alrud.com

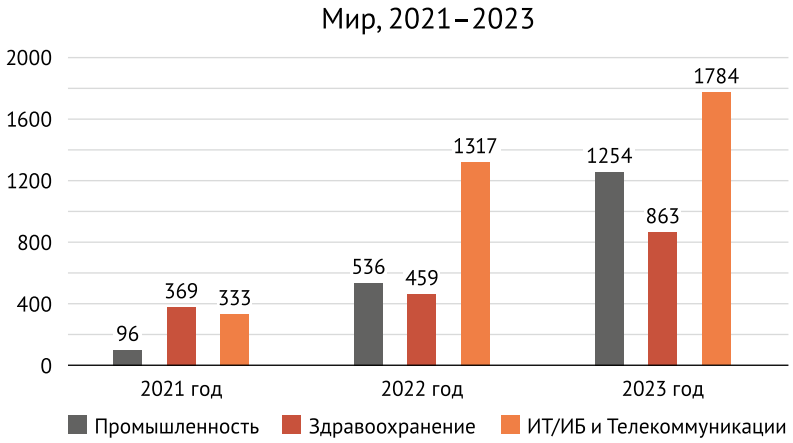
Защита данных: что нужно знать операторам в 2024 году?

АЛРУД

Уважаемые читатели,

Согласно отчёту Международной ассоциации защиты данных (IAPP)[1], в последние годы фиксируется существенное увеличение количества запросов в области персональных данных в сети Интернет, а команды юристов, занимающихся вопросами защиты персональных данных, растут.

31 мая 2024 года компания Infowatch опубликовала «Исследование утечек информации в отраслях за три года»[2]. Согласно данному исследованию, количество утечек в мире значительно и стабильно растет в таких ключевых отраслях, как здравоохранение, ИТ и телекоммуникации, промышленность. Вы можете ознакомиться с данными, приведенными в исследовании Infowatch, в диаграмме ниже.



В России, как и в мире, сильно увеличилось внимание к вопросам защиты данных в последнее время. Об этом свидетельствуют большое количество принимаемых в этой связи законов, увеличение активности Роскомнадзора, несмотря на мораторий на плановые проверки, и ожидаемые серьезные изменения по увеличению ответственности за нарушения в области защиты данных.

Так, например, в отчете Роскомнадзора за 2023 год[3] мы видим, что общая сумма наложенных административных штрафов составила **266 324 329 рублей.** Тогда как в отчете за 2022 год[4] мы видим общую сумму наложенных административных штрафов в размере **109 579 160 рублей.**
То есть, несмотря на мораторий на плановые проверки, активность Роскомнадзора в части привлечения лиц к ответственности за нарушения законодательства о защите персональных данных в 2023 году выросла по сравнению с предыдущим периодом более чем в два раза.

Вместе с тем российское законодательство о защите данных предъявляет множество требований к операторам и его соблюдение требует больших ресурсов и вовлеченности в процессы обработки персональных данных в компаниях. В этой связи у внутренних служб и DPO компаний часто возникают вопросы в отношении того, какие требования являются наиболее важными и сопряжены с наибольшим риском для бизнеса. Список требований может отличаться в зависимости от размера бизнеса, индустрии компании, бизнес-модели и других факторов, однако есть вопросы, которые будут актуальны для большинства операторов. В настоящей брошюре мы подсветили такие вопросы на текущий период и предлагаем Вам с ними ознакомиться.

Мария Осташенко, Партнер АЛРУД

Анастасия Петрова, Советник АЛРУД

1. IAPP-EY Privacy Governance Report 2023 – Executive Summary
2. Исследование утечек информации в отраслях за три года — Аналитический отчет (infowatch.ru)
3. gosdoklad_za_2023_ 03042024.pdf (rkn.gov.ru)
4. 2022_RKN_goskontrol.pdf

Важность письменного согласия

Согласие продолжает быть одним из важнейших правовых оснований обработки данных в глазах правоприменителя.

Одно из ключевых изменений конца 2023 года – кратное увеличение штрафов за обработку персональных данных без письменного согласия в случаях, когда такое согласие должно быть получено.

