

Приложение № 2
к приказу Роскомнадзора
от 31 марта 2022 г. № 55

Доклад
о правоприменительной практике
организации и проведения федерального государственного контроля
(надзора) за обработкой персональных данных
в 2021 году

I. Приоритетные вопросы правоприменительной практики организации и проведения федерального государственного контроля (надзора) за обработкой персональных данных.

1. Составление ежегодных планов.

Осуществление контрольной (надзорной) деятельности производится на основании планов деятельности территориальных органов Роскомнадзора (далее – территориальные органы), планов проверок юридических лиц и индивидуальных предпринимателей.

В соответствии с п. 18 ч. 3.1 ст. 1 Федерального закона от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (далее – Закон № 294-ФЗ) положения Закона № 294-ФЗ, устанавливающие порядок организации и проведения проверок, не применялись к государственному контролю и надзору за обработкой персональных данных.

Таким образом, согласование проведения контрольных (надзорных) мероприятий за обработкой персональных данных на 2021 год с органами прокуратуры не требовалось.

При планировании проверок использовался риск-ориентированный подход в соответствии с рекомендациями центрального аппарата Роскомнадзора.

В 2021 году территориальными органами Роскомнадзора проведено 595 плановых проверок, в том числе в отношении органов государственной власти проведено 25 контрольных (надзорных) мероприятий.

Нарушения обязательных требований были выявлены по результатам 468 плановых проверок (что составляет 79% от общего количества проведённых плановых проверок в 2021 году), что свидетельствует о качественном подходе к планированию и проведению плановых проверок в области персональных данных.

2. Использование оснований для проведения внеплановых проверок, согласование проведения внеплановых выездных проверок с органами прокуратуры.

В 2021 году проведено 14 внеплановых контрольных (надзорных) мероприятий, в том числе по требованию прокуратуры, в связи с проверкой исполнения ранее выданных предписаний, на основании обращений граждан о нарушении их прав, как субъектов персональных данных.

В органы прокуратуры направлены 2 запроса о согласовании проведения проверок, по результатам рассмотрения которых органы прокуратуры согласовали проведение внеплановых проверок.

3. Разработка и издание решений о проведении контрольных (надзорных) мероприятий.

Разработка и издание решений о проведении контрольных (надзорных) мероприятий осуществляются с использованием Единой информационной системы Роскомнадзора (ЕИС).

4. Выбор документального или выездного контрольного (надзорного) мероприятия; исчисление и соблюдение сроков проведения контрольного (надзорного) мероприятия; соблюдение прав юридических лиц и индивидуальных предпринимателей при организации и проведении контрольных (надзорных) мероприятий.

При выборе документального или выездного контрольного (надзорного) мероприятия учитывались положения законодательства о федеральном государственном контроле (надзоре) за обработкой персональных данных, а также необходимость достижения цели минимальными ресурсами.

В 2021 году проводились выездные контрольные (надзорные) мероприятия.

Такой вид проверки был избран в соответствии с рекомендациями центрального аппарата Роскомнадзора.

Контрольные (надзорные) мероприятия в 2021 году проведены без нарушения сроков их проведения.

Жалобы на действия проверяющих лиц в связи с проведением контрольных (надзорных) мероприятий не поступали.

5. Оформление результатов контрольных (надзорных) мероприятий и принятия мер по их результатам.

Организация, проведение и оформление результатов проверок осуществляется территориальными органами в соответствии с Законом № 248-ФЗ.

По результатам проведения проверок должностными лицами территориальных органов составляются акты в установленные законом сроки. С результатами проведения проверок и актами проверок контролируемые лица знакомятся под роспись, либо акты направляются лицам заказными письмами с уведомлениями о вручении.

В случае выявления в деятельности юридических лиц, а также органов государственной власти нарушений обязательных требований в области персональных данных, юридическим лицам, а также органам государственной власти выдавались предписания об устранении выявленных нарушений.

Контрольные (надзорные) мероприятия, в результате которых выявлены нарушения, но не принято никаких мер, отсутствуют.

6. Организация и проведение контрольных (надзорных) мероприятий, осуществляемых без взаимодействия.

В 2021 году территориальными органами проведено 3785 контрольных (надзорных) мероприятия, осуществляемых без взаимодействия.

Основаниями для проведения внеплановых контрольных (надзорных) мероприятий, осуществляемых без взаимодействия в 2021 году, послужили указания центрального аппарата Роскомнадзора, данные на основании имеющихся сведений о совершённых или готовящихся нарушениях.

Трудности с планированием, проведением контрольных (надзорных) мероприятий, осуществляемых без взаимодействия, не возникали.

7. Привлечение юридических лиц, должностных лиц, индивидуальных предпринимателей к ответственности за административные правонарушения, выявленные при осуществлении федерального государственного контроля (надзора) в области связи.

В 2021 году территориальными органами в соответствии с Кодексом Российской Федерации об административных правонарушениях (далее — КоАП РФ) по результатам контрольных (надзорных) мероприятий составлено 100 протоколов об административных правонарушениях, в том числе по следующим составам:

- обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 13.11 КоАП РФ (ч. 1 ст. 13.11 КоАП РФ);

- обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных (ч. 2 ст. 13.11 КоАП РФ);

- невыполнение оператором, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных (ч. 3 ст. 13.11 КоАП РФ);

- непредставление или несвоевременное представление сведений (информации), либо представление таких сведений (информации) в неполном объеме или в искаженном виде (ст. 19.7 КоАП РФ).

