента ее обнаружения.

В уведомлении нужно указать:

- сведения об инциденте;
- предполагаемые причины утечки ПДн;
- предполагаемый вред работникам, клиентам и правам других субъектов ПДн;
- принятые меры по устранению последствий инцидента;
- сведения о лице, которое уполномочено взаимодействовать с Роскомнадзором по инциденту.

Также при утечке нужно провести внутреннее расследование и сообщить в Роскомнадзор о результатах и лицах, действия которых стали причиной инцидента, если они есть. Срок — 72 часа с момента обнаружения.

Взаимодействие с ГосСОПКА:

Компании должны обеспечить взаимодействие с ФСБ через госсистему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России (ГосСОПКА). В том числе, теперь через эту систему нужно сообщать о кибератаках, повлекших утечку ПДн.

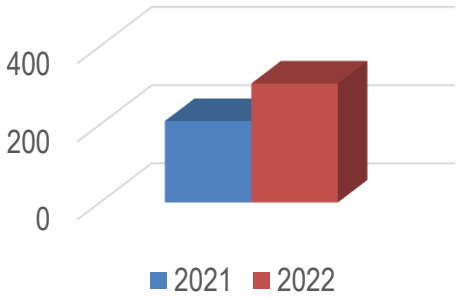
Утечки персональных данных

1. По данным Роскомнадзора, за первые шесть месяцев 2022 года доля обращений на тему незаконной обработки ПДн достигла 70% от общего числа.

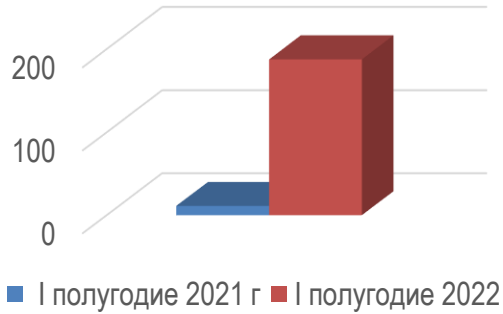
2. Количество утечек в России за первое полугодие 2022 г. составило 305 (+45,9% по сравнению с I полугодием 2021 г.) (по данным InfoWatch).

3. Объем похищенной информации увеличился более чем в 16 раз, составив 187,6 млн записей.
Таким образом всего за полгода в Сеть попало количество записей ПДн, которое превышает население России. (по данным InfoWatch).

Число утечек в России (по данным InfoWatch)



Количество утекших записей в России (по данным InfoWatch), млн



Утечки персональных данных

Законодательные инициативы в области утечек персональных данных

1. Оборотные штрафы для компаний за утечку персональных данных	2. Фонд материальных компенсаций для граждан, пострадавших от утечек	3. Уголовная ответственность за утечку персональных данных
Предлагается ввести **фиксированный штраф** за первую утечку данных, если от неё пострадали менее 10 тыс. клиентов компании. В остальных случаях будет оборотный штраф в размере от 1% до 3% от годового оборота компании. Компания может добиться **снижения такого штрафа**, если оперативно выявила утечку, публично призналась в утечке данных, провела внутреннее расследование и опубликовало его результаты, помогала надзорным органам, а в рамках расследования выяснилось, что утечка не произошла по причине нарушения требований информационной безопасности внутри компании.	Планируется создать **фонд материальных компенсаций для граждан**, пострадавших от утечек персональных данных из компаний. Предполагается, что в качестве финансовых средств в фонде будут использоваться оборотные штрафы, наложенные на компании за утечку данных. 	В разработке находится законопроект, предусматривающий **уголовную ответственность** для представителей компаний, которые допустили утечку персональных данных с тяжкими последствиями.

Утечки персональных данных: текущие варианты ответственности

Административная ответственность

- ч.1 ст. 13.11 КоАП РФ *(«Обработка персональных данных в случаях, не предусмотренных законодательством РФ»)* *(штраф в размере от 60 000 до 100 000 рублей)*

За повторное нарушение - штраф в размере от 100 000 до 300 000 рублей (ч. 1.1 ст. 13.11)

- ч.2 ст. 13.11 КоАП РФ *(«Обработка ПДн без согласия в письменной форме субъекта в случаях, когда такое согласие должно быть получено»)* *(штраф в размере от 30 000 до 150 000 рублей)*

Уголовная ответственность

- статья 137 УК РФ («Нарушение неприкосновенности частной жизни»)
- статья 272 УК РФ («Неправомерный доступ к компьютерной информации»)
- статья 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ»)

Гражданско-правовая ответственность

- статья 15 Закона РФ от 07.02.1992 N 2300-1 «О защите прав потребителей» («Компенсация морального вреда»)
- ч.2 ст. 24 Закона о персональных данных (“Ответственность за нарушение требований закона”)

Еще не все: изменения, вступающие в силу в 2023 году

Три изменения, которые вступят в силу 1 марта 2023 года

1. Ужесточаются правила трансграничной передачи персональных данных	До передачи ПДн за рубеж необходимо будет направить в Роскомнадзор **уведомление о намерении осуществить трансграничную передачу ПДн.** Срок рассмотрения уведомления — 10 рабочих дней. Срок может быть приостановлен. Пока уведомление рассматривают, передавать персональные данные можно **лишь в юрисдикцию, обеспечивающую адекватную защиту прав их субъектов.** Перечень целей, для которых Роскомнадзор может запретить или ограничить трансграничную передачу ПДн , расширится: добавится защита суверенитета, территориальной целостности, экономических, финансовых и иных интересов РФ на международной арене. Те, кто до 01.09.2022 осуществляли трансграничную передачу ПДн и продолжают ее осуществлять, обязаны **не позднее 01.03.2023** направить в Роскомнадзор уведомление.
2. Вводится новый срок для извещения Роскомнадзора об изменении сведений, указанных в уведомлении о начале обработки ПДн	Сделать это нужно не позднее **15-го числа месяца**, следующего за месяцем, в котором произошли изменения. Сейчас на уведомление дается 10 рабочих дней с момента изменения сведений.
3. Для обработки биометрических ПДн придется получать аккредитацию	Обрабатывать биометрические ПДн в информационных системах компании можно будет при соблюдении ряда условий. В том числе придется получить аккредитацию в Минцифры. **Без нее обрабатывать биометрические ПДн нельзя будет даже в целях обеспечения прохода работников на территорию организации посредством СКУД.** *NB: Скорее всего, выполнить требования по получению аккредитации смогут только крупные компании, которые имеют необходимое оборудование и лицензии.* Кроме того, при использовании биометрических персональных данных **для целей идентификации,** то есть для создания шаблонов таких данных, **обрабатывать их будет допустимо только в случаях, определенных Правительством РФ.** На данный момент таких случаев всего четыре.

АДВОКАТСКОЕ БЮРО
ЕГОРОВ ПУГИНСКИЙ АФАНАСЬЕВ И ПАРТНЕРЫ

СПАСИБО ЗА ВНИМАНИЕ!

191186, Россия,
Санкт-Петербург,
Невский пр., 24, офис 132,
Тел.: +7 (812) 332 96 81
Факс: +7 (812) 322 96 82
www.epam.ru

Елена Агаева
Руководитель практики защиты персональных данных

elena_agaeva@epam.ru