При этом нарушением является не только отсутствие согласия, но и несоответствие согласия обязательным требованиям, предъявляемым к нему законом. Увеличенный размер штрафов за данное нарушение выглядит следующим образом:

- **до 700 000 рублей** за первое нарушение вместо 150 000 рублей
- **до 1 500 000 рублей** за повторное нарушение вместо 500 000 рублей

Существенное повышение размера штрафов является индикатором пристального внимания Роскомнадзора к данному вопросу. В связи с этим компаниям рекомендуется перепроверить существующие письменные согласия на обработку персональных данных и внести в их формы требуемые изменения, если будут выявлены несоответствия с законом.

Наконец, напоминаем о возможности Роскомнадзора назначать штрафы, кратные количеству субъектов. Так, в отношении оператора в рамках одного эпизода по протоколам Роскомнадзора было вынесено пять судебных решений, сообразно количеству обратившихся лиц, чьи права были нарушены в результате незаконной обработки персональных данных[1].

Проверки Роскомнадзора

Роскомнадзор в конце 2023 года получил новое основание для проведения внеплановых проверок, использование которого позволит проводить проверки чаще, несмотря на продолжающееся действие моратория.

Основание – наличие 3-х и более несоответствий между сведениями, которые размещены на сайте оператора, и сведениями, которые оператор ранее включил:

- ☑ в уведомление о намерении начать обработку персональных данных;
- ☑ в уведомление о намерении осуществлять трансграничную передачу персональных данных.

Во избежание внепланового контрольного мероприятия операторам персональных данных следует регулярно проверять собственные сайты на предмет несоответствий. Выявить такое несоответствие Роскомнадзор может как в ходе мониторинга самостоятельно, без взаимодействия с оператором, так и по анонимной жалобе любых заинтересованных лиц.

Напоминаем, что во время действия моратория Роскомнадзор также вправе проверить оператора персональных данных в рамках:

1. мероприятий по контролю сайтов без взаимодействия с оператором;
2. профилактического визита;
3. внеплановой проверки (по определенному перечню оснований и при согласовании с прокуратурой).

1. См.: Дело Университета «Синергия» (Постановления мирового судьи судебного участка №383 Мещанского судебного района г. Москвы по делу: N 5-119/2020, N 5-120/2020, N 5-121/2020, N 5-122/2020, N 5-123/2020)

Требования к онлайн-ресурсам

Наращивание темпов внешнего контроля и новеллы 2023 года в области законодательства об информации и персональных данных вывели вопросы соответствия сайтов актуальным требованиям в разряд главных трендов 2024 года.

Помимо общих вопросов соблюдения законодательства, таких как обеспечение правовых оснований обработки персональных данных, а также обработки данных россиян в базах данных на территории РФ (требования о локализации), размещение политики конфиденциальности, направление уведомлений в Роскомнадзор, компаниям-владельцам сайтов стоит обратить внимание на следующие специальные применимые к сайтам аспекты:

- применение рекомендательных технологий (профайлинга): Роскомнадзор может заблокировать сайт, если его владелец не информирует пользователей об использовании таких алгоритмов и/или не публикует правила их применения;
- соблюдение требований авторизации пользователей: владельцы сайтов ограничиваются в возможных вариантах авторизации пользователей 4 способами (при помощи телефона, сервиса «Госуслуги», ЕБС или системы, отвечающей требованиям закона);
- использование иностранных сервисов: в частности, Google analytics, captcha и аналогов, посредством которых осуществляется обработка персональных данных на сайте. Их использование является триггером в отношении необходимости соблюдения правил трансграничной передачи и локализации, а также поводом для запроса со стороны Роскомнадзора предоставления доказательств их соблюдения оператором;
- использование файлов cookies: процесс их использования подразумевает обработку персональных данных и должен быть описан в политике оператора, а также должно быть обеспечено правовое основание для обработки персональных данных, например согласие пользователей;
- маркетинговые рассылки: маркетинговым рассылкам в адрес пользователей должен предшествовать сбор соответствующих обособленных согласий. Согласие на маркетинговые рассылки нельзя имплементировать в согласие на обработку персональных данных или в политику конфиденциальности, оно должно быть представлено пользователям отдельно;
- соблюдение требований к публикуемому контенту: запрет на размещение определённой информации в целом или для определенной аудитории (например, для детей, а также вытекающие из данного регулирования требования к возрастной маркировке контента на сайте).

