

Судебная практика по утечкам персональных данных и правовые риски при взаимодействии с обработчиками персональных данных



Управляющий партнер юридической фирмы Lukash & Partners,
профессиональный DPO и юрист в области информационного права

19 лет опыта

Совокупный опыт работы в ИТ-праве, телеком и медиа - праве, защите персональных данных

100+ компаний

Решено большое количество задач для корпораций и среднего бизнеса

36 стран

Опыт ведения проектов по законодательству России, СНГ, ЕС, MENA, APAC

3-х сторонний взгляд

Опыт работы со стороны Роскомнадзора, внутри компании и консультанта

2 образования

Высшее юридическое и высшее техническое образование

Автор курса

Авторский курс по легализации обработки персональных данных

Статья 21 152-ФЗ

3.1. 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:

1. в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
2. в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Приказ Роскомнадзора от 14.11.2022 № 187

«Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»

Часть 12 статья 19 152-ФЗ

Оператор обязан в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая **информирование его о компьютерных инцидентах, повлекших неправомерную передачу** (предоставление, распространение, доступ) персональных данных.

Приказ ФСБ от 13.02.2023 № 77

Приказ Федеральной службы безопасности Российской Федерации от 13.02.2023 № 77 "Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных"

Минимальный штраф по результатам «утечки» ПД

30 000

рублей

Штрафы за неправомерную или случайную передачу

Конкретно за «утечку» штрафов нет, штрафуют за нарушение законодательства, связанное с неправомерной или случайной передачей

Штрафуют:

1. По ч. 1 ст. 13.11 КоАП РФ: нарушения ч. 1 ст. 18.1 152-ФЗ
2. По ч. 2 ст. 13.11 КоАП РФ: нарушение ст. 10.1 152-ФЗ

И даже по ч. 3 ст. 13.11 КоАП РФ (по представлению прокуратуры, дело [№ 5-348/4/2023](#))

Основной метод доказывания:

1. признание оператора персональных данных,
2. информация из уведомления о неправомерной или случайной передаче,
3. собранные сведения во время внеплановой проверки.

Организация защиты по 21-му приказу ФСТЭК РФ не имела значения в судах

Уникальный идентификатор дела 77MS0347-01-2023-001607-77

Номер дела 05-0450/347/2023

внеплановая выездная проверка в отношении Оператора.

В ходе внеплановой выездной проверки было установлено, что Оператором допущено нарушение требований части 1 статьи 6, статьи 7, статьи 10.1, части 4 статьи 9 Закона, статьи 88 Трудового кодекса Российской Федерации в части предоставления неправомерного доступа к ИСПДн «Microsoft Active Directory», повлекшего за собой распространение персональных данных работников Оператора неограниченному кругу лиц путем размещения в сети Интернет по адресам: <https://t.me/niceleakbro/39>, <https://ofile.io/d/8mRvU1i>

ПОСТАНОВИЛ:

 признать виновным в совершении административного правонарушения, предусмотренного ч. 2 ст. 13.11 Кодекса РФ об административных правонарушениях и назначить наказание в виде административного штрафа в размере 30 000 (тридцать тысяч) рублей.

Какие планируются штрафы по ст. 13.11 для юрлиц

Не уведомление об обработке ПД
до 300 тыс. рублей.

Не уведомление об утечке ПД,
до 3 млн. рублей.

В зависимости от объема утекших персональных данных (начиная от 1000):

3-5 млн. рублей

5-10 млн. рублей

10-15 млн. рублей

«Утечка» спецкатегорий или биометрических ПД
15-20 млн.

Повторная «утечка»

0,1-3% выручки, но не менее 15 млн. и не более 500 млн., для спецкатегорий не менее 20 млн. руб.

ИП == Юрлица

+ административные расследования по утечкам

Оператор в ответе за Обработчика

Обработчик* – это оператор персональных данных, который не имеет собственных законных заранее определенных целей перед субъектом персональных данных. Действует по поручению (реального) оператора ПД на обработку.

Примеры обработчиков: [внешняя бухгалтерия](#), [провайдер хостинга](#), [SaaS сервис](#).

* Лицо, осуществляющее обработку персональных данных по поручению оператора

Оператор в ответе за Обработчика

Обработчик* – это оператор персональных данных, который не имеет собственных законных заранее определенных целей перед субъектом персональных данных. Действует по поручению (реального) оператора ПД на обработку.