Наибольшее количество протоколов составлено непредставление или несвоевременное представление сведений (информации), либо представление таких сведений (информации) в неполном объеме или в искаженном виде (ст. 19.7 КоАП РФ).

На рассмотрение в суды передано 100 протоколов об административных правонарушениях.

Основными причинами отказов в привлечении к административной ответственности явилось истечение сроков давности привлечения к административной ответственности и освобождение от административной ответственности с вынесением устного замечания (малозначительность).

Трудности при составлении протоколов об административных правонарушениях и направлении их в суды не возникали.

II. Приоритетные вопросы правоприменительной практики соблюдения обязательных требований.

1. Статистика соблюдения обязательных требований.

В 2021 году в деятельности 688 субъектов надзора выявлены нарушения.

Исходя из анализа мероприятий по контролю, можно выделить основные правонарушения, связанные с несоблюдением обязательных требований:

- несоблюдение оператором установленных требований обработки персональных данных после достижения цели обработки (ч. 4 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- несоблюдение требований конфиденциальности при обработке персональных данных (ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- отсутствие в поручении лицу, которому оператором поручается обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности, а также требований к защите обрабатываемых персональных данных (ч. 3 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- несоблюдение требований к письменной форме согласия на обработку персональных данных (ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- отсутствие перечня документов, утвержденных актом руководителя государственного органа (пп. «б» п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённых постановлением Правительства Российской Федерации от 21.03.2012 № 211 (далее – Перечень мер);

- отсутствие у оператора документов, устанавливающих места хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (п. 13 Положения об

особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденном постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении» (далее – Положение);

- несоответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации (п. 7 Положения);

- отсутствие документов, подтверждающих информирование лиц, осуществляющих обработку персональных данных без использования средств автоматизации о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии) (п. 6 Положения);

- непредставление и (или) несвоевременное представление уведомления по обработке персональных данных при осуществлении деятельности по обработке персональных данных, не попадающей под исключения ч. 2 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ч. 1 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- обработка персональных данных субъектов персональных данные в отсутствие правовых оснований, установленных пп. 2-11 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ч. 1 ст. 6 Закона);

- неуведомление уполномоченного органа по защите прав субъектов персональных данных об изменениях сведений, указанных в части 3 настоящей статьи, а также о прекращении обработки персональных данных, в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных (ч. 7 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- передача персональных данных работника без письменного согласия (ст. 88 Трудового кодекса Российской Федерации);

- обработка избыточных персональных данных по отношению к заявленным целям их обработки (ч. 5 ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- представление в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения (ч. 3 ст. 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- непринятие оператором мер по опубликованию или обеспечению неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных (ч. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- принятие оператором мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами (ч. 1 ст. 18.1 Федерального закона Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

- принятие государственным или муниципальным органом мер по опубликованию на официальном сайте органа документов, определяющих политику в отношении обработки персональных данных в установленный срок (п. 2 Перечня мер);

- несоблюдение установленных требований к ведению журналов, содержащих персональные данные (п. 8 Положения);

- несоблюдение оператором условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ (п. 15 Положения).

2. Типичные нарушения обязательных требований.

Анализ причин и условий, способствовавших совершению типичных (наиболее часто встречающихся) нарушений, свидетельствует о том, что основная их часть вызвана непроведением оператором мероприятий внутреннего контроля соответствия обработки персональных данных требованиям, установленным законодательством Российской Федерации, а также неозакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Так, наибольшим количеством выявленных в отчетном периоде нарушений являются нарушения, связанные с уведомлением уполномоченного органа об обработке персональных данных (непредставление и (или) несвоевременное представление уведомления по обработке персональных данных при осуществлении деятельности по обработке персональных данных, не попадающей под исключения, установленные законодательством представлению в уполномоченный орган уведомления об обработке персональных данных, содержащего неполные и (или) недостоверные сведения, непредставление в уполномоченный орган сведений о прекращении обработки персональных данных или об изменении информации, содержащейся в уведомлении об обработке персональных данных), принятие оператором мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, отсутствие у оператора места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ, несоблюдение оператором требований по информированию лиц, осуществляющих обработку персональных данных без использования средств

автоматизации, несоответствие письменной формы согласия на обработку персональных данных в случаях, установленных законодательством.

3. Применение обязательных требований во взаимосвязи положений различных нормативных правовых актов, в том числе, вопросы недостаточной ясности и взаимной согласованности обязательных требований.

Анализ потенциальной выполнимости обязательных требований, нарушения которых встречаются наиболее часто, показал, что соблюдение данных требований потенциально выполнимо.

Соблюдается баланс достаточного регулирования со стороны контрольного (надзорного) органа и возможности исполнения оператором обязательных требований законодательства в области персональных данных.

Условия, препятствующие выполнению обязательных требований, отсутствуют. Противоречия при применении нормативных правовых актов отсутствуют.

III. Предложения о совершенствовании законодательства на основе анализа правоприменительной практики контрольной (надзорной деятельности).

Существующее регулирование контрольной (надзорной) деятельности (Закон № 248-ФЗ, Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных, утвержденное постановлением Правительства Российской Федерации от 29.06.2021 № 1046) является актуальным и достаточным, отвечающим реалиям.

В целях обеспечения единообразия правоприменения требуется проведение комплексной работы, приоритетно разъяснительного и профилактического характера.
