КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ

02 ДЕКАБРЯ 2021

АКТУАЛЬНЫЕ ИЗМЕНЕНИЯ DATA PRIVACY COMPLIANCE В РФ: РАСПРОСТРАНЕНИЕ ДАННЫХ, ОБРАБОТКА БИОМЕТРИИ, КОНТРОЛЬ-НАДЗОРНЫЕ МЕРОПРИЯТИЯ

АЛЕКСЕЙ МУНТЯН, СУЧЕРЕДИТЕЛЬ СООБЩЕСТВА ПРОФЕССИОНАЛОВ ПРИВАТНОСТИ

МОСКВА

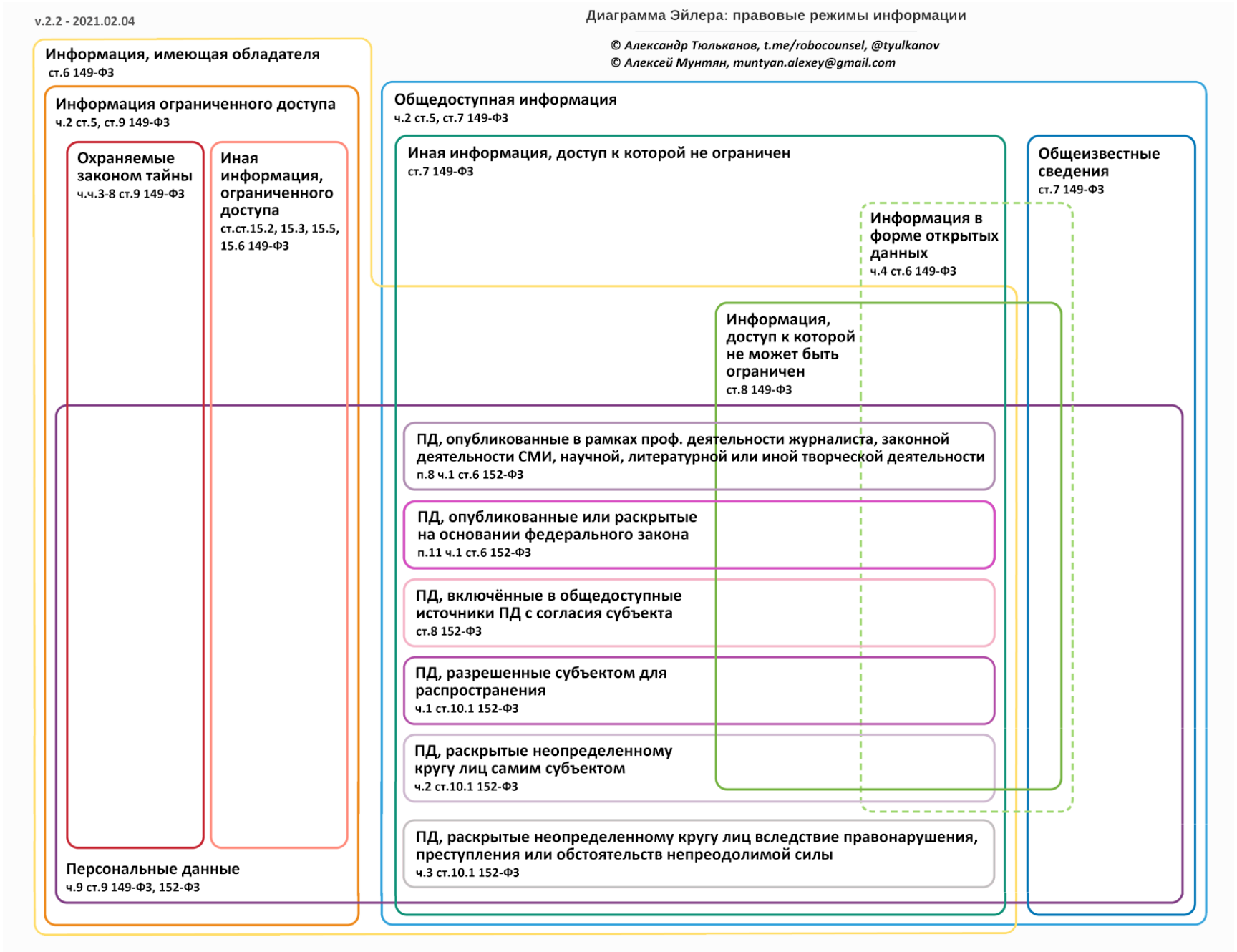
О спикере

Алексей Мунтян

- ***Основатель и CEO в компании Privacy Advocates***
- ***Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru***
- ***Внешний Data Protection Officer в транснациональном холдинге***
- ***Член Совета ТПП РФ по развитию антикоррупционного комплаенса и деловой этики***
- ***Редактор-консультант перевода на русский язык «Руководства по защите персональных данных в ходе гуманитарной деятельности» Международного Комитета Красного Креста***

+7 (903) 762-64-15
muntyan.alexey@gmail.com
facebook.com/alexey.muntyan
linkedin.com/in/alexey-muntyan

3 Правовые режимы информации в РФ



Распространение персональных данных

5 Распространение персональных данных согласно 519-ФЗ

Федеральный закон от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»

- Пункт 10 части 1 статьи 6 152-Ф «О персональных данных» утратил силу, и теперь доступность ПД неограниченному кругу лиц сама по себе больше не является основанием для их законной обработки, альтернативным согласию. Согласно части 2 статьи 10.1 152-ФЗ каждое лицо, осуществляющее распространение или иную обработку (даже доступ - ?!) РПД, обязано иметь соотв. законное основание из части 1 статьи 6 152-ФЗ.

