

Основные подходы
правоприменительной
практики в сфере защиты
данных и позиции
Роскомнадзора:
практические советы

alrud.com

АЛРУД

Введение

Уважаемые дамы и господа,

В последние годы Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций («**Роскомнадзор**»), а также судами было выработано множество позиций и подходов, которые операторам необходимо учитывать в своей деятельности. Ниже Вашему вниманию представлены некоторые практические рекомендации, подготовленные с учетом названных позиций и подходов, а также практического опыта наших юристов. Данный обзор не является юридической консультацией. Однако мы считаем, что он может служить в качестве общего практического руководства для компаний, желающих обеспечить соблюдение российского законодательства о защите персональных данных и учесть практические аспекты его применения.

1. Большинство компаний обязаны уведомлять Роскомнадзор об обработке персональных данных

В соответствии с Федеральным законом «О персональных данных» операторы персональных данных обязаны уведомлять Роскомнадзор о намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных законом. Как правило, операторы не направляют такие уведомления, полагаясь на такое исключение, как обработка персональных данных, осуществляемая в соответствии с трудовым законодательством.

Позиция Роскомнадзора: Указанное исключение не применяется, если компания обрабатывает персональные данные бывших работников (например, хранит эти данные) или соискателей на вакантные должности.

Позиция Роскомнадзора касательно представления информации о нахождении в России баз данных: Компании, направившие уведомления в Роскомнадзор ранее 1 сентября 2015 года, должны подать уточненные сведения о нахождении баз данных, используемых для обработки персональных данных, на территории России в течение 10 дней, начиная с 1 сентября 2015 года. Компании, не направившие своевременно уточненные данные, должны сделать это в кратчайший срок.

2. Третьи лица, которым передаются персональные данные работников, должны быть исчерпывающим образом указаны в согласии на передачу персональных данных

В случае передачи персональных данных работников третьим лицам, если такая передача не предусмотрена законом, необходимо получить письменное согласие. Законодательство о персональных данных устанавливает требования как к форме, так и к содержанию соответствующего согласия. В частности, требуется указать наименования и адреса третьих лиц, которым передаются данные.

Однако ввиду определенных сложностей (например, большого количества получателей этой информации, частого изменения их состава и, как следствие, необходимости переподписания форм согласий) операторы указывают лишь категории третьих лиц (например, аффилированные лица, провайдеры услуг и т.д.), не обозначая при этом их конкретные наименования и адреса.

Позиция Роскомнадзора: Любое третье лицо, которому передаются персональные данные работников, должно быть прямо поименовано в форме согласия путем указания его наименования и адреса.

3. Специфика неавтоматизированной обработки персональных данных должна быть урегулирована в соответствующем внутреннем акте компании

Как правило, обработка данных предполагает использование средств автоматизации (например, электронных устройств). Однако многие компании осуществляют также неавтоматизированную обработку, например, путем обработки бумажных анкет потенциальных клиентов или заявлений, заполняемых работниками. Необходимо иметь в виду, что в отношении такого типа обработки персональных данных законодательством установлен ряд специальных требований.

Позиция Роскомнадзора: Компании обязаны утвердить детальные внутренние правила относительно специфики неавтоматизированной обработки персональных данных, а также оформить иные документы, требуемые для осуществления такой обработки в соответствии с законодательством.

4. Резюме не принятых на работу соискателей на вакантные должности не могут храниться более 30 календарных дней без согласия субъекта данных

Как правило, компании хранят информацию о соискателях, которые не были приняты на работу (например, для целей формирования кадрового резерва).

Позиция Роскомнадзора: Как только компания отклонила кандидатуру соискателя, цели, для которых персональные данные этого соискателя обрабатывались, были достигнуты, такие персональные данные подлежат уничтожению или обезличиванию в течение 30 календарных дней в соответствии с законодательством о персональных данных, если иное не предусмотрено согласием субъекта персональных данных.

Кроме того, Роскомнадзор обращает внимание на наличие политики о кадровом резерве.

Позиция Московского городского суда по делу N 33а-3957 от 4 июня 2018 г. (дело компании «Макдоналдс»): нарушением законодательства о персональных данных было признано хранение в составе личного дела работника резюме и согласия на обработку персональных данных кандидата.

