Постановление Правительства РФ от 13 февраля 2019 года №146 «Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных»

Постановление опубликовано 15 февраля 2019 года - http://publication.pravo.gov.ru/Document/View/0001201902150008 .

В соответствии со ст. 3 Федерального закона от 21 июля 2014 г. N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» и ст. 2 Федерального закона от 22 февраля 2017 года № 16-ФЗ «О внесении изменений в главу 5 Федерального закона «О персональных данных» и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», общий порядок осуществления государственного контроля (надзора) с 1 сентября 2015 года не распространяется на государственный контроль и надзор за обработкой персональных данных (п. 20 ч. 3.1 ст. 1 Федерального закона от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»).

13 февраля 2019 года Правительством РФ принято постановление, регулирующее порядок организации и проведения проверок операторов персональных данных. Контроль и надзор за обработкой персональных данных осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Данные правила не распространяются на контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, установленных в соответствии со статьей 19 Федерального закона «О персональных данных». Иными словами, установленные Постановлением правила контроля не распространяются на предпринимаемые операторами организационные и технические меры безопасности персональных данных. В качестве таковых законом, в частности, установлены:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Таким образом, Роскомнадзор при осуществлении контроля в сфере обработки персональных данных не проверяет «техническую сторону» их защиты.

Следует отметить, что плановые проверки могут проводиться не только в отношении операторов, включенных в предусмотренный законом реестр (п. 3 ч. 5 ст. 23 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», https://pd.rkn.gov.ru/operators-registry/operators-list/), но и в отношении операторов, не включенных в него (п. 32.2 Административного регламента предоставления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соблюдением обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных Утвержден Приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312).

Постановлением устанавливается особая периодичность проведения плановых проверок – не чаще 1 раза в 2 года (по общему правилу периодичность плановых проверок юридических лиц не может быть чаще 1 раза в 3 года), при этом для включения в план проверок устанавливается ряд необходимых критериев (п. 7 Постановления):

а) оператор осуществляет обработку персональных данных в информационных системах персональных данных, имеющих в соответствии с федеральными законами статус государственных информационных систем;

б) оператор осуществляет сбор биометрических и специальных категорий персональных данных;

в) оператор осуществляет трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных;

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ
Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

г) оператор осуществляет обработку персональных данных по поручению иностранного государственного органа, иностранного юридического лица, иностранного физического лица, которые не зарегистрированы в установленном порядке на территории Российской Федерации.

Более подробного анализа заслуживают пункты «б», «в» и «г».

В соответствии с п. «б» в плановом порядке могут проверяться операторы, обрабатывающие специальные категории персональных данных. Применительно к деятельности некоммерческих организаций, наиболее вероятно попадание в план проверок различных организаций инвалидов или благотворительных организаций, оказывающих помощь людям, страдающим от различных заболеваний, поскольку такие организации априори осуществляют обработку таких персональных данных как сведения о состоянии здоровья (диагнозы, присвоенные группы инвалидности и т.д.), которые в соответствии со ст. 10 ФЗ «О персональных данных» отнесены к специальным категориям персональных данных.

Следующая категория организаций, подпадающая под критерии включения в план проверок Роскомнадзора (п. «в») – организации, осуществляющие трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных. Это актуально для некоммерческих организаций, осуществляющих свою деятельность на международном уровне, или сотрудничающих с международными или иностранными организациями. К государствам, обеспечивающим адекватную защиту прав субъектов персональных данных, относятся:

- страны, подписавшие и ратифицировавшие Конвенцию о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. ETS № 108. На сегодняшний день – это 56 государств, а именно: Австрия, Азербайджан, Албания, Андорра, Аргентина, Армения, Бельгия, Болгария, Босния и Герцеговина, Буркина Фасо, бывшая Югославская республика Македония, Великобритания, Венгрия, Германия, Греция, Грузия, Дания, Ирландия, Исландия, Испания, Италия, Кабо-Верде, Кипр, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Марокко, Мексика, Монако, Маврикий, Нидерланды, Норвегия, Польша, Португалия, Молдова, Россия, Румыния, Сан-Марино, Сенегал, Сербия, Словакия, Словения, Тунис, Турция, Украина, Уругвай, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония - https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=Z3hgtzKF ;

- страны, имеющие общенациональные нормативные правовые акты в области защиты персональных данных и уполномоченный надзорный орган по защите прав субъектов персональных данных. Это 19 стран: Австралия, Израиль, Канада, Монголия, Малайзия, Новая Зеландия, Ангола, Бенин, Республика Корея, Перу, Чили, Специальный административный район Гонконг Китайской Народной Республики, Коста-Рика, Катар, Мали, Сингапур, Южно-Африканская Республика, Габон, Казахстан. Перечень таких стран определяет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - https://pd.rkn.gov.ru/library/p193/p199/ .