«Экстерриториальный» принцип действия 152-ФЗ

«Экстерриториальный» принцип – новелла законодательства о персональных данных 2022 года. Подобный принцип содержится в законодательстве многих государств, а его закрепление в российском законодательстве связано с намерением законодателя распространить действие национального права на тех операторов, которые используют данные российских граждан в своих бизнес-процессах. Необходимость в данном принципе вызвана развитием цифровой экономики и потребностью в регулировании, в первую очередь, зарубежных интернет-ресурсов, направленных на российский рынок.

«Экстерриториальный» принцип в России предполагает распространение российского законодательства о персональных данных на тех операторов, которые заключают соглашения с российскими пользователями и / или получают согласия на обработку персональных данных у российских пользователей. Иностранные обработчики (лица, действующие по поручению операторов) несут ответственность перед субъектами персональных данных наряду с оператором.

На практике это означает, что иностранным лицам, обрабатывающим персональные данные российских граждан, нужно оценить объем применимости российского законодательства о персональных данных и размер ответственности за его соблюдение и впоследствии регулярно уделять внимание его соблюдению, а и таже следить за изменениями.

Тенденция на локализацию

В 2024 году цифровая индустрия в РФ сохраняет тренд на локализацию и обеспечение внутренней информационной независимости и безопасности IT-решений.

Тенденции способствуют множество факторов:

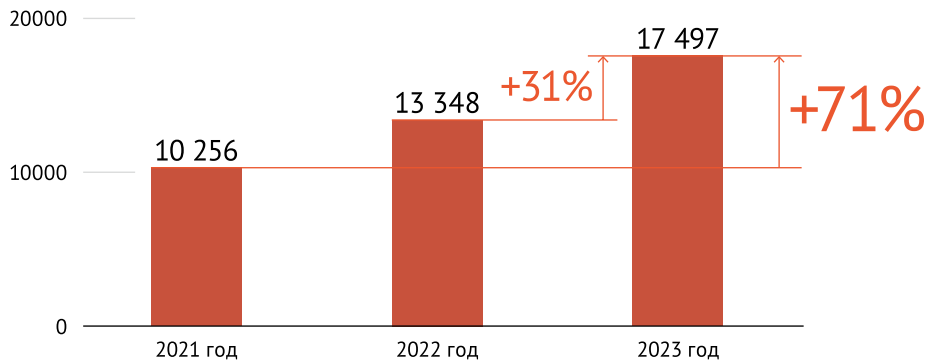
- внешних – введение 12-го пакета санкций ЕС, ограничивающего использование европейского ПО и получение IT-услуг;
- внутренних – курс на суверенный сегмент сети Интернет, новые правила для провайдеров-хостинга, импортозамещение ПО и средств защиты информации (запрет приобретения иностранного ПО и сопутствующих услуг в рамках госзакупок для использования на значимых объектах критической информационной инфраструктуры («**КИИ**»), запрет использования субъектами КИИ средств защиты информации из недружественных стран, запрет использования субъектами КИИ «недоверенных» программно-аппаратных комплексов (ПАК) при наличии российского аналога, вероятный запрет на использование иностранного ПО на любых значимых объектах КИИ).

Отдельно отметим основное требование Федерального закона «О персональных данных» от 27.07.2006 №152-ФЗ в части локализации: обрабатывать при сборе персональные данные граждан РФ следует с использованием баз данных, размещенных на территории РФ. Несоблюдение такого требования закона грозит штрафом в размере:

- **до 6 миллионов рублей** за первое нарушение;
- **до 18 миллионов рублей** за повторное нарушение. Штраф за повторное нарушение может налагаться неоднократно без ограничений по количеству раз.

Таким образом, ожидается, что в ближайшей перспективе тенденции по локализации только усилятся. Компаниям стоит обратить отдельное внимание на степень применимости к ним действующих ограничений и требований в части локализации и импортозамещения, а также непрерывно анализировать потенциальную применимость новых вводимых требований и ограничений.

