ПРОЕКТ

Расширен перечень оснований для проведения Роскомнадзором внеплановых проверок в отношении операторов персональных данных

Вниманию операторов персональных данных

Юридическая компания «Пепеляев Групп» сообщает, что 18 ноября 2023 года вступил в силу Приказ Минцифры России от 17.08.2023 № 720[1], дополняющий перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных.

Приказом Минцифры России от 15.11.2021 № 1187[2] утвержден перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных (далее – индикатор риска). Выявление Роскомнадзором у оператора хотя бы одного индикатора риска является основанием для проведения внепланового контрольного (надзорного) мероприятия (далее – **внеплановой проверки**).

Приказом Минцифры от 17.08.2023 № 720 к данному перечню добавлен новый индикатор риска, а именно:

- Установление Роскомнадзором трех и более фактов несоответствия информации, указанной оператором в уведомлениях (о намерении осуществлять обработку персональных данных; об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных; о намерении осуществлять трансграничную передачу персональных данных; о прекращении обработки персональных данных) сведениям, размещенным на принадлежащем контролируемому лицу сайте в информационно-

---

[1] Приказ Минцифры России от 17.08.2023 № 720 «О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утвержденный приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 ноября 2021 г. № 1187»

[2] Приказ Минцифры России от 15.11.2021 № 1187 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных»

телекоммуникационной сети «Интернет» в соответствии с ч. 2 ст. 18.1 Федерального закона «О персональных данных» .

Комментарий «Пепеляев Групп»

В соответствии с ч. 2 ст. 18.1 Федерального закона «О персональных данных» оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Политика в отношении обработки персональных данных должна определять для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований[3].

Роскомнадзором активно проводятся мероприятия по контролю без взаимодействия с контролируемым лицом, которые включают в себя:

a) наблюдение за соблюдением требований при размещении информации в сети «Интернет»;

b) наблюдение за соблюдением требований посредством анализа информации о деятельности контролируемого лица, которая представляется оператором (например, в уведомлении о намерении осуществлять обработку персональных данных) в Роскомнадзор или может быть получена Роскомнадзором (в том числе в рамках межведомственного информационного взаимодействия)[4].

То есть Роскомнадзор вправе самостоятельно анализировать сайт оператора (без взаимодействия с ним). Полагаем, что в случае сравнения Роскомнадзором информации, указанной в реестре операторов персональных данных, и в политике в отношении обработки персональных данных, размещенной на сайте оператора, и выявления несоответствий в указанных сведениях, в отношении оператора может быть проведено внеплановое контрольное (надзорное) мероприятие.

---

[3] П. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

[4] П. 59 Положения о федеральном государственном контроле (надзоре) за обработкой персональных данных, утвержденного Постановлением Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»

Указанный выше индикатор риска действует с 18 ноября 2023 г.

Помимо приведенного выше, основанием для проведения Роскомнадзором внеплановой проверки может также стать выявление одного из следующих индикаторов риска:

- Установление Роскомнадзором в течение календарного года 10 и более фактов несоответствия сведений, предоставляемых оператором по запросу Роскомнадзора, и информации, поступившей в Роскомнадзор от граждан, в части, касающейся наличия в деятельности оператора признаков неправомерной обработки их персональных данных.

Комментарий «Пепеляев Групп»

В соответствии с п. 1 ч. 3 ст. 23 Федерального закона «О персональных данных» Роскомнадзор имеет право запрашивать у физических или юридических лиц (операторов) информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию. Оператор обязан сообщить в Роскомнадзор необходимую информацию в течение 10 рабочих дней с даты получения такого запроса.

В то же время согласно ч. 1 ст. 17 Федерального закона «О персональных данных», если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в Роскомнадзор или в судебном порядке.

Если в течение календарного года Роскомнадзором будет установлено 10 и более фактов несоответствия сведений, предоставляемых оператором, и информации, поступившей от субъектов персональных данных, в отношении оператора может быть проведено внеплановое контрольное (надзорное) мероприятие.

Установление Роскомнадзором в течение календарного года 10 и более фактов предоставления неограниченному кругу лиц доступа к базам персональных данных и (или) распространения баз персональных данных в информационно-телекоммуникационной сети «Интернет», имеющих признаки принадлежности оператору.

Комментарий «Пепеляев Групп»

Полагаем, в данном случае речь идет об «утечках» персональных данных в тех случаях, когда невозможно достоверно определить, кому именно принадлежит база данных, подверженная «утечке», однако по отдельным признакам можно говорить о принадлежности базы данных определенному оператору.

Напомним, что предметом федерального государственного контроля (надзора) за обработкой персональных данных является соблюдение операторами обязательных требований в области персональных данных, установленных ФЗ «О персональных данных» и принимаемыми в соответствии с ним иными нормативными правовыми актами.

В соответствии с п. 37 Положения о федеральном государственном контроле (надзоре) за обработкой персональных данных[5], такой контроль (надзор) осуществляется посредством проведения плановых и внеплановых контрольных (надзорных) мероприятий (далее – проверок).

Исходя из положений п. 11(3) Постановления Правительства РФ от 10.03.2022 № 336 «Об особенностях организации и осуществления государственного контроля (надзора), муниципального контроля» до 2030 года в планы проведения плановых проверок включаются проверки только в отношении операторов, отнесенных к категории высокого риска[6].