Новые правомочия субъектов персональных данных:

- определение конкретных распространяемых персональных данных по каждой категории данных в согласии;
- запрет на передачу (кроме предоставления доступа) распространяемых персональных данных оператором неограниченному кругу лиц;
- запрет на обработку или установление условий обработки (кроме получения доступа) распространяемых персональных данных неограниченным кругом лиц;
- прекращение передачи (распространение, предоставление, доступ) персональных данных любым лицом – по первому требованию субъекта.

Как определить факт распространения персональных данных

Статья 3. Основные понятия, используемые в 152-ФЗ «О персональных данных»

1.1) персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, **доступ неограниченного круга лиц** к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

5) распространение персональных данных - действия, направленные на **раскрытие** персональных данных **неопределенному кругу лиц**;

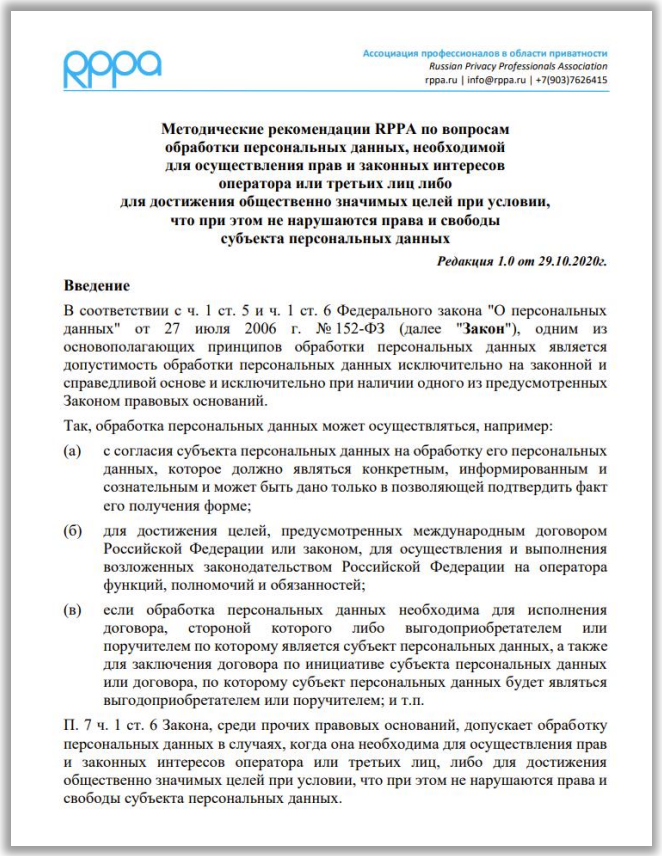
Для квалификации действий с ПД в качестве их распространения требуется выполнение хотя бы одного из нижеописанных условий:

- отсутствие действий, направленных на фактическое ограничение доступа к ПД в отношении любых лиц
- отсутствие возможности достоверно установить круг (перечень) лиц, обладающих или обладавших правом доступа к ПД в определённый момент или период времени

7 Легализация сбора и дальнейшей обработки распространяемых ПД

Трудности выбора и обеспечения правого основания

1) согласие субъекта на обработку его персональных данных;
2) осуществление и выполнение возложенных законодательством на оператора функций, полномочий и обязанностей;
3) заключение и исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект;
4) осуществление прав и законных интересов оператора или третьих лиц.



rppa

Ассоциация профессионалов в области приватности
Russian Privacy Professionals Association
rppa.ru | info@rppa.ru | +7(903)7626415

Методические рекомендации RPPA по вопросам обработки персональных данных, необходимой для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных

Редакция 1.0 от 29.10.2020г.

Введение

В соответствии с ч. 1 ст. 5 и ч. 1 ст. 6 Федерального закона "О персональных данных" от 27 июля 2006 г. № 152-ФЗ (далее "**Закон**"), одним из основополагающих принципов обработки персональных данных является допустимость обработки персональных данных исключительно на законной и справедливой основе и исключительно при наличии одного из предусмотренных Законом правовых оснований.

Так, обработка персональных данных может осуществляться, например:

(а) с согласия субъекта персональных данных на обработку его персональных данных, которое должно являться конкретным, информированным и сознательным и может быть дано только в позволяющей подтвердить факт его получения форме;

(б) для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

(в) если обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем; и т.п.

П. 7 ч. 1 ст. 6 Закона, среди прочих правовых оснований, допускает обработку персональных данных в случаях, когда она необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

Методические рекомендации RPPA по использованию законного интереса как правового основания обработки персональных данных

https://rppa.ru/_media/meroprijatija/2020.10.29_legitimate_interests.pdf

Соблюдение требований о локализации баз с ПД

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить **запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение** персональных данных **граждан Российской Федерации** с использованием баз данных, находящихся на **территории Российской Федерации**…

Базовые принципы реализации требований ч.5 ст.18 152-ФЗ:

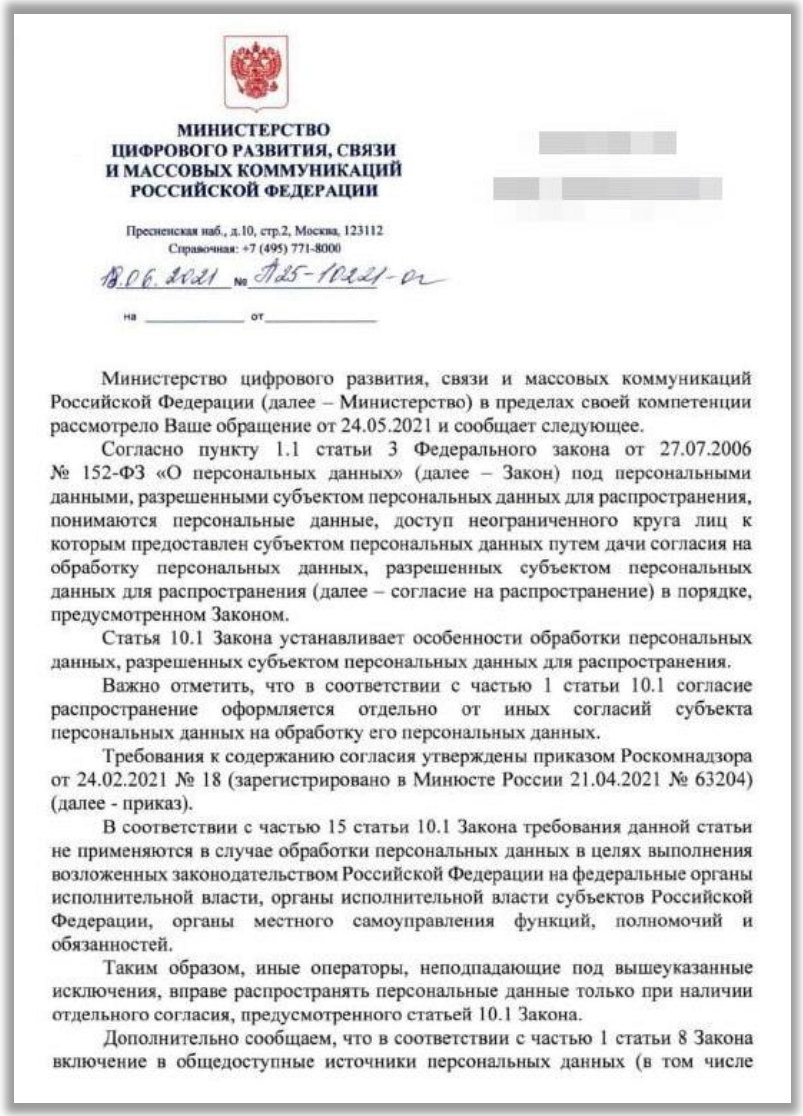
1. Сбор персональных данных граждан РФ, в том числе с территории иностранных государств, должен вестись только в базы данных, находящиеся на территории РФ.

2. Объем и актуальность персональных данных, хранящихся на территории РФ, должны быть равны или превосходить соответствующие показатели в отношении персональных данных, хранящихся за рубежом.

3. Получение новых персональных данных посредством использования (анализа) имеющихся в наличии данных, которые ранее были собраны в базы данных на территории РФ и переданы за рубеж, может производиться посредством зарубежных баз данных и без предварительной локализации в РФ.

8 Письмо Минцифры РФ от 18.06.2021г. по статье 10.1 152-ФЗ

- Косвенно заявлена необходимость получения отдельного согласия на распространение персональных данных по ст.10.1 152-ФЗ даже при одновременном наличии иных оснований для обработки персональных данных по ч.1 ст.6 152-ФЗ.
- Согласие на включение персональных данных в общедоступные источники **в целях информационного обеспечения** (ст.8 152-ФЗ) должно соответствовать требованиям к письменной форме (ч.4 ст.9 152-ФЗ), а не требованиям приказа Роскомнадзора от 24.02.2021 № 18



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Пресненская наб., д.10, стр.2, Москва, 123112
Справочная: +7 (495) 771-8000

18.06.2021 № П25-101221-02

на _____ от _____

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Министерство) в пределах своей компетенции рассмотрело Ваше обращение от 24.05.2021 и сообщает следующее.

Согласно пункту 1.1 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон) под персональными данными, разрешенными субъектом персональных данных для распространения, понимаются персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (далее – согласие на распространение) в порядке, предусмотренном Законом.

Статья 10.1 Закона устанавливает особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.

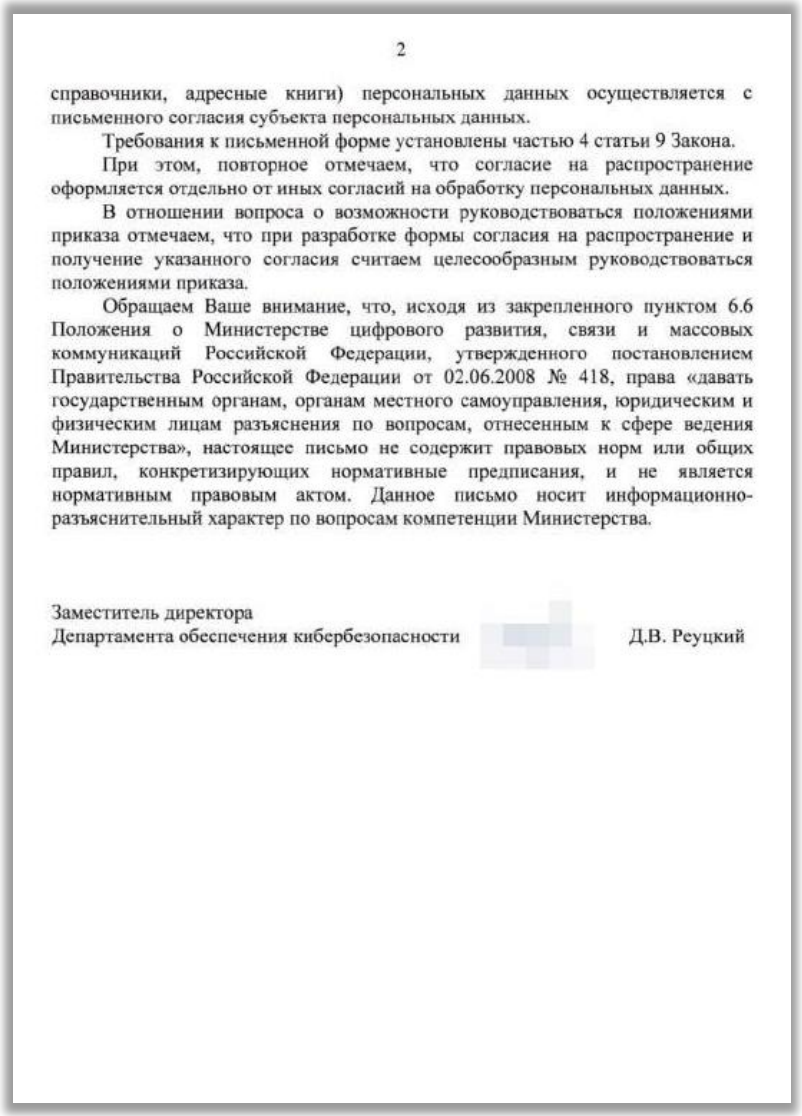
Важно отметить, что в соответствии с частью 1 статьи 10.1 согласие распространение оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Требования к содержанию согласия утверждены приказом Роскомнадзора от 24.02.2021 № 18 (зарегистрировано в Минюсте России 21.04.2021 № 63204) (далее - приказ).

