**Локальные акты оператора по вопросам обработки персональных данных**

Если вы [обрабатываете персональные данные](consultantplus://offline/ref=F440A9931652C43D958CBFF26FEC8513ABDE6988D08B909364786319BD4F4B2F5630B87E3657CE4F38D51A069C97FCB8871DB2B7E5505A93F7G8F) (являетесь оператором), то вы должны принять меры для их защиты. Эти меры должны быть достаточными, чтобы обеспечить выполнение оператором обязанностей и не допустить неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, копирование, распространение, а также иные неправомерные действия с ними ([ч. 1 ст. 18.1](consultantplus://offline/ref=F440A9931652C43D958CB0F971EC8513A8D76A82DD83909364786319BD4F4B2F5630B87E3657CD4A36D51A069C97FCB8871DB2B7E5505A93F7G8F), [ч. 1 ст. 19](consultantplus://offline/ref=F440A9931652C43D958CB0F971EC8513A8D76A82DD83909364786319BD4F4B2F5630B87E3657CD4937D51A069C97FCB8871DB2B7E5505A93F7G8F) Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных).

**МЕРЫ**

|  |  |
| --- | --- |
| **правовые.** Это создание комплекта [документов](consultantplus://offline/ref=F440A9931652C43D958CBFF26FEC8513ABDE6988D088909364786319BD4F4B2F5630B87E3657CE4D3FD51A069C97FCB8871DB2B7E5505A93F7G8F) (локальных актов), необходимых для защиты персональных данных\*  \_\_\_\_\_\_\_\_  **\****для операторов, являющихся государственными или муниципальными органами Правительством РФ установлен перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (ПП РФ от 21 марта 2012 г. № 211)* | **технические и организационные.** Это [действия](consultantplus://offline/ref=F440A9931652C43D958CBFF26FEC8513ABDE6988D088909364786319BD4F4B2F5630B87E3657CE4E3DD51A069C97FCB8871DB2B7E5505A93F7G8F), которые вы должны совершить, чтобы обеспечить безопасность. (например, установить шифрование, обучить сотрудников) |

Создание документов по персональным данным (локальных актов) - одна из обязанностей оператора, предусмотренная ст. 18.1 - Закона о персональных данных.

**Локальные акты** — это документальное отражение происходящих у оператора процессов обработки персональных данных. Их наличие подтверждает выполнение оператором большинства предусмотренных законодательством обязанностей.

**Исходя из складывающейся практики общие требования к документам**

* Локальный нормативный акт должен быть утвержден уполномоченным лицом (генеральным директором, директором, советом директоров или другими уполномоченными лицами, определенными учредительными документами) оператора.
* В документах надлежит подробно отразить весь процесс обработки персональных данных.
* Закон о персональных данных не устанавливает требований к количеству локальных актов по работе с персональными данными. Перечень локальных актов, а также их содержание зависят от особенностей обработки персональных данных у оператора.

Согласно п.2 ч.1 ст. 18.1 Закона о персональных оператор, являющийся юридическим лицом издает документы, которые можно условно разделить на три блока:

* определяющих политику оператора в отношении обработки персональных данных;
* локальные акты по вопросам обработки персональных данных;
* локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений
* Локальный акт может быть единым, в котором урегулированы все вопросы, либо может быть принято несколько актов. (*Например, общие вопросы регламентирует положение об обработке персональных данных, а отдельные моменты другие локальные акты: порядок хранения персональных данных*; *инструкция по обеспечению безопасности персональных данных; инструкция по работе с персональными данными в автоматизированных системах (при их наличии); требования к помещениям для работы с персональными данными и т. д.)*

