ADVANT Beiten

Информационное письмо

Декабрь 2024

Беспрецедентное ужесточение ответственности за утечки персональных данных

English version

30 ноября 2024 года подписан закон об усилении **административной** ответственности за утечки[1] персональных данных (№ 420-ФЗ) ("**Закон**"). Закон вступает в силу **30 мая 2025 года**.

Также **11 декабря 2024** года вступает в силу новая статья 272.1 **Уголовного кодекса** РФ, которая устанавливает ответственность за незаконные использование и/или передачу, сбор и/или хранение компьютерной информации, содержащей персональные данные.

ОСНОВНЫЕ ПАРАМЕТРЫ НАСТУПЛЕНИЯ НОВОЙ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ ЗА УТЕЧКИ:

- не только в случае, когда персональные данные стали **неправомерно общедоступными**, но и когда они **неправомерно переданы ограниченному кругу лиц**;

- только за действия (бездействие) оператора персональных данных, повлекшие **неправомерную** передачу персональных данных. Таким образом, ответственность за случайную передачу не установлена. Однако иногда сложно установить, является ли передача неправомерной или случайной. Например, когда по ошибке данные направлены на другой адрес электронной почты, чем предполагалось;

- штрафы **дифференцируются** в зависимости от **количества** "утекших" данных и того, какие **категории** данных были неправомерно переданы, а также от наличия **ранее наложенных** штрафов;

- генеральные директора и иные должностные лица частных компанией к административной ответственности за утечки персональных данных, по общему правилу, **не привлекаются** (но см. примечание *** в таблице ниже);

- конкретные размеры штрафов для компаний в зависимости от обстоятельств и соответствующие пояснения указаны в таблице ниже:

<table>
<tr><th></th><th>Безотносительно количества субъектов или идентификаторов**</th><th>1.000-10.000 субъектов и/или 10.000-100.000 идентифи-каторов</th><th>10.000-100.000 субъектов, 100.000-1.000.000 идентифи-каторов</th><th>>100.000 субъектов, >1.000.000 идентификаторов</th></tr>
<tr><td rowspan="2">"Обычные" персональные данные</td><td>Первично: 150-300 тыс. руб.***</td><td>(1) 3-5 млн. руб.</td><td>(1) 5-10 млн. руб.</td><td>(1) 10-15 млн. руб.</td></tr>
<tr><td>Повторно: 300-500 тыс. руб.***</td><td>(2) 1-3% годовой выручки (но не <20 и не >500 млн. руб.)</td><td>(2) 1-3% годовой выручки (но не <20 и не >500 млн. руб.)</td><td>(2) 1-3% годовой выручки (но не <20 и не >500 млн. руб.)</td></tr>
<tr><td rowspan="2">Специальные категории персональных</td><td>(1) 10-15 млн. руб.</td><td colspan="3" rowspan="2">* Согласно позиции Роскомнадзора биометрическими данные являются только в том случае, если конкретные данные</td></tr>
<tr><td></td></tr>
</table>

данных (включая данные о здоровье)	(2)**** 1-3% годовой выручки***** (но не <25 и не >500 млн. руб.)	прямо названы в качестве биометрических в нормативном правовом акте. ** *Идентификатор* – это уникальное обозначение сведений о человеке в информационной системе (может содержаться, например, в логах системы). *** Также возможен штраф на *должностных лиц* в размере от 50 до 100 тыс. руб. (первичное нарушение) и от 100 до 200 тыс. руб. (повторное нарушение). **** Здесь и далее (2) означает совершение административного правонарушения лицом, *подвергнутым* административному наказанию за утечку (то есть, по общему правилу, совершение нарушения в период со дня вступления в законную силу предыдущего постановления о назначении административного наказания до истечения *1 года* со дня окончания исполнения данного постановления). ***** Здесь и далее в случае *кредитной организации* – 1-3 % размера собственных средств.
Биометрические персональные данные*	(1) 15-20 млн. руб.	
	(2) 1-3% годовой выручки (но не <25 и не >500 млн. руб.)	

ОБЯЗАТЕЛЬНЫЕ МЕРЫ ДЛЯ СНИЖЕНИЯ ОТВЕТСТВЕННОСТИ

При этом установлено 3 условия, при одновременном соблюдении которых оборотный штраф уменьшается до 0.1 % (но не <15 и не >50 млн. руб.) (исполнить эти условия нужно до вынесения судом постановления):

1) **Траты** на проведенные лицензированными[2] компаниями мероприятия по обеспечению **информационной безопасности** в течение 3 календарных лет до выявления нарушения составляли у оператора ежегодно не менее **0.1 % годовой выручки**.