В соответствии с частью 15 статьи 10.1 Закона требования данной статьи не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления функций, полномочий и обязанностей.

Таким образом, иные операторы, неподпадающие под вышеуказанные исключения, вправе распространять персональные данные только при наличии отдельного согласия, предусмотренного статьей 10.1 Закона.

Дополнительно сообщаем, что в соответствии с частью 1 статьи 8 Закона включение в общедоступные источники персональных данных (в том числе



справочники, адресные книги) персональных данных осуществляется с письменного согласия субъекта персональных данных.

Требования к письменной форме установлены частью 4 статьи 9 Закона.

При этом, повторное отмечаем, что согласие на распространение оформляется отдельно от иных согласий на обработку персональных данных.

В отношении вопроса о возможности руководствоваться положениями приказа отмечаем, что при разработке формы согласия на распространение и получение указанного согласия считаем целесообразным руководствоваться положениями приказа.

Обращаем Ваше внимание, что, исходя из закрепленного пунктом 6.6 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 02.06.2008 № 418, права «давать государственным органам, органам местного самоуправления, юридическим и физическим лицам разъяснения по вопросам, отнесенным к сфере ведения Министерства», настоящее письмо не содержит правовых норм или общих правил, конкретизирующих нормативные предписания, и не является нормативным правовым актом. Данное письмо носит информационно-разъяснительный характер по вопросам компетенции Министерства.

Заместитель директора
Департамента обеспечения кибербезопасности Д.В. Реуцкий

9 Требования к содержанию согласия на распространение ПД

Приказ Роскомнадзора от 24.02.2021 № 18

1) фамилия, имя, отчество субъекта персональных данных

2) контактная информация субъекта персональных данных

3) сведения об операторе - организации, физическом лице или гражданине, являющимся индивидуальным предпринимателем

4) сведения об информационных ресурсах оператора (**адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы**), посредством которых будет осуществляться распространение персональных данных

5) цель (цели) обработки персональных данных

6) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных

7) категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов

8) условия, при которых полученные персональные данные могут передаваться оператором

9) срок действия согласия

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)
Китайгородский проезд, д. 7, стр. 2, Москва, 109992
тел./факс: (495) 983-33-93; http://rkn.gov.ru/

Мунтян А.В.

17.09.2021 № 08-61656
На
О результатах рассмотрения обращения
Мунтян А.В.

Уважаемый Алексей Витальевич!

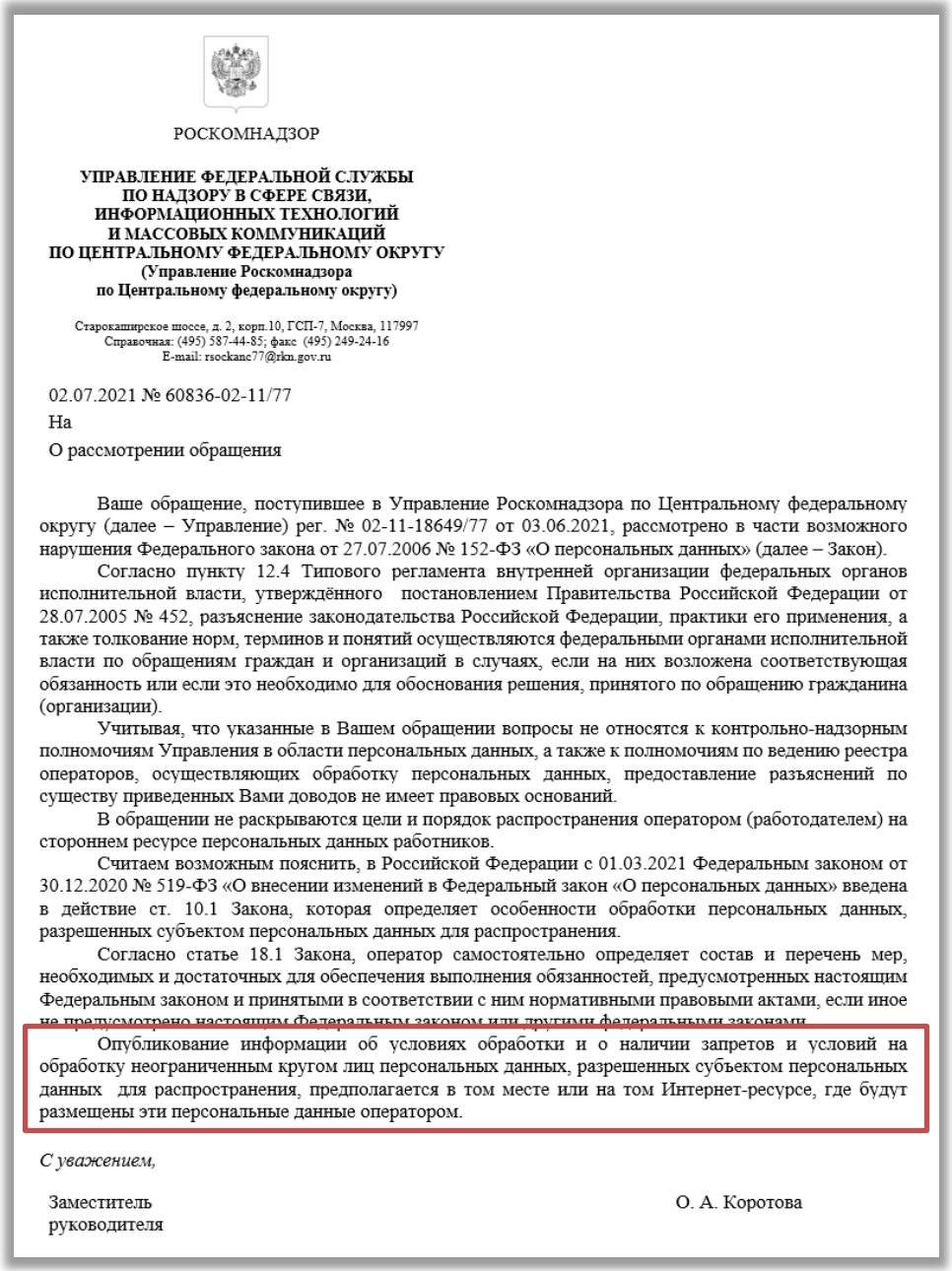
Роскомнадзор рассмотрел Ваше обращение от 20.08.2021 № 02-11-16951 и сообщает, что правовая конструкция Требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждённых приказом Роскомнадзора от 24.02.2021 № 18, предполагает размещение персональных данных на интернет-ресурсах оператора.

