АДВОКАТСКОЕ БЮРО ЕГОРОВ ПУГИНСКИЙ АФАНАСЬЕВ И ПАРТНЕРЫ

Основные риски в сфере персональных данных: слабые места и защита для компании и менеджмента

Елена Агаева, адвокат, советник

10.12.2021

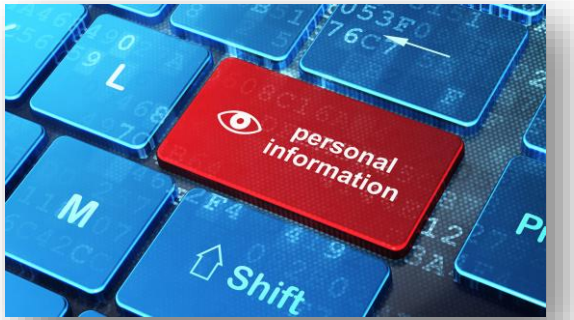
Персональные данные: почему это важно для компании и менеджмента

1. Введена **существенная ответственность** как для компаний, так и для должностных лиц.

2. Стало **больше проверок** регулятором.

3. Нарушения влекут серьезные **репутационные риски**.

4. Появились риски применения к российским компаниям зарубежных правил (**GDPR**), и **ответственность по ним значительна**.



АДВОКАТСКОЕ БЮРО ЕГОРОВ ПУГИНСКИЙ АФАНАСЬЕВ И ПАРТНЕРЫ

Штрафы выросли в 2 раза

Федеральный закон от 24.02.2021 № 19-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"

- ❑ **Увеличены штрафы за нарушения в области персональных данных.**
- ❑ **Установлена повышенная ответственность за повторные правонарушения.**

✓ Обработка персональных данных в случаях, не предусмотренных законодательством РФ в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных.		для ДЛ- от 10 тыс. до 20 тыс. руб.; для компаний – от 60 тыс. до 100 тыс. руб.; *при повторном правонарушении*: для ДЛ - от 20 тыс. до 50 тыс. руб.; для компаний – от 100 тыс. до 300 тыс. руб.
✓ Обработка персональных данных без согласия в письменной форме субъекта, когда такое согласие обязательно, либо нарушение требований к его содержанию.		для ДЛ- от 20 тыс. до 40 тыс. руб.; для компаний – от 30 тыс. до 150 тыс. руб.; *при повторном правонарушении*: для ДЛ - от 40 тыс. до 100 тыс. руб.; для компаний – от 300 тыс. до 500 тыс. руб.
✓ Неопубликование политики оператора в отношении обработки персональных данных или сведений о реализуемых требованиях к защите персональных данных.		для ДЛ- от 6 тыс. до 12 тыс. руб.; для компаний – от 30 тыс. до 60 тыс. руб.
✓ Невыполнение оператором требования об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.		для ДЛ- от 8 тыс. до 20 тыс. руб.; для компаний – от 50 тыс. до 90 тыс. руб.; *при повторном правонарушении*: для ДЛ - от 30 тыс. до 50 тыс. руб.; для компаний – от 300 тыс. до 500 тыс. руб.

Наиболее существенные риски

Наибольшие штрафы – нарушение «правила о локализации»

Для должностных лиц – от 100 000 до 200 000 рублей; для юридических лиц – **от 1 000 000 до 6 000 000 руб**.

При повторном правонарушении: для должностных лиц – от 500 000 до 800 000 руб.; для юридических лиц – **от 6 000 000 до 18 000 000 руб**.

Компания	Мера
Twitter, Facebook, WhatsApp (первое нарушение)	Штраф 4 млн. руб.
Facebook, Twitter (повторное нарушение)	Штраф 15 млн. руб. и 17 млн. руб. соответственно.
Центр немецкого языка (привлечение к ответственности директора)	Штраф на директора в относительно небольшом размере, но дело показательно само по себе.
Google	Штраф 3 млн. руб.

Наиболее существенные риски (2)

- Риск **блокировки сайта** компании.
- Риск **отзыва лицензии**.
- Риск **дисквалификации** должностного лица.
- Риск **уголовной ответственности** для должностных лиц.
- Риск **вреда репутации** компании и должностных лиц.
- Особая зона рисков – **риски нарушения европейских правил (GDPR)**: большие штрафы, сжатые сроки, сложный compliance, нестыковки с российскими правилами.

Case study: «Группа компаний vs локализация»

1. Российское ООО входит в международную группу компаний.

2. Российское ООО в процессе деятельности собирает данные граждан РФ:

- ФИО.
- Адрес места жительства.
- Паспортные данные.
- ИНН.
- E-mail.
- Номер телефона.
- Семейное положение и состав семьи.
- Информация о банковских счетах.
- Сведения о доходах, имущественном положении и др.

3. Данные граждан РФ первоначально сохраняются в базе данных, находящейся:

- **В глобальной базе данных группы компаний, расположенной за границей (Workday и др.).**
- **В РФ (1С и др.).**
- **Одновременно сохраняются в базах данных, расположенных и в РФ, и за границей.**

Как урегулировать риски

1. Провести **аудит процессов и документов** по обработке персональных данных (обязательно привлечение специалистов – юристов и специалистов по информационной безопасности).
2. Выводы и план действий **предоставить комитету по рискам и комитету по аудиту**.
3. Утвержденный **план действий реализовать**. Назначить ответственных лиц.
4. Для уменьшения рисков единоличного исполнительного органа необходимо **делегировать полномочия и ответственность** за определенные направления соответствующим работникам компании.

Контрольные блоки

- ✓ Пакет документов по обработке персональных данных.
- ✓ Лицо, ответственное за организацию обработки персональных данных.
- ✓ Лицо, ответственное за обеспечение безопасности персональных данных.
- ✓ Меры по обеспечению безопасности персональных данных.
- ✓ Доступ к политике по обработке персональных данных.
- ✓ Уведомление Роскомнадзора.
- ✓ Ознакомление работников с локальными актами.
- ✓ Обучение работников.
- ✓ Система контроля.

Перечень документов

- ✓ Политика в отношении обработки персональных данных.
- ✓ Политика в отношении файлов cookies (если применимо).
- ✓ Форма согласия на обработку персональных данных работников/соискателей/членов семей работников/контрагентов и т.п.
- ✓ Форма согласия на обработку персональных данных, разрешенных субъектом для распространения.
- ✓ Форма договора поручения на обработку персональных данных.
- ✓ Приказ о назначении ответственного за организацию обработки персональных данных.
- ✓ Перечень мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации/ при их автоматической обработке.
- ✓ Приказ об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных.
- ✓ Приказ об утверждении перечня работников, имеющих доступ к персональным данным.
- ✓ Приказ о создании комиссии по уничтожению персональных данных.
- ✓ Форма акта об уничтожении персональных данных.
- ✓ Приказ об утверждении мест хранения материальных носителей персональных данных.
- ✓ Журнал ознакомления работников с документами, устанавливающими порядок обработки данных.
- ✓ Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных.
- ✓ Форма обязательства о неразглашении персональных данных и др.

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 слияний и поглощений и корпоративного права в Санкт-Петербурге
elena_agaeva@epam.ru