

Особенности соблюдения закона о персональных данных провайдерами ХОСТИНГА



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

19 лет опыта

Совокупный опыт работы в IT-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

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Хэширование

Китайгородский проезд, д. 7, стр. 2, Москва, 109992
тел./факс: (495) 983-33-93; <http://rkn.gov.ru/>

01.06.2023 № 08-45913

На

О результатах рассмотрения обращения

Роскомнадзор по результатам рассмотрения Вашего обращения от 17.05.2023 № 02-11-15258 сообщает следующее.

Хеш-функция является в соответствии с «ГОСТ Р 34.11-2012. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.» средством криптографической защиты информации, а не способом обезличивания персональных данных. В связи с чем, преобразованные данные с помощью хеш-функции, являются персональными данными, на которые в полной мере распространяются порядок и условия их обработки, установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Начальник Управления по защите
прав субъектов персональных данных

Ю.Е. Контемиров

Хэшированные данные тоже
персональные

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

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 \(B2B\)](#), [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.

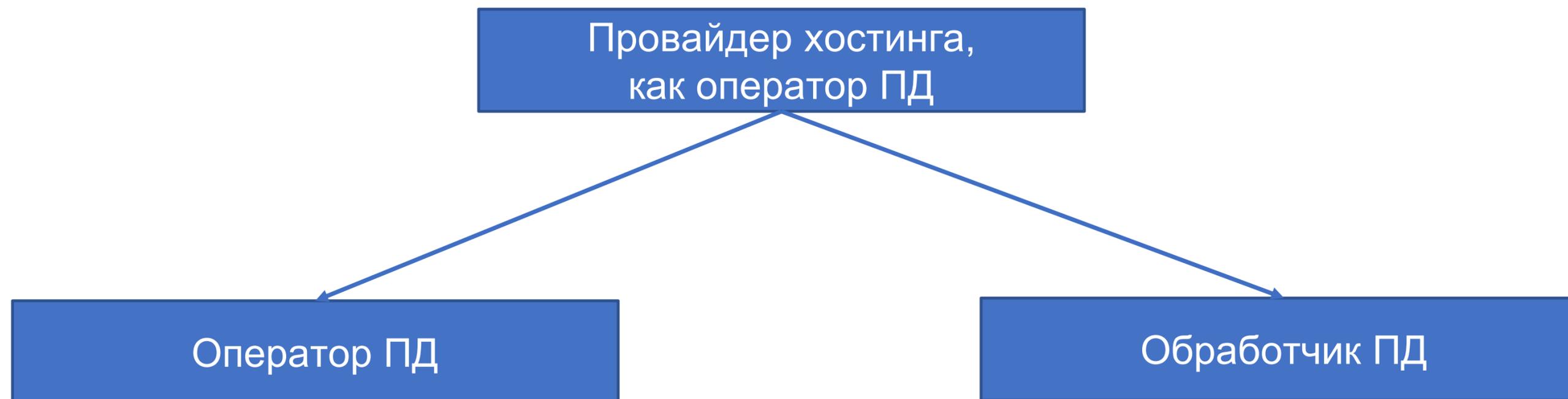
ч. 3 и ч. 5 ст. 6 152-ФЗ

предусматривают ответственность Оператора ПД за действия Обработчика.

взамен

оператору ПД даются гражданско-правовые механизмы контроля Обработчика

* Лицо, осуществляющее обработку персональных данных по поручению оператора



В отношении клиентов – Физлиц
В отношении представителей клиентов

В отношении конечных пользователей клиентов

Для полноты: еще есть

Совместные операторы

Последующие обработчики

Поручение обработки персональных данных

ч. 3 ст. 6 152-ФЗ

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом. **В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные [частью 5 статьи 18](#) и [статьей 18.1](#) настоящего Федерального закона, 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, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со [статьей 19](#) настоящего Федерального закона, в том числе требование об уведомлении оператора о случаях, предусмотренных [частью 3.1 статьи 21](#) настоящего Федерального закона.**

Вопрос:

Как Хостинг-провайдер может узнать перечень ПД?