В случае, если предполагается распространение персональных данных на иных интернет-ресурсах, не принадлежащих оператору, получившему согласие субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения (далее – согласие), указанное согласие также должно быть получено лицом, являющимся владельцем сторонних интернет-ресурсов.

Привлечение третьих лиц для осуществления распространения персональных данных допускается при условии, что указанная длительность будет осуществляться третьим лицом от имени оператора, на информационных интернет-ресурсах, принадлежащих оператору, указанных в согласии, предоставленному оператору, а также с соблюдением иных требований ч. 3 ст. 6 и ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Начальник Управления по защите
прав субъектов персональных данных Ю.Е. Контемиров

Не для всех способов распространения ПД можно указать адрес информационного ресурса



РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
(Управление Роскомнадзора по Центральному федеральному округу)

Старокаширское шоссе, д. 2, корп.10, ГСП-7, Москва, 117997
Справочная: (495) 587-44-85; факс (495) 249-24-16
E-mail: rsockanc77@rkn.gov.ru

02.07.2021 № 60836-02-11/77
На
О рассмотрении обращения

Ваше обращение, поступившее в Управление Роскомнадзора по Центральному федеральному округу (далее – Управление) рег. № 02-11-18649/77 от 03.06.2021, рассмотрено в части возможного нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон).

Согласно пункту 12.4 Типового регламента внутренней организации федеральных органов исполнительной власти, утверждённого постановлением Правительства Российской Федерации от 28.07.2005 № 452, разъяснение законодательства Российской Федерации, практики его применения, а также толкование норм, терминов и понятий осуществляются федеральными органами исполнительной власти по обращениям граждан и организаций в случаях, если на них возложена соответствующая обязанность или если это необходимо для обоснования решения, принятого по обращению гражданина (организации).

Учитывая, что указанные в Вашем обращении вопросы не относятся к контрольно-надзорным полномочиям Управления в области персональных данных, а также к полномочиям по ведению реестра операторов, осуществляющих обработку персональных данных, предоставление разъяснений по существу приведенных Вами доводов не имеет правовых оснований.

В обращении не раскрываются цели и порядок распространения оператором (работодателем) на стороннем ресурсе персональных данных работников.

Считаем возможным пояснить, в Российской Федерации с 01.03.2021 Федеральным законом от 30.12.2020 № 519-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» введена в действие ст. 10.1 Закона, которая определяет особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения.

Согласно статье 18.1 Закона, оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами.