Судебные споры, связанные с персональными данными в России[1]



Количество судебных споров, связанных с персональными данными, в России за два года увеличилось на 71%

1. https://mosdigitals.ru/media/za-poslednie-dva-goda-v-rossii-kolichestvo-sudebnykh-del-po-personalnym-dannym-vyroslo-na-71

Трансграничная передача данных

В 2024 году продолжают действовать правила трансграничной передачи персональных данных, вступившие в силу 1 марта 2023 года.

Напомним, что теперь трансграничная передача осуществляется только после специального уведомления Роскомнадзора. Такому уведомлению должна предшествовать оценка получателя персональных данных за границей на предмет соблюдения мер по конфиденциальности и защите персональных данных.

Роскомнадзор может запретить или ограничить трансграничную передачу. На практике такое случается не часто, однако риски ограничения процессов по трансграничной передаче в отношении тех или иных операторов не стоит недооценивать, т.к. в ряде случаев они могут вылиться в приостановку бизнес-процессов.

На практике уведомление о трансграничной передаче данных вызывает множество вопросов: как соблюсти требования к оценке иностранного получателя данных, требуется ли подавать повторное уведомление при изменении процессов обработки в части объема данных и т.д.

Иной аспект трансграничной передачи, требующий внимания операторов – использование иностранных сервисов для сбора данных с сайтов и приложений, при создании отчетов с информацией, полезной для бизнеса, например с помощью известного сервиса Google Analytics. По мнению Роскомнадзора, применение таких сервисов свидетельствует о трансграничной передаче и влечет необходимость соблюдения соответствующих требований об уведомлении регулятора и оценке получателя данных за границей.

Немаловажным аспектом является то, что уведомить Роскомнадзор о трансграничной передаче возможно только при наличии регистрации в реестре операторов персональных данных.

В настоящий момент прослеживается тенденция возрастания контроля регулятора за осуществлением операторами трансграничной передачи.

Обезличенные данные

2024 год может стать основополагающим для регулирования обезличенных персональных данных в случае принятия законопроекта[1], который закладывает фундаментальные основы для всей индустрии.

На сегодняшний день для частного бизнеса нет установленных прозрачных правил, которыми можно было бы руководствоваться для целей обезличивания данных. Роскомнадзор склоняется в большинстве случаев к выводу о том, что обезличенные данные остаются персональными со всеми вытекающими ограничениями законодательства в отношении обработки такой информации.

Новый законопроект предлагает установить общие рамки регулирования обезличивания, а множество отдельных вопросов в дальнейшем разрешить на уровне подзаконных актов.

Для бизнеса предлагаемые законопроектом изменения могут означать появление таких новых требований: передача обезличенных дата-сетов в государственную информационную систему, соблюдение предписанного порядка использования таких данных и иные требования. При этом непосредственная обязанность по обезличиванию данных возлагается на бизнес и должна происходить за счет самих компаний. Ожидается, что правовое регулирование данной сферы будет претерпевать дальнейшие изменения и, вероятно, будет являться подспорьем для развития технологий искусственного интеллекта.

Верная стратегия для бизнеса в 2024 году – отслеживание развития законодательства в сфере обезличивания и использования обезличенных данных.

1. Законопроект №992331-7 «О внесении изменений в Федеральный закон «О персональных данных» (https://sozd.duma.gov.ru/bill/992331-7#D97CDA3F-60FD-489B-B8D7-1A94A87991AC)

Утечки персональных данных

Конец 2023 года ознаменовался внесением ряда законопроектов, существенно усиливающих ответственность за нарушения в области защиты данных: как административной, так и уголовной[1]. 2024 год должен стать определяющим в плане их финализации.

На данный момент законопроекты проходят этапы обсуждений и одобрений. Таким образом, их финальные версии всё ещё могут измениться. Однако перед бизнесом уже возникает масса актуальных вопросов:

- Каким требованиям должна отвечать компания с учетом нововведений, чтобы избежать привлечения к административной ответственности и назначения крупных штрафов?
- Какие правовые механизмы следует предусмотреть для снижения рисков?
- Как владельцам и работникам бизнеса не попасть под уголовную ответственность при неопределенности правоприменения?