5. Обработка персональных данных родственников работников в объеме, превышающем установленные трудовым законодательством пределы, допускается только при наличии согласий, полученных напрямую от этих лиц

В соответствии с трудовым законодательством при несчастном случае на производстве работодатель обязан сообщить об этом родственникам работника. В связи с этим работодатель может законно осуществлять обработку контактной информации

родственников работника. Однако в действительности работодатели обрабатывают более широкий круг информации, касающейся родственников работников (например, информацию о профессии, наличии/отсутствии у них судимости и т.д.). Обработку этой информации невозможно обосновать необходимостью выполнения требований Трудового кодекса.

Позиция Роскомнадзора: Если работодатель обрабатывает данные о родственниках работника в объеме, превышающем объем данных, необходимый для выполнения установленных законодательством обязанностей, то необходимо получать согласия напрямую от родственников работников.

6. В случае если используемая в компании система доступа в помещения основана на идентификации работника по фотографии, компания обязана получить письменное согласие на обработку биометрических данных

Многие компании используют электронные системы доступа, предполагающие идентификацию работников по их изображению на фотографии (путем сравнения фотографии, отображающейся на компьютере после использования электронного пропуска с лицом, использовавшим этот пропуск).

Позиция Роскомнадзора: При данных обстоятельствах фотография является биометрическими персональными данными. В связи с этим работодатель обязан получить письменные согласия работников, соответствующие по своей форме и содержанию законодательным требованиям.

Позиция Верховного Суда: Фотографические изображения являются биометрическими персональными данными, поскольку характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность. Предписание по эпизоду, связанному с нарушением порядка обработки биометрических персональных данных, признано соответствующим действующему законодательству и не нарушающим права и законные интересы предприятия.

7. Обработка персональных данных бывшего работника должна основываться на согласии

Многие компании продолжают обработку данных своих бывших работников в информационных системах за пределами установленного законодательством срока хранения таких данных.

Позиция Роскомнадзора: Обработка персональных данных бывших работников в случаях, не предусмотренных законодательством, должна осуществляться с согласия субъектов данных. Также специфика правовых оснований для обработки таких данных, особые сроки их хранения и порядок обработки должны регулироваться локальными нормативными актами компании.

Позиция Московского городского суда по делу N 33а-3957 от 4 июня 2018 г. (дело компании «Макдоналдс»): нарушением законодательства о персональных данных было признано отсутствие внутренних локальных актов, регламентирующих обработку персональных данных при включении непринятых кандидатов на работу и уволенных работников в кадровый резерв, а также отсутствие отдельных письменных согласий субъектов персональных данных на включение информации о них в кадровый резерв.

8. Компанией должны быть установлены правила уничтожения персональных данных

На практике компании используют shreddеры и другие подобные механические средства уничтожения документов. Однако детальное руководство, регламентирующее порядок уничтожения различных видов персональных данных (включая информацию, хранящуюся в электронных информационных системах), как правило, отсутствует.

Позиция Роскомнадзора: Необходимо наличие внутренних правил, утверждающих порядок уничтожения персональных данных в зависимости от их вида и способа обработки, а также специальных актов, удостоверяющих факт уничтожения.

9. Согласие субъекта персональных данных должно быть ограничено одной целью

Компании зачастую указывают в письменном согласии на обработку персональных данных несколько целей такой обработки.

Позиция Роскомнадзора и судов: Согласно п. 4 ч. 4 ст. 9 Федерального закона «О персональных данных» письменное согласие должно включать в себя «цель обработки персональных данных». Следовательно, если оператор обрабатывает персональные данные одного субъекта в нескольких целях, и такая обработка требует письменного согласия, необходимо запрашивать отдельное согласие субъекта для каждой цели обработки.

10. Обработка данных из социальных сетей должна быть совместима с целями сбора такой информации

Многие компании обрабатывают персональные данные из социальных сетей, ссылаясь на их общедоступный характер. Однако такая обработка в отрыве от целей первоначального сбора данных рассматривается как нарушение законодательства о персональных данных.

Позиция Роскомнадзора и судов: законодательство о персональных данных не признает общедоступными данные, размещенные пользователями в социальных сетях.. Такие данные обрабатываются на основе пользовательского соглашения между субъектом данных и социальной сетью.

11. Хотя телефонный номер сам по себе не относится к персональным данным, законодательство о рекламе ограничивает использование телефонных номеров

В некоторых случаях компании обрабатывают исключительно номера телефонов клиентов и контрагентов.

Позиция Роскомнадзора: номер телефона без дополнительной информации о субъекте данных относится к устройству, а не к субъекту данных, и его использование без дополнительной

информации о субъекте не является обработкой персональных данных.

