

Оператор персональных данных

Определение целей действий с персональными данными, состава подлежащих обработке персональных данных, конкретного перечня действий с персональными данными, а также принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных, возложено на операторов персональных данных.

В соответствии п. 2 ст. 3 Закона о персональных данных оператор – это государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Согласно статье 22 Закона о персональных данных оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, которым согласно абзацу 2 пункта 1 Постановления Правительства РФ от 16.03.2009 N 228 является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом, в частности в качестве уполномоченного лица в случае, если оператором является юридическое лицо, может выступать руководитель организации или иное лицо, действующее от имени организации по доверенности, а уведомление от имени физического лица может быть подписано им самостоятельно либо уполномоченным им лицом по доверенности.

Уведомление следует направлять в территориальный орган Роскомнадзора по месту регистрации оператора в налоговом органе.

Форма уведомления установлена ч. 3 ст. 22 Закона о персональных данных, в частности в уведомлении необходимо указывать:

- наименование (фамилию, имя, отчество), адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

описание мер, предусмотренных ст. 18.1 и 19 Закона о персональных данных, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

фамилию, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

дату начала обработки персональных данных;

срок или условие прекращения обработки персональных данных ;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения о месте нахождения базы данных информации, содержащей персональные данные граждан РФ;

сведения об обеспечении безопасности персональных данных в соответствии с Требованиями к защите персональных данных, установленными Постановлением Правительства РФ от 01.11.2012 N 1119.

Приказом Роскомнадзора от 30.05.2017 N 94 утверждены Методические рекомендации, которыми целесообразно руководствоваться при направлении уведомления. Согласно п. 3.1.13 Рекомендаций уведомление рекомендуется оформлять на бланке организации, осуществляющей обработку персональных данных по форме, определенной Приложением 1 к Рекомендациям.

Обращаем внимание, что в вопросах ведения реестра операторов, осуществляющих обработку персональных данных, Роскомнадзор и территориальные органы руководствуются вышеуказанными методическими рекомендациями.

Роскомнадзор в течение 30 дней с даты поступления уведомления об обработке персональных данных вносит сведения в реестр операторов персональных данных.

Если будут представлены неполные или недостоверные сведения, в реестр операторов персональных данных они не вносятся, а в адрес оператора персональных данных направляется письмо, содержащее перечень недостающих сведений и предложение их предоставить. Уточненные по запросу сведения рекомендуется сообщить в течение 30 дней со дня получения такого запроса, а если в течение 30 дней со дня получения запроса оператор персональных данных не представил уточненные сведения, то по истечении указанного срока уведомление с неполными или недостоверными сведениями возвращается оператору без внесения сведений о нем в реестр операторов персональных данных.

В соответствии с частью 7 статьи 22 Закона о персональных данных если предоставленные для внесения в реестр операторов сведения будут изменены либо будет прекращена обработка персональных данных, то оператор обязан уведомить об этом Роскомнадзор в течение 10 рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Информация о внесении сведений об операторе в реестр операторов размещается на официальном сайте и Портале персональных данных в общедоступной форме (за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке), и любое лицо может ознакомиться с ней на Портале персональных данных по адресу <http://pd.rkn.gov.ru>.

Не требуется уведомлять Роскомнадзор об обработке следующих персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных (при этом такие персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных);
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством РФ, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;
- сделанных субъектом персональных данных общедоступными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации;

- обрабатываемых в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

При этом операторами персональных данных юридические или физические лица являются независимо от включения в реестр операторов персональных данных.

Согласно ч. 3 ст. 6 Закона о персональных данных оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных. Если обработка персональных данных поручена третьему лицу в силу ч. 3 ст. 6 Закона о персональных данных, с оператора не снимаются обязанности уведомлять Роскомнадзор об обработке персональных данных, поскольку ст. 22 Закона о персональных данных, регулирующая вопросы уведомления об обработке персональных данных, таких исключений не содержит. В тоже время, в соответствии с ч. 5 ст. 6 Закона о персональных данных в случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор, а лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных.

Поручение оператора третьему лицу на обработку персональных данных должно содержать:

- перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом;
- цели обработки;
- обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;
- требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Закона о персональных данных.

При этом лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку

персональных данных по поручению оператора, несет ответственность перед оператором.

При сборе персональных данных оператор должен исполнять следующие обязанности.

Во-первых, субъект персональных данных имеет право на получение информации от оператора персональных данных, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

Следует обратить внимание, что указанный перечень сведений предоставляется субъекту персональных данных или его представителю оператором персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя.

При этом, запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

Согласно ст. 20 Закона о персональных данных оператор персональных данных обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя. Сведения должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Субъект персональных данных вправе требовать от организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Во-вторых, оператор персональных данных обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные. Если предоставление персональных данных является обязательным, то оператор должен разъяснить последствия непредоставления таких данных, например, отказ в предоставлении персональных данных работодателю при заключении трудового договора повлечет невозможность заключения такого договора.

В-третьих, при обработке персональных данных граждан РФ использовать базы данных, находящиеся на территории Российской Федерации. При записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), извлечении персональных данных граждан РФ, в том числе при сборе персональных данных посредством Интернета, должны обязательно использоваться базы данных, находящиеся на территории Российской Федерации, за исключением специально предусмотренных случаев, указанных в части 5 статьи 18 Закона о персональных данных .

В-четвертых, принимать меры, необходимые и достаточные для обеспечения выполнения возложенных на оператора обязанностей.