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ
Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

В соответствии с п. «г» в плановом порядке должны проверяться операторы, осуществляющие «*обработку персональных данных по поручению иностранного государственного органа, иностранного юридического лица, иностранного физического лица, которые не зарегистрированы в установленном порядке на территории Российской Федерации*». В отношении данного пункта имеется неопределенность, как именно Роскомнадзор будет определять наличие такого «поручения» при условии, что «иностранный государственный орган, иностранное юридическое лицо, иностранное физическое лицо» не зарегистрированы в установленном порядке на территории РФ. Применительно к деятельности НКО, вероятно, речь может идти о реализации проектов, профинансированных иностранными организациями.

О проведении плановой проверки проверяемый оператор персональных данных должен быть извещен не менее, чем за 3 рабочих дня до ее начала, а о проведении внеплановой – не менее чем за сутки (сроки уведомления о начале проверки аналогичны требованиям 294-ФЗ).

Сроки проведения плановой проверки также аналогичны требованиям 294-ФЗ – 20 рабочих дней, в то время как сроки проведения внеплановой проверки Роскомнадзора сокращены до 10 рабочих дней.

Должностные лица при осуществлении государственного контроля и надзора вправе (п. 21 Постановления):

а) во время проведения проверки запрашивать и получать от оператора информацию, документы, в том числе локальные акты, необходимые для реализации органом по контролю и надзору своих полномочий;

б) посещать во время проведения выездной проверки помещения, используемые оператором при осуществлении деятельности по обработке персональных данных, и проводить их обследование;

в) выдавать по итогам проведения проверки предписание об устранении выявленных нарушений;

г) использовать во время проведения проверки или мероприятия по контролю без взаимодействия с оператором принадлежащие органу по контролю и надзору технику и оборудование;

д) получать во время проведения выездной проверки доступ к информационным системам персональных данных оператора в режиме просмотра и выборки информации, необходимой для оценки законности деятельности по обработке персональных данных, в том числе на предмет соответствия содержания, объема, способов обработки и сроков хранения обрабатываемых персональных данных целям их обработки;

е) во время проведения проверки или мероприятия по контролю без взаимодействия с оператором в пределах своей компетенции проверять и оценивать принятые оператором меры по обеспечению выполнения требований;

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ
Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

ж) по итогам проведения проверки или мероприятия по контролю без взаимодействия с операторами принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований;

з) по итогам проведения мероприятия по контролю без взаимодействия с оператором требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

и) по итогам проведения проверки или мероприятия по контролю без взаимодействия с операторами составлять протоколы об административном правонарушении по основаниям и в порядке, которые установлены законодательством Российской Федерации;

к) в рамках проведения выездной проверки обращаться в правоохранительные органы, в том числе в органы прокуратуры, за содействием в предотвращении или пресечении действий, препятствующих осуществлению государственного контроля и надзора должностными лицами, а также в установлении лиц, виновных в нарушении требований;

л) в рамках проведения проверки запрашивать и получать от оператора устные и письменные пояснения по вопросам, относящимся к предмету проверки.

Отдельно следует рассмотреть пункты «б», «д», «и» и «л» пункта 21 Постановления.

В пункте «б» необходимо подчеркнуть, что право Роскомнадзора посещать и обследовать помещения при проведении выездной проверки распространяется только на помещения, используемые оператором при осуществлении деятельности по обработке персональных данных. Перечень таких помещений определяется локальными актами оператора персональных данных.