Позиция ФАС: не допускается распространение рекламы по сетям электросвязи, включая телефонную связь, в отсутствие предварительного согласия абонента на получение рекламных сообщений. Нарушение данного требования может повлечь наложение административного штрафа в размере до 500 тысяч рублей.

12. Информация, содержащаяся в файлах cookie и других аналитических данных, является персональными данными

Многие компании автоматически собирают аналитические данные (файлы cookie, MAC адрес, IP-адрес). В некоторых случаях они полагают, что такая информация не позволяет идентифицировать лицо и, следовательно, не подпадает под действие законодательства об обработке персональных данных.

Позиция Роскомнадзора и судов: автоматически собираемые данные (файлы cookie, MAC адрес, IP-адрес) являются персональными данными. При обработке таких данных необходимо соблюдать законодательство о персональных данных.

Позиция Таганского районного суда города Москвы по делу № 2-4261/18 от 19 декабря 2018 года (дело по веб-сайту <https://2019.vote/>): использование сервисов Google Analytics и Яндекс Метрика является действиями по сбору и обработке персональных данных. Информация об их использовании должна быть отражена в политике конфиденциальности оператора.

13. Обработка обезличенных персональных данных должна соответствовать требованиям законодательства о персональных данных

Многие компании обезличивают персональные данные в целях вывода таких данных из-под действия законодательства о персональных данных и их дальнейшей коммерциализации.

Позиция Роскомнадзора и судов: обработка обезличенных персональных данных позволяет

косвенно определить субъекта персональных данных. Обезличенные персональные данные не перестают быть персональными, и их обработка должна осуществляться в соответствии с законом.

14. Письменная форма согласия считается соблюденной при использовании простой электронной цифровой подписи

Позиция Роскомнадзора: Согласно позиции представителей Роскомнадзора, озвученной в ходе публичных мероприятий в 2018 – 2019 гг., письменная форма согласия на обработку персональных данных считается соблюденной при использовании простой электронной подписи. При этом необходимо предварительно заключить соглашение об использовании простой электронной подписи.

Помимо упомянутых выше подходов Роскомнадзора, мы хотели бы также обратить Ваше внимание на следующие рекомендации:

- В ходе проверки от компании потребуются доказать, что процедуры по обработке данных (например, сроки хранения, процедура обезличивания, их уничтожение и т.д.), установленные в соответствующих внутренних документах, фактически применяются на практике.
- Если компания направила уведомление об обработке персональных данных, в ходе проверки Роскомнадзор проверит соответствие информации, указанной в уведомлении, фактическим процессам по обработке данных. Недопустимо указание в уведомлении всей информации, содержащейся в законе, в отрыве от фактической деятельности компании.
- Роскомнадзор будет полагаться на информацию, указанную во внутренних документах компании по обработке данных, даже в том случае, если компания фактически не осуществляет те или иные действия, указанные в таких документах. Например, если на веб-сайте компании указано, что данные могут быть переданы в США, Роскомнадзор будет исходить из того, что это реальный процесс по обработке персональных данных,

и, следовательно, может поставить соответствующие вопросы относительно наличия законных оснований для такой передачи.

- Такую информацию, как IP-адреса, информацию, полученную посредством cookies и т.д. Роскомнадзор относит к персональным данным (даже если компания не обрабатывает какую-либо иную дополнительную информацию в отношении физических лиц). В связи с этим, если в размещенной на сайте политике о конфиденциальности есть положения об обезличенном характере данной информации,

они должны быть изменены. При разработке внутренней документации по вопросам обработки данных, посетителей веб-сайта компании необходимо рассматривать в качестве субъектов, чьи персональные данные обрабатываются компанией. Это также относится и к тем посетителям, которые не имеют персональных аккаунтов на веб-сайте и не предоставляют свои имена и адреса электронной почты, поскольку компании в любом случае получают их IP адреса.

Ключевые контакты




Мария Остащенко

Партнер

Коммерческое право, Интеллектуальная собственность,
Защита данных и кибербезопасность

E: mostashenko@alrud.com



Обращаем Ваше Внимание на то, что данная брошюра была составлена на основе информации, полученной из открытых источников.
Юридическая фирма АЛРУД и авторы данной брошюры не несут ответственность за последствия, возникшие в результате принятия решений на основе данной информации.

Юридическая фирма АЛРУД
ул. Скаковая, д. 17, стр. 2, 6 эт.
Москва, Россия, 125040

T: +7 495 234 96 92
+7 495 926 16 48
E: info@alrud.com
alrud.com



АЛРУД