Оператор персональных данных обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами .

К таким мерам могут, в частности, в организациях относиться:

Назначение организацией из числа сотрудников или привлеченной организации лица, ответственного за организацию обработки персональных данных. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением организацией и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Издание организацией документов, определяющих политику организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Постановлением Правительства РФ от 01.11.2012 N 1119 утверждены Требования к защите персональных данных при их обработке в информационных системах персональных данных, определяющие критерии уровней защищенности и требования к защите, а состав и содержание необходимых мер определяются в соответствии с Приказами ФСТЭК России от 18.02.2013 N 21 "Об утверждении Составов и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и ФСБ России от 10.07.2014 N 378 "Об утверждении Составов и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

Примерный перечень локальных актов оператора персональных данных включает:

- Политику оператора персональных данных в отношении обработки персональных данных;
- Положение об обработке и защите персональных данных;
- Обязательство о соблюдении режима конфиденциальности персональных данных;
- Перечень должностей сотрудников, имеющих доступ к персональным данным;

Приказ о назначении лица, ответственного за организацию обработки персональных данных;

- Приказ об утверждении мест хранения материальных носителей персональных данных.

Организация обязана опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему ее политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

Если оператор персональных данных осуществляет сбор персональных данных с использованием информационно-телекоммуникационных сетей, он обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

Если обработка персональных данных осуществляется не в Интернете, то доступ к политике в отношении обработки персональных данных может быть обеспечен любым доступным способом.

В соответствии с письмом Минобрнауки России от 14 мая 2018 года N 08-1184 общеобразовательные организации размещают локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся, в том числе по вопросам обработки персональных данных, в разделе «Информационная безопасность» на своих официальных сайтах в сети «Интернет».

В примерную форму Политики организации в отношении обработки персональных данных рекомендуется включить следующие структурные компоненты:

Общие положения. В указанном разделе рекомендуется описать назначение Политики, а также включить основные понятия, используемые в ней (обработка персональных данных, оператор, субъект персональных данных, конфиденциальность персональных данных и т.д.), перечислить основные права и обязанности оператора и субъекта (ов) персональных данных.

Цели сбора персональных данных. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Цели обработки персональных данных могут происходить, в том числе, из анализа правовых актов, регламентирующих деятельность организации, целей фактически осуществляемой организацией деятельности, а также деятельности, которая предусмотрена учредительными документами организации, и конкретных процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

Правовые основания обработки персональных данных. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми организация осуществляет обработку персональных данных. В качестве правового основания обработки персональных данных могут быть указаны:

о федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью организации ;

о уставные документы организации;

о договоры, заключаемые между организацией и субъектом персональных данных (учащимся, его законными представителями);

о согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям организации).

Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. К категориям субъектов персональных данных могут быть отнесены, в том числе:

-о работники организации, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;

-о учащиеся, их законные представители;

-о представители/работники клиентов и образовательной организации (юридических лиц).

В рамках каждой из категорий субъектов и применительно к конкретным целям рекомендуется перечислить все обрабатываемые организацией персональные данные, а также, если применимо, отдельно описать все случаи обработки специальных категорий персональных данных.

Порядок и условия обработки персональных данных. В данном разделе рекомендуется указывать перечень действий, совершаемых организацией с персональными данными субъектов, а также используемые оператором способы обработки персональных данных и сроки обработки персональных данных.

В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных рекомендуется указывать условия передачи персональных данных в адрес третьих лиц (например, наличие договора поручения на обработку персональных данных), цели осуществляемой передачи, объем передаваемых персональных данных, перечень действий по их обработке, способы и иные условия обработки, включая требования к защите обрабатываемых персональных данных.

Кроме того, оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

Также рекомендуется указывать сведения о соблюдении требований конфиденциальности персональных данных, установленных ст. 7 Закона о персональных данных, а также информацию о принятии оператором мер, предусмотренных ч. 2 ст. 18.1, ч. 1 ст. 19 Закона о персональных данных.

Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

Хранение персональных данных рекомендуется осуществлять в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Рекомендуется указывать сроки хранения персональных данных и иные условия хранения персональных данных, в том числе, при обработке персональных данных без использования средств автоматизации.

Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации оператором, а обработка должна быть прекращена, соответственно. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

-о иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

-о оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

-о иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

Оператор обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

Рекомендуется включить в Политику регламент(ы) реагирования на запросы(или) обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным, а также соответствующие формы запросов и (или) обращений.

Соблюдение условий обработки персональных данных, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором, в том числе принимается документ, подтверждающий утверждение оператором перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ, и конкретных мест хранения персональных данных (материальных носителей).

Ознакомление работников организации, 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, и (или) обучение указанных работников.

Оператором должен быть:

- оформлен лист ознакомления работников с положениями законодательства о персональных данных и документами оператора по вопросам обработки персональных данных;
- включены положения законодательства в области персональных данных в трудовые договоры с работниками, должностные регламенты и иные локальные акты оператора;
- организовано прохождение соответствующих образовательных программ.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором) должны быть проинформированы о:

- факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации,
- категориях обрабатываемых персональных данных,
- 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).

В-пятых, в соответствии с частью 4 ст. 20 Закона о персональных данных представить по запросу Роскомнадзора в течение 30 дней с даты получения такого запроса документы и локальные акты, определяющие политику и порядок обработки персональных данных, а также подтверждение принятия необходимых мер по защите персональных данных.