**Несмотря на наличие в Законе о персональных данных обязанности по внедрению локальных актов, четкий перечень этих документов Законом не установлен.**

|  |  |
| --- | --- |
| **Перечень документов для операторов**  ***(примерный)*** | [**Перечень**](consultantplus://offline/ref=8D11990A33A53C54225CB59E8058FABA28DFD69F1BA3A14426394F561858AB62D01CECDC2B9CFCAFF86C3F1D62BE28327C13AA4B583052DAfAsBE) **мер (документов) для операторов, являющихся государственными или муниципальными органами (утв. ПП РФ от 21.03.2012 № 211)** |
| * Согласие на обработку персональных данных * Приказ о назначении ответственного за обработку персональных данных * Политика оператора в отношении обработки персональных данных * Информированное согласие пользователя сайта (при сборе персональных данных через Интернет) * Положение об обработке и защите персональных данных * Последствия отказа предоставить персональные данные * Соглашение о неразглашении информации содержащей персональные данные * Перечень форм, содержащих персональные данные * Правила рассмотрения запросов субъектов персональных данных * Правила осуществления внутреннего контроля * Модель угроз безопасности * Приказ о назначении ответственного за обеспечение безопасности персональных данных * Приказ о хранении бумажных носителей персональных данных и порядке их уничтожения * Приказ об утверждении перечня персональных данных * Приказ о допуске к обработке персональных данных * Приказ об утверждении перечня ИСПДн * Инструкция ответственного за организацию обработки персональных данных * Инструкция ответственного за обеспечение безопасности персональных данных * Инструкция по учету лиц, допущенных к работе с персональными данными в ИСПДн * Инструкция по проведению инструктажа, допущенных к работе в ИСПДн * Инструкция пользователя ИСПДн * Инструкция по учёту и хранению съёмных носителей персональных данных * Инструкция по резервному копированию и восстановлению персональных данных * Журнал учета запросов субъектов персональных данных * Журнал учета съемных носителей, содержащих персональные данные * Журнал учёта прав доступа к ИСПДн * Журнал учёта средств защиты информации * Форма уведомления органа по защите прав субъектов персональных данных * Акт определения уровня защищённости персональных данных * Акт оценки потенциального вреда субъектам персональных данных * Акт об уничтожении персональных данных * Документы, подтверждающие ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) обучение указанных работников (документы, подтверждающие факт проведения обучения работников Оператора в области защиты персональных данных и изучения требования законодательства РФ в этой области) * Локальные акты, подтверждающие выполнение Оператором требований Положения об обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства от 15.09.2008 № 687: * типовые формы документов и связанные с ними документы (инструкции по заполнению, карточки, реестры, журналы), предполагающие или допускающие содержание персональных данных, как утвержденные законодательством РФ, так и самим оператором; * журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор и инструкции по их заполнению; * документы, устанавливающие места хранения персональных данных (материальных носителей), в том числе, устанавливающие необходимость раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях; * документы, устанавливающие перечень лиц, осуществляющих обработку персональных данных неавтоматизированным способом, либо имеющих к ним доступ; * документы, устанавливающие перечень мер, необходимых для обеспечения сохранности персональных данных и исключающих несанкционированный к ним доступ при хранении материальных носителей; * документы, устанавливающие перечень лиц, ответственных за реализацию мер, необходимых для обеспечения сохранности персональных данных и исключающих несанкционированный к ним доступ при хранении материальных носителей; * документы, подтверждающие информирование лиц, осуществляющих обработку персональных данных без использования средств автоматизации (сотрудников Оператора и (или) лиц, осуществляющих такую обработку по договору с Оператором) 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 актам и федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Оператора (при их наличии) | * + Приказ о назначении ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих и (или) работников указанного органа, замещающих должности, не являющиеся должностями государственной гражданской службы Российской Федерации или муниципальной службы, на основании трудового договора (далее - служащие);   + Утверждение актом руководителя государственного или муниципального органа следующих документов: * правил обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований; * правил рассмотрения запросов субъектов персональных данных или их представителей; * правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора; * правил работы с обезличенными данными в случае обезличивания персональных данных; * перечня информационных систем персональных данных; * перечней персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций; * перечней должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных; * перечней должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным; * должностного регламента (должностные обязанности) или должностной инструкции ответственного за организацию обработки персональных данных в государственном или муниципальном органе; * типового обязательства служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей; * типовой формы согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовой формы разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные; * порядка доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных; * при эксплуатации информационных систем персональных данных в случае, если государственный или муниципальный орган является оператором таких информационных систем, принимаются правовые меры по обеспечению безопасности персональных данных при их обработке, предусмотренные Постановлением Правительства РФ от 01.11.2012 N 1119"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", исполнение которых обеспечивает установленные уровни защищенности персональных данных |