При анализе пункта «д» необходимо отметить размытость законодательного определения термина «информационная система персональных данных». Так, в соответствии с п. 10 ст. 3 ФЗ «О персональных данных», «*информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств*». Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (п. 2 ст. 2 Федерального закона от 27.07.06 №149-ФЗ «Об информации, информационных технологиях и о защите информации»). В приложении 1 к ГОСТ 34.003-90, информационная технология определяется как приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных. В связи с различиями в определениях, содержащихся в нормативных правовых актах, информационными системами персональных данных можно считать не только электронные базы данных, но и базы данных в «бумажном» виде (например, архивы).

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ
Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

Пункт «и» Постановления противоречит действующему законодательству. В соответствии с данным пунктом, Роскомнадзор наделяется правом составления протоколов об административных нарушениях по итогам мероприятий по контролю без взаимодействия с операторами персональных данных. Как уже отмечалось выше, положения Федерального закона от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» на государственный контроль и надзор за обработкой персональных данных не распространяются, в то время как именно в данном законе закреплен порядок осуществления таких мероприятий. Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных» в статье 23 закрепляет обязанность Правительства РФ установить «порядок организации и проведения **проверок** юридических лиц и индивидуальных предпринимателей, являющихся операторами». Мероприятия по контролю без взаимодействия с юридическими лицами не являются проверками. Более того, в соответствии со ст. 8.3 Федерального закона от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», мероприятия по контролю без взаимодействия с юридическими лицами не могут сами по себе служить основанием для составления протокола об административном правонарушении, а лишь для инициирования назначения внеплановой проверки или вынесения юридическому лицу предостережения о недопустимости нарушения обязательных требований.

В пункте «л» закреплено право Роскомнадзора получать от оператора устные и письменные пояснения. Пояснения вправе давать руководитель организации (как лицо, имеющее право действовать от имени организации без доверенности) и лицо, ответственное за обработку персональных данных (которое должно быть назначено в соответствии со ст. 22.1 ФЗ «О персональных данных»).

В соответствии с п. 25 Постановления, внеплановые документарные проверки не проводятся, т.е. все внеплановые проверки Роскомнадзора в сфере обработки персональных данных могут проводиться исключительно в форме выездных (по месту нахождения оператора персональных данных).

Постановлением устанавливаются сроки предоставления оператором персональных данных информации по запросу Роскомнадзора: в случае проведения документарной проверки – 5 рабочих дней, в случае выездной проверки – 2 рабочих дня.

Акт проверки (с протоколами, справками, пояснениями оператора и иными документами, подтверждающими заключение по результатам проверки) должен быть направлен оператору в 10-дневный срок со дня подписания акта проверки. Вместе с актом проверки оператору может быть выдано предписание об устранении выявленных нарушений, срок исполнения которого не может превышать 6 месяцев.

В случае неисполнения или частичного исполнения ранее выданного предписания может быть проведена внеплановая выездная проверка.

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ

Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

Юристы за гражданское общество
ассоциация

Пункты 50 и 51 Постановления закрепляют право Роскомнадзора направлять в адрес оператора требование о приостановлении деятельности по обработке персональных данных в случае неисполнения ранее выданного предписания об устранении выявленных нарушений. Данные нормы нуждаются в уточнении, т.к. Роскомнадзор должен требовать приостановления деятельности по обработке персональных данных только в отношении обработки персональных данных конкретного субъекта, законность которой оспаривается. Закрепленная в Постановлении размытая формулировка позволяет Роскомнадзору требовать приостановления обработки персональных данных в целом, а не только в отношении конкретного физического лица. Такое требование может парализовать деятельность юридического лица и, вероятно, привести к его ликвидации, поскольку приостановление обработки всех персональных данных не позволит организации осуществлять текущую деятельность, в т.ч. хозяйственную. Действующая редакция пунктов 50 и 51 Постановления необоснованно ограничивает права юридических лиц и является избыточной для целей защиты прав субъектов персональных данных. Само по себе закрепление права Роскомнадзора направлять оператору «требование о приостановлении деятельности по обработке персональных данных» представляется необоснованным при наличии законодательно закрепленного права направлять предостережение о недопустимости нарушения закона.

ФОНД ПРЕЗИДЕНТСКИХ ГРАНТОВ

Материал подготовлен в рамках реализации проекта «Правовая поддержка НКО» с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.