**Примерный перечень документов, которые должен иметь оператор персональных данных во исполнение требований законодательства в области персональных данных**

Операторам персональных данных: примерный перечень документов для надлежащей обработки персональных данных

Согласно ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) оператор персональных данных – это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку таких данных, а также определяющие цели их обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с данными.

Общим признаком оператора персональных данных для всех организаций является обработка персональных данных работников. Организации, оказывающие услуги населению, обрабатывают еще и персональные данные клиентов. То есть, по сути, операторами персональных данных являются все без исключения организации.

Зачастую многие операторы персональных данных так или иначе сталкиваются с необходимостью подготовки пакета документов в сфере защиты персональных данных. Это может происходить в разных случаях. Некоторые операторы готовят документы при открытии или расширении собственного бизнеса. Кто-то – из-за надвигающейся проверки Роскомнадзора. В любом случае каждому оператору необходимо знать о существовании примерного перечня документов для надлежащей обработки персональных данных.

**1. Документ, определяющий политику оператора в отношении обработки персональных данных, и подтверждение ознакомления с ним работников оператора**

В соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) к **обязанностям**оператора персональных данных относится, в том числе издание документа, определяющего политику оператора в отношении обработки персональных данных, что позволяет обеспечить реализацию принципов законности, конфиденциальности и безопасности информации.

Многие организации этот документ так и называют – «Политика в отношении обработки персональных данных». Ранее он составлялся в произвольной форме, но в августе 2017 года **Роскомнадзор разработал Рекомендации** по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Законом № 152-ФЗ. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к указанному документу и к сведениям о реализуемых требованиях к защите персональных данных.

Согласно ч.1 ст.18.1 Закона № 152-ФЗ, оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, может относиться ознакомление работников оператора, 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.

**2. Отдельные локальные акты по вопросам обработки таких данных, документы об ознакомлении с ними работников оператора.**

Помимо Политики у оператора должны быть **отдельные локальные акты** по вопросам обработки таких данных и локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий нарушений: **например,**

* различные положения (об обработке персональных данных, об обеспечении безопасности персональных данных и т. п.),
* перечни (должностей и лиц, допущенных к обработке персональных данных, применяемых средств защиты и др.),
* инструкции и регламенты.

Согласно ч.4 ст.22.1 Закона № 152-ФЗ, лицо, ответственное за организацию обработки персональных данных, в частности, обязано доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

**3. Уведомление об обработке персональных данных (изменения в уведомление об обработке персональных данных).**

В соответствии со ст.22 Закона № 152-ФЗ, оператор до начала обработки персональных данных **обязан подготовить уведомление**об обработке персональных данных (и при необходимости, изменения в уведомление об обработке персональных данных) и **направить**данное уведомление о своем намерении осуществлять обработку персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

**Исключения (когда оператор имеет право обрабатывать персональные данные без уведомления уполномоченного органа), в частности, установлены в отношении персональных данных:**
• обрабатываемых в соответствии с трудовым законодательством;
• полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если они не распространяются, не предоставляются третьим лицам без согласия субъекта данных, 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 объединением или организацией, 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 в соответствии с федеральными законами или иными нормативными правовыми актами РФ, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;
• обрабатываемых в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

**4. Приказ (распоряжение) о назначении ответственного за организацию обработки персональных данных у оператора.**

В соответствии со ст.22.1 Закона № 152-ФЗ, оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных, то есть у оператора должен быть издан приказ (распоряжение) о назначении ответственного за организацию обработки персональных данных у оператора.

**5. Согласие субъекта персональных данных на обработку его персональных данных.**

В соответствии со ст.9 Закона № 152-ФЗ, субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных возлагается на оператора. То есть у оператора также должен быть такой документ, как согласие субъекта персональных данных на обработку его персональных данных.

**6. Документы, подтверждающие предоставление субъекту персональных данных информации, в случае если персональные данные получены не от субъекта персональных данных.**

Согласно ст.18 Закона № 152-ФЗ, если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных **обязан предоставить** субъекту персональных данных следующую информацию:
1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки персональных данных и ее правовое основание;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных;
5) источник получения персональных данных.

**7. Документы, содержащие положения о принятии оператором ПД правовых, организационных и технических мер для защиты персональных данных.**

Согласно ч.1 ст.19 Закона № 152-ФЗ, оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

**8. Документы по организации приема и обработке обращений и запросов субъектов персональных данных.**

Согласно ч.4 ст.22.1 Закона № 152-ФЗ, лицо, ответственное за организацию обработки персональных данных, в частности, обязано 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.

* Документ о классификации информационных систем;
* Список лиц, которым необходим доступ к персональным данным, обрабатываемым в информационной системе, утвержденный оператором или уполномоченным лицом.

В соответствии со ст.ст. 86-88 Трудового кодекса РФ от 30 декабря 2001 года № 197-ФЗ работодатель обязан иметь документ, устанавливающий порядок обработки персональных данных работников, с которым работники и их представители должны быть ознакомлены под роспись.

Действие Закона № 152-ФЗ распространят свое действие как на случаи обработки персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и, в большинстве случаев, без использования таких средств. Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства РФ от 15.09.2008 г. № 687 (далее – Положение № 687), ***урегулированы вопросы обработки персональных данных (использование, уточнение, распространение, уничтожение) без использования средств автоматизации.***

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Оператором персональных данных при обработке персональных данных, осуществляемой без использования средств автоматизации, должны быть оформлены также следующие документы.
• **Документы, определяющие категории обрабатываемых персональных данных, особенности и правила их обработки без использования средств автоматизации.**
Согласно п.6 Положения № 687, 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 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).

• **Типовые формы документов.**
Согласно п. 7 Положения № 687, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться определенные условия:
- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

• **Документ, устанавливающий требования к ведению журналов (реестров, книг…), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор.**
Согласно п.8 Положения № 687, при ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:
- необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

• **Документ, устанавливающий требования к хранению материальных носителей, содержащих персональные данные**
Согласно п.15 Положения № 687, при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие 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.

Требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных установлены Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».