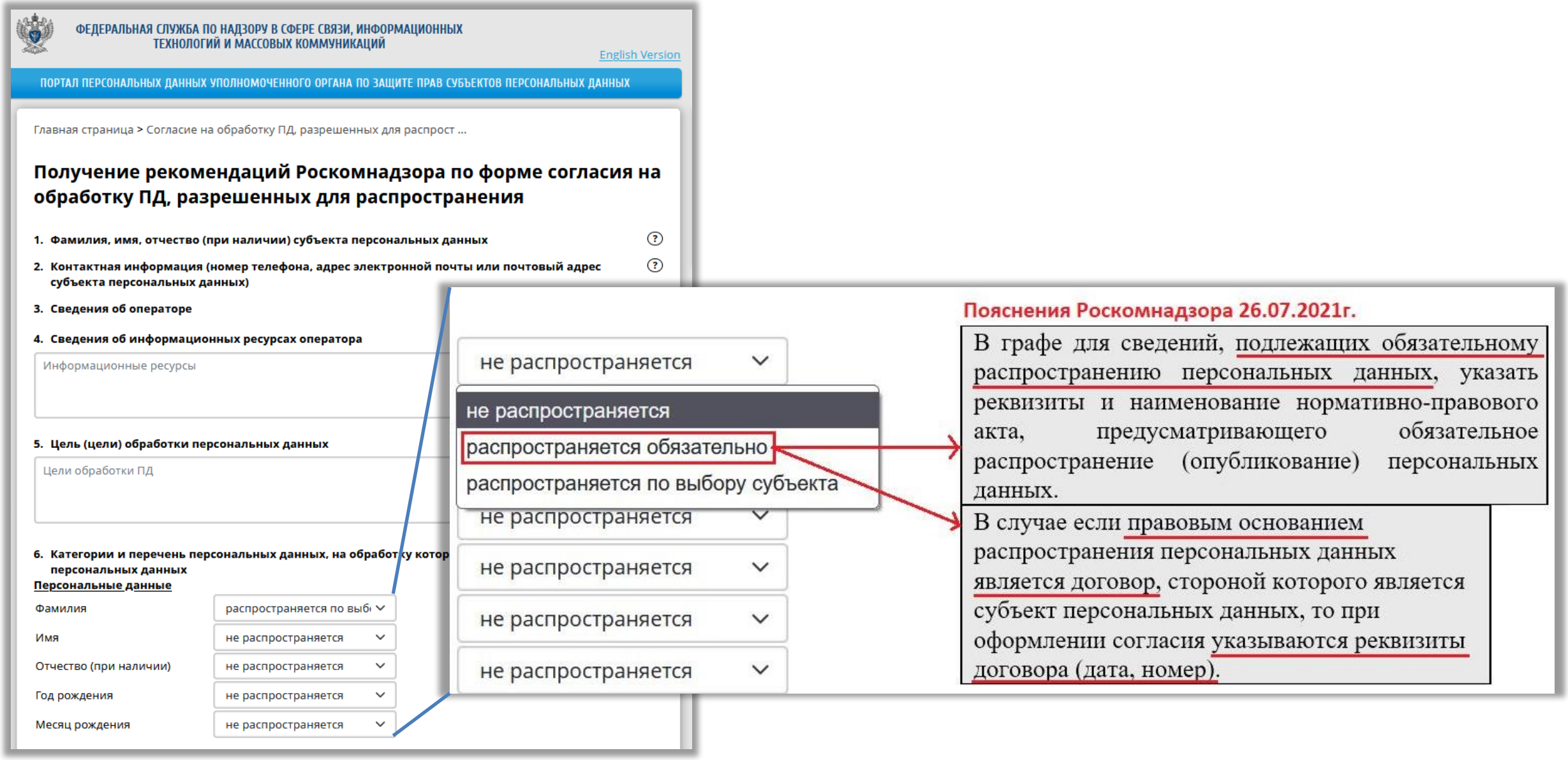
Опубликование информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения, предполагается в том месте или на том Интернет-ресурсе, где будут размещены эти персональные данные оператором.

С уважением,

Заместитель руководителя О. А. Коротова

- размещение в открытом доступе на различных внешних информационных ресурсах и глобальных электронных порталах, сайтах в сети «Интернет», мобильных приложениях
- размещение в открытом доступе в системах мгновенного обмена сообщениями (в том числе WhatsApp, Viber, Telegram) и (или) социальных сетях (в том числе Facebook, Twitter, Instagram, ВКонтакте, Одноклассники, Мой Мир)
- указание в общедоступных информационных (в том числе электронных) стендах, киосках и терминалах
- публичная демонстрации в рамках потоковой видеотрансляции в режиме реального времени посредством видеостриминговых сервисов (например, YouTube, Livestream, Periscope) и (или) посредством платформ для организации видеоконференций/веб-мероприятий (например, Zoom) в сети «Интернет»
- публикация в периодических изданиях, средствах массовой информации
- распространение сообщения радио- или телепередачи, содержащих персональные данные, посредством продажи либо иного отчуждения оригинала или экземпляров записи сообщения радио- или телепередачи, сообщения в эфир (в том числе через спутник) или по кабелю, доведения до всеобщего сведения, а также посредством публичного исполнения
- рассылка информационных/сервисных/рекламных сообщений по электронной почте и (или) системам мгновенного обмена сообщениями в адрес любых потенциально заинтересованных лиц
- внесение в общедоступные справочные и адресные книги
- сообщение любым заинтересованным лицам (неопределенному/неограниченному кругу лиц)
- размещение информационных надписей в общедоступных местах на объектах недвижимости – в случае возложения на работника ответственности за пожарную безопасность, защиту от чрезвычайных ситуаций и (или) хранение аптечек для оказания первой медицинской помощи
- открытое ношение работником своего служебного пропуска (ID-карты) на территории объектов недвижимости
- внесение в общедоступные реестры выданных и аннулированных сертификатов ключей проверки электронных подписей

Рекомендации Роскомнадзора по форме согласия на распространение ПД, полученные автором 26.07.2021г. в рамках сервиса pd.rkn.gov.ru/soglasiya/maket

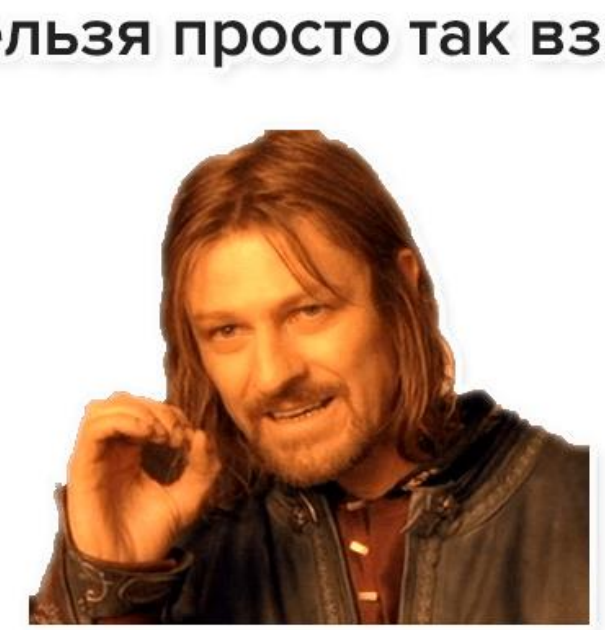


Обработка биометрических персональных данных

Обработка биометрических персональных данных согласно 479-ФЗ

Федеральный закон от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»

- В информационных системах организаций финансового рынка, иных организаций, индивидуальных предпринимателей, нотариусов сбор и обработка используемых в целях идентификации и (или) аутентификации биометрических персональных данных, за исключением указанных в частях 18.18 и 18.20 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ случаев, а также за исключением сбора и обработки биометрических персональных данных для размещения в единой биометрической системе в соответствии с федеральными законами, **запрещены**.