Одним из возможных изменений в рамках законопроекта является введение компенсаторного механизма для пострадавших от утечек. Пострадавшие субъекты персональных данных смогут запросить у компании компенсацию посредством сервиса «Госуслуги». В случае, если две трети обратившихся субъектов согласятся с предложенной нарушителем суммой, то подобный шаг будет учитываться как обстоятельство, смягчающее для него размер административной ответственности (в том числе в рамках применения пониженных коэффициентов при определении оборотного штрафа).

Компаниям на данном этапе следует оценить соответствие процессов обработки персональных данных будущим нормативным требованиям: провести внутренний аудит процессов обработки, разработать и внедрить процедуру своевременного реагирования на утечки, оценить и соблюдать требования в части информационной безопасности, которые помогут предотвратить различные инциденты, продумать компенсаторные меры. Эти и иные меры позволят бизнесу избежать крупных штрафов в размере вплоть до 500 млн рублей и потенциальных оборотных штрафов.

Уведомление об инцидентах, связанных с утечками персональных данных

Правило, подразумевающее необходимость операторов уведомлять Роскомнадзор о произошедшей утечке, вступило в силу ещё в 2022 г. Согласно действующей норме операторы обязаны уведомлять ведомство о произошедшей утечке в течение 24 часов (а также повторно в течение 72 часов о принятых мерах по устранению инцидента).

Положения продолжают быть крайне актуальными, в том числе в связи с потенциальным введением обновлённой санкции: если сейчас штраф за несообщение о произошедшем инциденте составит для компании незначительную сумму в размере до 5 000 руб., то предлагаемыми изменениями такой размер штрафа существенно увеличивается. В случае привлечения компаний к ответственности он может составить от 1 000 000 до 3 000 000 руб. за одно нарушение[2].

1. Законопроект №502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (https://sozd.duma.gov.ru/bill/502104-8) / Законопроект №502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (https://sozd.duma.gov.ru/bill/502113-8)
2. Законопроект упоминается выше. Законопроект №502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (https://sozd.duma.gov.ru/bill/502104-8)

Персональная ответственность менеджмента, введение уголовной ответственности

Если в предшествующие годы законодательный тренд на усиление ответственности в сфере защиты данных касался в основном компаний-операторов, то уже в начале 2024 года законодатель выходит за рамки механизма «обезличенной» ответственности.

Так, обсуждается новый законопроект[1] от Центрального Банка РФ об отстранении от должности лиц, ответственных за информационную безопасность в финансовых организациях, за допущенные ими утечки данных и иные нарушения.

Также одним из проявлений данного тренда является уже упомянутый законопроект о введении уголовной ответственности за незаконный оборот и утечки персональных данных, в рамках которого виновному физическому лицу может грозить лишение свободы на срок до 10 лет.

Подобные инициативы свидетельствуют о попытках перехода к механизму индивидуальной ответственности в области нарушения законодательства о персональных данных и информационной безопасности. Законодатель явно намерен повысить внимание менеджмента к соблюдению действующих норм.

1. Законопроект опубликован не был. Ссылка на источник: https://iz.ru/1636949/natalia-ilina/10-let-bez-prava-top-menedzherov-bankov-diskvalifitciruiut-za-utechki-dannykh

Ключевые контакты

Мария Осташенко
Партнер

Коммерческое право,
Интеллектуальная собственность,
Защита данных и кибербезопасность

MOstashenko@alrud.com

Анастасия Петрова
Советник

Защита данных и кибербезопасность,
Трудовое право

APetrova@alrud.com

Елизавета Костюченко
Юрист

Интеллектуальная собственность,
Защита данных и кибербезопасность

EKostyuchenko@alrud.com

Виктория Швецова
Юрист

Защита данных и кибербезопасность

VShvetsova@alrud.com

Ул. Скаковая, д. 17, стр. 2, 6 эт., Москва, Россия, 125040
E-mail: info@alrud.com | www.alrud.com | Тел. +7 495 234-9692

АЛРУД