Примеры обработчиков: внешняя бухгалтерия, провайдер хостинга, SaaS сервис.

ч. 3 и ч. 5 ст. 6 152-ФЗ

предусматривают ответственность Оператора ПД за действия Обработчика.

взамен

оператору ПД даются гражданско-правовые механизмы контроля Обработчика

* Лицо, осуществляющее обработку персональных данных по поручению оператора

Если Оператора оштрафуют за действия Обработчика, возможно ли взыскание убытков с Обработчика?

ч. 10. ст. 12.21.1 КоАП РФ (как пример из судебной практики)

Постановление Арбитражного суда Поволжского округа от 6 июля 2017 г. № Ф06-22228/2017 по делу № А65-19461/16

Компания обратилась в суд с иском о взыскании убытков в связи со штрафом по [ч. 10. ст. 12.21.1 КоАП РФ](#). Была договорная оговорка о компенсации штрафов.

В ходе судебного заседания Общество предъявило к Компании встречный иск о признании недействительным пункт дополнительного соглашения к договору о возмещении сумм административных штрафов по [ч. 10. ст. 12.21.1 КоАП РФ](#). В обоснование требований Общество указало на ничтожность данного пункта в силу [ст. 168-169 ГК РФ](#), так как по мнению Общества данный пункт противоречит основам российского правопорядка, ибо перекладывает административную ответственность на другое лицо, что не допускается действующим законодательством, при этом позволяя Компании беспрепятственно нарушать действующее законодательство, полагая, что ответственность в этом случае будет возложена на контрагента.

Установив, что Покупатель, несмотря на согласование условия о самовывозе не учитывал необходимую грузоподъемность транспортного средства, чем нарушил требования законодательства и условия договора, суды, с ссылками на [ст. 309-310, ст. 393, ст. 15 ГК РФ, п. 12 постановления Пленума Верховного Суда Российской Федерации от 23 июня 2015 г. № 25](#), удовлетворили первоначальные требования в полном объеме.

Договорная оговорка помогла, но это не гарантия

Статья 406.1. Возмещение потерь, возникших в случае наступления определенных в договоре обстоятельств

1. Стороны обязательства, действуя при осуществлении ими предпринимательской деятельности, могут своим [соглашением](#) предусмотреть обязанность одной стороны возместить имущественные потери другой стороны, возникшие в случае наступления определенных в таком соглашении обстоятельств и не связанные с нарушением обязательства его стороной (потери, вызванные невозможностью исполнения обязательства, предъявлением требований третьими лицами или органами государственной власти к стороне или к третьему лицу, указанному в соглашении, и т.п.). Соглашением сторон должен быть определен размер возмещения таких потерь или порядок его определения.

Для удовлетворения требований истца о возмещении имущественных потерь на основании [ст. 406.1 ГК РФ](#) указанное условие должно быть сформулировано в договоре явно и недвусмысленно. В случае **неясности** того, что устанавливает соглашение сторон – **возмещение потерь или условия ответственности за неисполнение обязательства**, положения [ст. 406.1 ГК РФ](#) **не подлежат применению** (п. 17 Постановления [Пленума](#) Верховного Суда РФ от 24 марта 2016 г. № 7 "О применении судами некоторых положений Гражданского кодекса РФ об ответственности за нарушение обязательств").

1. Заключение поручения, опросники, отнестись серьезно

*«... обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, **предоставлять документы и иную информацию**, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей ..»*

Опросник = ГК РФ Статья 431.2. Заверения об обстоятельствах

2. Подробнее и реалистично оговорить взаимодействие по утечкам
3. Оговорить высокую конфиденциальность на случай взаимодействия по утечке

1. Штрафуют за невыполнение требований 152-ФЗ, а не «утечку»
2. Основной метод доказывания – это признание оператора
3. Внеплановая проверка по утечке тоже связана с признанием
4. Защита персональных данных по требованиям ФСТЭК/ФСБ не исключает и не смягчает наказание за утечку
5. Следует больше внимания уделять Обработчикам
6. Своевременное уведомление об «утечке» может быть смягчающим обстоятельством



СПАСИБО

Денис Лукаш

telegram: @linfo

denis@lukash.info

+79265900373