и начать обработку биометрических персональных данных

Постановление Правительства РФ от 23.10.2021 № 1815

Можно осуществлять идентификацию и/или аутентификацию с помощью биометрических данных:

1. водителей легкового такси;
2. водителей транспортных средств в рамках каршеринга;
3. посетителей территории организаций;
4. участников собрания гражданско-правового сообщества.

Некоторые из подзаконных актов к 479-ФЗ

Постановления Правительства РФ:

- 30.09.2021 № 1657 «Об утверждении Правил осуществления контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями и нотариусами организационных и технических мер по обеспечению безопасности биометрических персональных данных и использованием средств защиты информации»
- 11.10.2021 № 1729 «Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере идентификации и (или) аутентификации»
- 15.10.2021 № 1754 «Об утверждении требований к проверке простой электронной подписи, которой согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий»
- 20.10.2021 № 1799 2Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц»
- 23.10.2021 № 1815 «Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц»

Приказы Минцифры России:

- 27.08.2021 № 896 «Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающей услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц»
- 01.09.2021 № 902 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц»
- 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»

Идентификация, аутентификация и установление личности субъекта персональных данных

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Пресненская наб., д.10, стр.2, г. Москва, 123112
Справочная: +7 (495) 771-8000

05.10.2021 № П24-17679-ОГ

на №_____от_____

Мунтяну А.В.

О рассмотрении обращения

Уважаемый Алексей Витальевич!

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации рассмотрело Ваше обращение, зарегистрированное от 23.08.2021 г. № М-17018, и в рамках компетенции, сообщает следующее.

В соответствии со статьей 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149):

идентификация - совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такого лица;

аутентификация - совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным.

Таким образом, мероприятия по идентификации, аутентификации и установлению личности направлены на определение физического лица.

В части права организаций и индивидуальных предпринимателей на осуществление обработки биометрических персональных данных, сообщаем, что в соответствии с частью 18.17 статьи 14.1 ФЗ № 149 (в редакции Федерального закона от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации») в информационных системах организаций финансового рынка, иных организаций, индивидуальных предпринимателей, нотариусов сбор и обработка используемых в целях идентификации и (или) аутентификации биометрических персональных данных, за исключением указанных в частях 18.18 и 18.20 статьи 14.1 ФЗ № 149 (в редакции Федерального закона от 29.12.2020 № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации») случаев, а также за исключением сбора и обработки биометрических персональных данных для размещения в единой биометрической системе в соответствии с федеральными законами, запрещены.

Заместитель директора Департамента
развития технологий цифровой идентификации Ю.О. Шабанов

Государственная контрольно-надзорная деятельность

Постановление Правительства РФ от 29.06.2021 № 1046

С **1 июля 2021г. п**ри осуществлении федерального государственного контроля (надзора) за обработкой персональных данных применяется система оценки и управления рисками.
Надзорный орган при осуществлении государственного контроля (надзора) относит поднадзорные объекты к одной из пяти категорий риска причинения вреда (ущерба).

Группы тяжести			
А	Б	В	Г
Спецкатегории	обработка в целях, отличных от заявленных на этапе сбора	ПДн близких родственников	обработка ПДн, полученных из общедоступных источников
БПДн	ПДн несовершенно-летних за искл. по закону		обработка ПДн без уведомления Роскомнадзора
-	>20000	1000...20000	<1000
сбор в БД за пределами РФ	сбор через Интернет и через сервисы за рубежом		
Трансграничка в неадекватные страны		Трансграничка в страны из перечня Роскомнадзора	Трансграничка на территорию стран-членов СЕ
передача 3-м лицам обезличенных* ПДн		обезличивание* пдн, обработка обезличенных* ПДн, без передачи 3-м лицам	

	Группа вероятности			
	1	2	3	4
КоАП, статья 13.11	ч. 1.1, 2.1, 5.1, 9	ч. 1, 2, 5, 6, 8	ч. 4, 7	-
прим:	Повторное нарушение	Нарушение	Нарушение	-
В течение последних 2 лет оператору Роскомнадзором выдавались				
предписание	Да	Да	Да	-
требование	Да	Да	Да	-
предупреждение	Да	Да	Да	-
В течение 3 календарных лет до принятия решения об отнесении к категории риска, вступили в законную силу решения о назначении административного наказания:				
назначении адм. наказания	Да	Да	Да	-

Группа вероятности / Группа тяжести	1	2	3	4
А	Высокий	Значительный	Значительный	Средний
Б	Высокий	Средний	Средний	Низкий
В	Средний	Средний	Умеренный	Низкий
Г	Умеренный	Умеренный	Низкий	Низкий

*ПДн, полученные в результате обезличивания, с использованием методов обезличивания, утвержденных в соответствии с законодательством Российской Федерации в области персональных данных

Плановые контрольные (надзорные) мероприятия и профилактика рисков

Под оператором понимается контролируемое лицо, самостоятельно или совместно с другими контролируемыми лицами организующее и (или) осуществляющее обработку персональных данных, **в том числе на основании поручения**, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

		Плановые контрольные (надзорные) мероприятия				Профилактика рисков
		Инспекционный визит	**Документарная проверка**	**Выездная проверка**	**Периодичность, лет**	**Обязательный профилактический визит**
	Уведомление	Без уведомления	-	не позднее 24 часов до начала	-	не позднее 5 рабочих дней
	Макс. срок проведения, рабочих дней	1	10	10	-	5
	Возможность отказаться от мероприятия	Нет	Нет	Нет	-	Да (за 3 рабочих дня)
Риск	Высокий	Да	Нет	Да	2	Да
	Значительный	Да	Нет	Да	3	Да
	Средний	Да	Да	Да	4	Нет
	Умеренный	Нет	Да	Да	6	Нет
	Низкий	Нет	Нет	Нет	Нет	Нет
	Лица, начинающие деятельность					Да