2) Наличествует документально подтвержденное соблюдение компанией требований к защите персональных данных при их обработке в информационных системах. Такие требования установлены, в частности, в Постановлении Правительства РФ от

01.11.2012 г. № 1119 и включают минимально такие меры как а) организация **режима обеспечения безопасности помещений**, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения; б) обеспечение **сохранности носителей** персональных данных; в) утверждение руководителем оператора документа, определяющего **перечень лиц**, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей; г) использование **средств защиты информации**, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. Документом, подтверждающим соблюдение требований, может быть **отчет об аудите**, который с учетом Закона следует проводить **не реже чем каждые 12 месяцев**.

3) Отсутствуют такие **отягчающие обстоятельства** как (а) продолжение противоправного поведения, несмотря на требование уполномоченных лиц прекратить его, или (б) ранее наложенные[3] на компанию штрафы за нарушение законодательства РФ в области персональных данных или правил защиты информации (включая штрафы за неуведомление Роскомнадзора об обработке персональных данных).

При наложении оборотных штрафов отягчающим обстоятельством будет, среди прочего, также административное правонарушение в виде неуведомления Роскомнадзора об утечке (первичное уведомление должно быть направлено в Роскомнадзор в электронной форме в течение 24 часов с момента выявления инцидента). Также само по себе неуведомление об утечке будет теперь являться отдельным составом административного правонарушения – штраф за это установлен для компании в размере не менее 1 млн. руб.

РЕКОМЕНДАЦИИ

В свете вышеуказанного компаниям-операторам персональных данных (включая иностранные компании, осуществляющие деятельность в России, в том числе, через Интернет) в **ближайшие полгода** рекомендуется предпринять, среди прочего, следующие действия:

1) Российским компаниям или представительствам/филиалам иностранных компаний направить, если еще не направили, **уведомление** об обработке персональных данных в Роскомнадзор. Закон также устанавливает штрафы за **невыполнение** оператором

обязанности по направлению уведомления в размере до 300 тыс. руб. на компанию.

2) Провести обязательный **аудит** в сфере персональных данных для выявления и устранения возможных несоответствий.

3) Провести обязательный **тренинг** по защите персональных данных для работников, поскольку человеческий фактор остается одной из основных причин утечек.

4) Подписать **поручения** на обработку персональных данных по установленной Законом о персональных данных форме, в первую очередь, со всеми облачными и иными провайдерами, которым поручается обработка значительных объемов или чувствительных категорий персональных данных.

5) Выдать **доверенности** уполномоченным представителям для взаимодействия с Роскомнадзором и судами на случай утечки.

Мы будем рады оказать Вам содействие в проведении аудитов, тренингов и подготовке необходимых документов.

[1] Согласно российскому Закону о персональных данных утечки персональных данных – это неправомерная или случайная передача (предоставление, распространение, доступ) персональных данных, повлекшая нарушение прав субъектов персональных данных.

[2] Лицензия на разработку, производство, распространение шифровальных (криптографических) средств или на деятельность по технической защите конфиденциальной информации должна быть у подрядчика или у самого оператора персональных данных.

[3] Когда на момент совершения правонарушения (на момент вынесения судом постановления) лицо считается подвергнутым административному наказанию (см. примечание **** в таблице выше).

С уважением,

Андрей Слепов
Партнер
Andrey.Slepov@advant-beiten.com

Подписаться на информационные письма
Переслать E-Mail

Примечания

Настоящая публикация не является юридической консультацией.

Если Вы в дальнейшем не хотите получать информацию от нас, Вы можете в любое время отказаться от рассылки.

© БАЙТЕН БУРКХАРДТ
Рехтсанвальтсгезельшафт мбХ
Все права защищены 2024

Выходные данные

ADVANT BEITEN
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
(Издатель)
Ganghoferstraße 33, 80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811
Подробная информация (контакты) по ссылке:
https://www.advant-beiten.com/en/imprint

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH является членом ADVANT, объединения независимых юридических фирм. Каждая фирма-член является отдельным и независимым юридическим лицом, которое несет ответственность только за свои собственные действия и бездействие.