Что касается внеплановых проверок, то в 2023 году они проводятся исключительно по основаниям, перечисленным в пункте 3 Постановления Правительства № 336, в том числе:

- при выявлении индикаторов риска нарушения обязательных требований;
- по решению руководителя, заместителя руководителя Роскомнадзора, в случае если установлен факт распространения (предоставления) в сети «Интернет» баз данных (или их части), содержащих персональные данные.

В соответствии с положениями ч. 2 ст. 90 Федерального закона от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» в случае выявления несоответствий требованиям законодательства результатом проведенной внеплановой проверки может стать:

---

[5] Утверждено Постановлением Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных».

[6] Критерии отнесения операторов к определенной категории риска определены Приложением к Положению о контроле за обработкой персональных данных.

- предписание об устранении выявленных нарушений;
- административная ответственность;
- уголовная ответственность.

Также напомним, что административная ответственность за нарушение законодательства РФ в области персональных данных установлена ст. 13.11 Кодекса РФ об административных правонарушениях. Например, в случае отсутствия у оператора согласий на обработку персональных данных (если их получение обязательно), на него может быть наложен административный штраф в размере от 60 тысяч до 100 тыс. руб.[7] А в случае использования оператором баз данных, находящихся за пределами территории РФ, при сборе персональных данных, в том числе посредством сети «Интернет»[8], штраф может составить от 1 млн руб. до 6 млн руб.

О чем подумать, что сделать

Проведение Роскомнадзором внеплановой проверки (даже в условиях действующих ограничений) в отношении оператора возможно в следующих случаях:

- если в течение календарного года Роскомнадзором будет установлено 10 и более фактов несоответствия сведений, предоставляемых оператором, и информации, поступившей от субъектов персональных данных (недовольных клиентов/бывших работников/конкурентов);
- если в течение календарного года Роскомнадзором будет установлено 10 и более фактов утечек баз персональных данных, имеющих признаки принадлежности оператору;
- если в результате сравнения Роскомнадзором информации, указанной в реестре операторов персональных данных, и в политике в отношении обработки персональных данных, размещенной на сайте оператора, будет выявлено 3 и более фактов несоответствия.

Таким образом, у каждого оператора персональных данных есть риск проведения Роскомнадзором внеплановой проверки, что может привести к привлечению оператора к административной и/или уголовной ответственности.

Для минимизации рисков привлечения к ответственности за нарушения в области законодательства о персональных данных рекомендуем:

1. провести аудит соответствия требованиям законодательства о персональных данных самостоятельно или с привлечением консультантов, устранить выявленные нарушения;
2. вести внутренний реестр процессов обработки персональных данных, содержащий информацию о целях обработки персональных

---

[7] Ч. 1 ст. 13.11 КоАП РФ.
[8] Ч. 8 ст. 13.11 КоАП РФ.

данных, категориях и перечне обрабатываемых персональных данных, категориях субъектов, персональные данные которых обрабатываются, способах, сроках их обработки и хранения, порядке уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;

3. отслеживать изменения в процессах обработки персональных данных, своевременно обновлять информацию в локальных нормативных актах (например, в политике в отношении обработки персональных данных);
4. на регулярной основе проводить обучение сотрудников компании требованиям к обработке персональных данных, а также контролировать уровень осведомленности сотрудников (путем проведения тестирований).

Особое внимание рекомендуем уделить содержанию и функционала сайта компании. Необходимо:

1. проанализировать, какие персональные данные обрабатываются с помощью сайта (например, посредством форм сбора данных, cookie-файлов, сервисов сбора технических данных),
2. обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации (то есть обеспечить хостинг сайта в Российской Федерации, отказаться от использования иностранных сервисов сбора персональных данных (например, Google Analytics, Google Forms), использовать российские CMS),
3. опубликовать на всех страницах сайта, с использованием которых осуществляется сбор персональных данных, политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных,
4. обеспечить соответствие информации, указанной в реестре операторов персональных данных (в уведомлении о намерении осуществлять обработку персональных данных), информации, размещенной на сайте (в том числе, в политике в отношении обработки персональных данных).

В случае, если компания не подавала уведомление о намерении осуществлять обработку персональных данных и не внесена в реестр операторов персональных данных, необходимо дополнительно оценивать риски, связанные с возможным выявлением несоответствий в предоставленной информации.

Помощь консультанта

Специалисты «Пепеляев Групп» готовы оказать компаниям всестороннюю юридическую поддержку в соблюдении требований законодательства о персональных данных.

Спектр услуг «Пепеляев Групп» включает:

- актуализация и приведение внутренних документов компании в соответствие с требованиями 152-ФЗ, включая политику в отношении обработки персональных данных, положения об обработке персональных данных, форм согласий на обработку персональных данных и иных необходимых документов в области персональных данных;
- подготовка и направление в Роскомнадзор уведомления о намерении осуществлять обработку персональных данных, уведомления о намерении осуществлять трансграничную передачу персональных данных, уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, трансграничную передачу персональных данных, уведомления о прекращении обработки персональных данных;
- подготовка правовых заключений и проведение консультаций по вопросам обработки персональных данных;
- правовая поддержка при взаимодействии с Роскомнадзором и/или субъектом персональных данных.

Контактная информация

Николай Солодовников
Партнер

T: +7 (495) 767 00 07
n.solodovnikov@pgplaw.ru

Полина Бардина
Руководитель цифровой группы

T: +7 (495) 767 00 07
p.bardina@pgplaw.ru