Проект изменений в Постановление от 29.06.2021 № 1046

Утверждено
постановлением Правительства
Российской Федерации
от «___» _____ 2021 г. N _____

**ИЗМЕНЕНИЕ,
КОТОРОЕ ВНОСИТСЯ В ПОЛОЖЕНИЕ О ФЕДЕРАЛЬНОМ
ГОСУДАРСТВЕННОМ КОНТРОЛЕ (НАДЗОРЕ)
ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Дополнить разделом VIII следующего содержания:
"VIII. Ключевые показатели федерального контроля
и их целевые значения"

Наименование ключевого показателя федерального контроля	Целевые значения				
	Период				
	2022	2023	2024	2025	2026
Доля контролируемых лиц, в деятельности которых по итогам плановых проверок выявлены нарушения законодательства Российской Федерации в области персональных данных от общего числа контролируемых лиц в отношении которых были проведены плановые проверки (%)	90	89	88	87	86

Утверждено
постановлением Правительства
Российской Федерации
от «___»_____ 2021 г. N _____

**ИЗМЕНЕНИЕ,
КОТОРОЕ ВНОСИТСЯ В ПОЛОЖЕНИЕ О ФЕДЕРАЛЬНОМ
ГОСУДАРСТВЕННОМ КОНТРОЛЕ (НАДЗОРЕ)
ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Дополнить разделом VIII следующего содержания:
"VIII. Ключевые показатели федерального контроля
и их целевые значения

Наименование ключевого показателя федерального контроля	Целевые значения ключевого показателя (не более указанной величины ключевого показателя)				
	Период				
	2022	2023	2024	2025	2026
Доля контролируемых лиц, категория риска которых повышена в отчетном периоде по причинам, не связанным с изменением группы тяжести указанных контролируемых лиц, к общему числу контролируемых лиц	5%	5%	4%	4%	3%

https://regulation.gov.ru/projects#npa=121034

ФГУП «ГРЧЦ»: автоматизированная система мониторинга нарушений прав субъектов персональных данных в сети «Интернет»

Функционал системы:

1. поиск ресурсов со сбором и распространением ПД, оценивать соблюдение законодательства;
2. проверка информационных ресурсов, на которые пожаловались, и ресурсов в плане мероприятий систематического наблюдения Роскомнадзора;
3. интеграция с формой обращений граждан, расположенной на сайте Роскомнадзора;
4. мониторинг 500 000 информационных ресурсов в сети «Интернет» ежегодно, не менее 15 000 еженедельно, по ключевым словам, например: «согласие», «обработка», «подтверждаю», «персональный», «имя», «фамилия», «скачать базу», «продам базу», «база данных», «персональный», «имя», «фамилия» и т.д.;
5. модуль по доказательной базе.

Ранжирование выявляемых нарушений:

1. нет согласия на обработку ПД
2. нет документа, определяющего политику в отношении обработки ПД (Политики ПД)
3. несоответствие объема, собираемого формой, Политике ПД
4. наличие ссылок на сторонние формы сбора ПД
5. осуществление сбора ПД граждан РФ при нахождении хостинг-провайдера за границами Российской Федерации
6. отсутствие информации об осуществлении трансграничной передачи ПД в Политике ПД (при наличии трансграничной передачи)
7. сбор метрической информации в отсутствие указания об этом в Политике ПД
8. отсутствие или некорректное указание срока (условия) прекращения обработки персональных данных в Политике ПД.

Приоритетность мониторинга по видам деятельности операторов:

1. финансово-кредитные организации (банки, негосударственные пенсионные фонды, микрофинансовые организации, небанковские платежные компании и т. д.);
2. страховые компании;
3. коллекторские агентства;
4. социальные сети;
5. операторы связи;
6. «Интернет»-магазины;
7. транспортные компании, и компании, осуществляющие перевозку пассажиров;
8. почтовые сервисы;
9. медицинские учреждения;
10. образовательные учреждения;
11. организации в сфере ЖКХ, управляющие компании;
12. многофункциональные центры предоставления государственных и муниципальных услуг;
13. государственные и муниципальные органы власти.

https://zakupki.gov.ru/223/purchase/public/purchase/info/common-info.html?lotId=14448431&purchaseId=10912751&purchaseMethodType=KESMBO

Минцифры России: мониторинг утечек персональных данных в сети Интернет

Ручной и автоматизированный мониторинг открытых и закрытых источников (darknet) в сети Интернет:

- Форумы киберкриминальной тематики как с открытым, так и с ограниченным доступом (в том числе требующие оплаты для регистрации учетной записи);
- Telegram-каналы и чаты киберкриминальной тематики;
- Блоги и веб-сайты злоумышленников, распространяющих вредоносное ПО (программы-вымогатели);
- Новостные ресурсы (включая комментарии пользователей);
- Форумы IT-тематики;
- Telegram-каналы IT-тематики;
- Веб-приложения для обмена текстом и исходным кодом (такие как Pastebin и GitHub).

Сбор и анализ сообщений о факте наличия утечки данных из ИС органов государственной власти, операторов связи и государственных компаний, обрабатывающих ПД граждан РФ:

- о продаже ПД или баз персональных данных;
- о покупке ПД или баз ПД;
- любые другие сообщения, свидетельствующие об указанных фактах.

https://zakupki.gov.ru/epz/order/notice/ea44/view/common-info.html?regNumber=0173100007521000114

Благодарю за ваше внимание

Алексей Мунтян

Основатель и CEO в компании Privacy Advocates

Соучредитель и член Правления в Russian Privacy Professionals Association - RPPA.ru

+7 (903) 762-64-15
muntyan.alexey@gmail.com
facebook.com/alexey.muntyan
linkedin.com/in/alexey-muntyan