МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)

ПРИКАЗ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71851
от "28" декабря 2022 г.

14.11.2022 № 187

Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных

В соответствии с частью 10 статьи 23 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233), абзацем вторым пункта 1 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного постановлением Правительства Российской Федерации от 16 марта 2009 г. № 228 (Собрание законодательства Российской Федерации, 2009, № 12, ст. 1431), п р и к а з ы в а ю:

1. Утвердить Порядок и условия взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных в соответствии с приложением к настоящему приказу.

2. Настоящий приказ вступает в силу с 1 марта 2023 г.

Руководитель А.Ю. Липов

УТВЕРЖДЕНЫ
приказом Федеральной службы
по надзору в сфере связи,
информационных технологий
и массовых коммуникаций
от 14.11.2022 № 187

Порядок и условия взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных

1. Взаимодействие Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в целях учета в реестре учета инцидентов в области персональных данных информации о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, осуществляется в форме направления операторами в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомления о таких фактах[1] (далее – уведомление), содержащего:

информацию о произошедшем инциденте[2] (далее – первичное уведомление);

информацию о результатах внутреннего расследования выявленного инцидента (далее – дополнительное уведомление)[3].

2. Первичное уведомление должно содержать:

2.1. Сведения[4]:

о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы

---

[1] Часть 3.1 статьи 21 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Далее – Федеральный закон «О персональных данных» (Собрание законодательства Российской Федерации, 2022, № 29, ст. 5233).

[2] Пункт 1 части 3.1 статьи 21 Федерального закона «О персональных данных» (Собрание законодательства Российской Федерации, 2022, № 29, ст. 5233).

[3] Пункт 2 части 3.1 статьи 21 Федерального закона «О персональных данных» (Собрание законодательства Российской Федерации, 2022, № 29, ст. 5233).

[4] Пункт 1 части 3.1 статьи 21 Федерального закона «О персональных данных».

данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – скомпрометированная база данных), количество содержащихся в ней записей. Дополнительно оператор может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона «О персональных данных»[5]);

о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых оператором организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона «О персональных данных»[6]);

о лице, уполномоченном оператором на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

2.2. Данные оператора, направившего уведомление:

фамилию, имя и отчество (при наличии) гражданина, индивидуального предпринимателя;

полное и сокращенное (при наличии) наименование юридического лица;

идентификационный номер налогоплательщика юридического лица, индивидуального предпринимателя, физического лица;

---

[5] Собрание законодательства Российской Федерации, 2011, № 31, ст. 4701; 2022, № 29, ст. 5233.

[6] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701; 2022, № 29, ст. 5233.

адрес регистрации по месту жительства (пребывания) физического лица, индивидуального предпринимателя;

адрес юридического лица в пределах места нахождения юридического лица;

адрес электронной почты (при наличии) для направления информации, предусмотренной пунктом 8 настоящего Порядка.

2.3. Иные сведения и материалы, находящиеся в распоряжении оператора, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

3. Дополнительное уведомление должно содержать сведения[7]:

о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица оператора с указанием должности (если причиной инцидента стали действия сотрудника оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении оператора).

4. В случае если оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

5. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

---

[7] Пункт 2 части 3.1 статьи 21 Федерального закона «О персональных данных».

6. Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

7. Уведомление в форме электронного документа направляется оператором посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети «Интернет» (далее – Портал персональных данных), после прохождения процедуры идентификации и аутентификации посредством федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»[8] (далее – ЕСИА) и подписывается электронной подписью в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[9].

8. Оператору с момента поступления уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления.

9. При направлении дополнительного уведомления посредством Портала персональных данных оператор должен указать номер и ключ уведомления, полученного в соответствии с пунктом 8 настоящего Порядка.

---

[8] Постановление Правительства Российской Федерации от 10 июля 2013 г. № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (Собрание законодательства Российской Федерации, 2013, № 30, ст. 4108; 2022, № 21, ст. 3453).

[9] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2022, № 29, ст. 5306.

10. В случае направления оператором неполных или некорректных сведений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, не позднее трех рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос оператору о представлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

11. Недостающие сведения и (или) пояснения относительно некорректности представленных в уведомлении сведений предоставляются оператором в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение трех рабочих дней со дня получения запроса, указанного в пункте 10 настоящего Порядка, одним из способов, предусмотренных пунктом 5 настоящего Порядка.

12. В случае если по истечении сроков, установленных пунктом 2 части 3.1 статьи 21 Федерального закона «О персональных данных», дополнительное уведомление в адрес Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций не поступило, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций оператору направляется требование о необходимости представить сведения о результатах внутреннего расследования выявленного инцидента (далее – требование о предоставлении сведений).

13. Ответ на требование о предоставлении сведений направляется оператором Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение одного рабочего дня со дня получения такого требования одним из способов, предусмотренных пунктом 5 настоящего Порядка.

14. В случае если Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций выявлен факт неправомерного распространения скомпрометированной базы данных, содержание которой указывает на ее принадлежность к конкретному оператору, такому оператору Федеральной службой по надзору в сфере связи,

информационных технологий и массовых коммуникаций направляется требование о необходимости представить уведомление (далее – требование о предоставлении уведомления).

15. Оператор, которому направлено требование о предоставлении уведомления, направляет его в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в сроки, установленные частью 3.1 статьи 21 Федерального закона «О персональных данных».

16. В случае неподтверждения оператором факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, и (или) неустановления принадлежности скомпрометированной базы данных, содержащей персональные данные, указанному оператору при выявлении такого инцидента Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций или иным заинтересованным лицом, оператором направляется уведомление, предусмотренное частью 3.1 статьи 21 Федерального закона «О персональных данных».

В указанном случае к дополнительному уведомлению оператором прикладывается акт о проведенном внутреннем расследовании, подтверждающий отсутствие факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, и (или) неустановления принадлежности скомпрометированной базы данных, содержащей персональные данные, соответствующему оператору в деятельности такого оператора.

17. В случае установления оператором, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, содержащихся в базе данных, характеристики которых полностью соответствуют ранее скомпрометированной базе данных, оператором направляется уведомление, предусмотренное частью 3.1 статьи 21 Федерального закона «О персональных данных».

В указанном случае при направлении уведомления оператором указывается дата и номер ранее направленного уведомления, содержащего сведения, предусмотренные частью 3.1 статьи 21 Федерального закона «О персональных данных», о ранее скомпрометированной базе данных, содержащей персональные данные.

18. В случае если посредством Портала персональных данных поступила информация, не относящаяся к факту неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, такое уведомление не подлежит рассмотрению Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.