Статья 3 152-ФЗ

3) **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, **хранение**, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Риск не заключения поручения обработки на операторе ПД

- Что делают обработчики
 1. По умолчанию могут не давать поручение обработки
 2. Могут давать урезанный вариант поручения обработки
 3. Не заключать договор с требующим поручение обработки по различным причинам

- Оператор ПД – клиент не несет сильную административную ответственность, в основном это гражданско-правовые риски Оператора ПД

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").

Клиенты-операторы ПД

*«... 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 ..»*

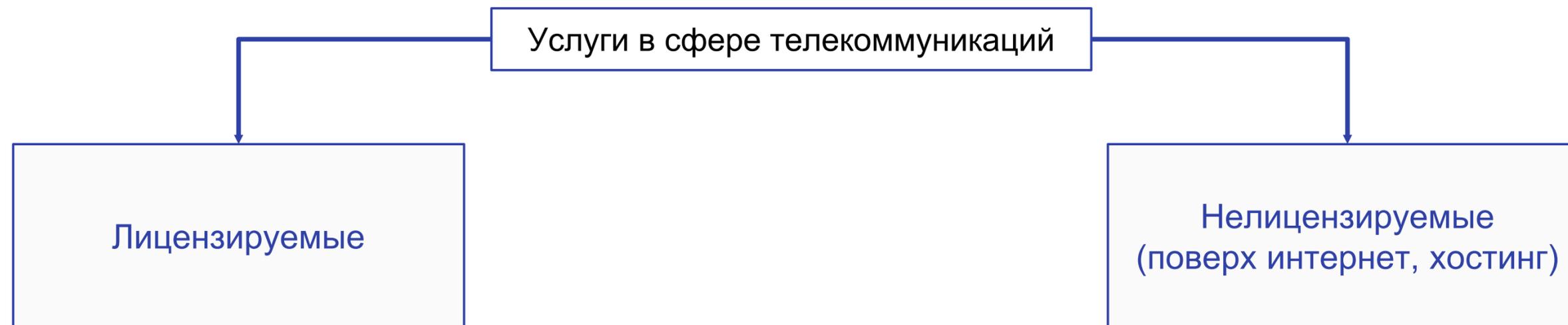
Опросник = ГК РФ Статья 431.2. Заверения об обстоятельствах

Провайдеру хостинга нужно отнестись серьезно к опроснику

Предлагаю темы для разговора в контексте услуг хостинга:

1. Уведомление в Роскомнадзор
2. Действия при утечках
3. Удаление персональных данных
4. Больше про трансграничную передачу
5. Что такое персональные данные
6. Организация работы службы DPO
7. Типовые документы по ПД
8. Проверки РКН по ПД
9. Frontend-комплаенс

Проблемы в сфере персональных данных в Телеком



Лучше работают типовые решения по ЛНА в области ПД

- Консервативность услуг, основанная на регулировании
- Преобладающие основания обработки персональных данных:

Закон → Договор
- Преимущественно передача без поручения обработки B2B

Сложно легализовать типовыми ЛНА без потери конкурентных преимуществ

- Выше предпринимательское усмотрение
- Преобладающие основания обработки персональных данных:

Договор & Согласие
- Преимущественно передача с поручением обработки в B2B

Проектный комплаенс может закрыть большинство проблем

Нужен профессиональный Ответственный за организацию обработки ПД на постоянной поддержке

- Риск - менеджмент в области ПД
- Presale DPO (для B2B)

Если нет штатного DPO, лучше нанять внешнего консультанта - DPO для стратегических решений.

Юрист или ИБ-специалист может выполнять повседневную работу по созданной DPO стратегии.

Больше информации по почте denis@lukash.info



СПАСИБО

Денис Лукаш

telegram: @linfo

denis@lukash.info

+79265900373