* Политика в отношении обработки персональных данных ([п. 2 ч. 1 ст. 18.1](consultantplus://offline/ref=1DE7887AB6EC01EF6328027807E60E178430DFD931B617C3BA43875814F402D7D9A3E379D6FD13E2769BE4564FA5C2EFFACA2F9126A60B3A7Bz3F) Закона о персональных данных). Это самый главный документ, который устанавливает категории, цели, способы обработки персональных данных, порядок их хранения и использования ([Рекомендации](consultantplus://offline/ref=1DE7887AB6EC01EF6328027807E60E17843AD8D635BA17C3BA43875814F402D7CBA3BB75D7FA0EE47F8EB2070A7Fz9F) Роскомнадзора по его составлению можно найти на сайте Роскомнадзора в разделе «Персональные данные» по адресу https://rkn.gov.ru/personal-data/p908/)
* Целесообразно принять отдельно локальные акты по обработке персональных данных сотрудников (лиц, состоящих с оператором в трудовых или служебных отношениях) и локальные акты по обработке персональных данных субъектов (физических лиц), состоящих с оператором в договорных или иных гражданско-правовых отношениях
* Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.
* В случае, если Оператор, осуществляет сбор персональных данных с использованием информационно-телекоммуникационных сетей, то 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.

Документы, определяющие политику в отношении обработки персональных данных операторов, являющихся государственными или муниципальными органами, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

* Со всеми локальными нормативными актами по персональным данным под роспись должны быть ознакомлены все сотрудники Оператора

Полезные ссылки

* **Приказ Минспорта России от 27.02.2019 N 168. "О персональных данных в Министерстве спорта Российской Федерации"**

(вместе с "Правилами обработки персональных данных в Министерстве спорта Российской Федерации", "Правилами рассмотрения запросов субъектов персональных данных или их представителей в Министерстве спорта Российской Федерации", "Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора", "Правилами работы с обезличенными данными в случае обезличивания персональных данных в Министерстве спорта Российской Федерации", "Порядком доступа федеральных государственных гражданских служащих Министерства спорта Российской Федерации в помещения, в которых ведется обработка персональных данных")

* **Приказ Минздрава России от 04.03.2019 N 110н. "Об обработке персональных данных в Министерстве здравоохранения Российской Федерации"**

(вместе с "Правилами обработки персональных данных в Министерстве здравоохранения Российской Федерации")

* + **Приказ Росгвардии от 19.11.2018 N 507. "Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, Правил работы с обезличенными данными в случае обезличивания персональных данных, Должностного регламента (должностных обязанностей, должностной инструкции) ответственного за организацию обработки персональных данных, Перечня информационных систем персональных данных войск национальной гвардии Российской Федерации и Порядка доступа личного состава войск национальной гвардии Российской Федерации в помещения, в которых ведется обработка персональных данных"**
  + **Приказ Минюста России от 18.12.2017 N 260. "Об утверждении перечня информационных систем персональных данных Министерства юстиции Российской Федерации"**
  + **Приказ Минстроя России от 30.01.2019 N 61/пр. "О персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Российской Федерации"**

(вместе с "Правилами обработки персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Российской Федерации", "Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", "Правилами рассмотрения запросов субъектов персональных данных или их представителей", "Правилами работы с обезличенными данными в случае обезличивания персональных данных в Министерстве строительства и жилищно-коммунального хозяйства Российской Федерации")

* + **Приказ Роскомнадзора от 03.12.2012 № 1255 "Об утверждении Положения об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций"**