РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

Программа внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

ВВЕДЕНИЕ

Настоящий документ представляет собой программу внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора, которая содержит рекомендации по порядку проведения периодических проверок условий обработки персональных данных.

Программа разработана для государственных и муниципальных органов, а также их подведомственных организаций, и носит рекомендательный характер.

Целью программы внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства является содействие в исполнении государственными и муниципальными органами, а также их подведомственными организациями требований законодательства о персональных данных в части проведения периодических проверок условий обработки персональных данных.

Задачи программы:

- формирование у сотрудников государственных и муниципальных органов, а также их подведомственных учреждений теоретических знаний по проведению внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства.
- исполнение государственными и муниципальными органами, а также их подведомственными учреждениями требований законодательства о персональных данных в полном объеме в части проведения периодических проверок условий обработки персональных данных.

В методической программе представлена нормативная правовая база, регулирующая отношения, связанные с обработкой персональных данных, рекомендации по порядку проведения периодических проверок условий обработки персональных данных, а также типовые формы плана проведения периодических проверок условий обработки персональных данных, акта мероприятия внутреннего контроля соответствия обработки персональных данных установленным требованиям и плана мероприятий по устранению нарушений, выявленных по результатам периодических проверок условий обработки персональных данных.

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ, РЕГУЛИРУЮЩИЕ ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ – Глава 14 «Защита персональных данных работника»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
- Указ Президента РФ от 01.02.2005 № 112 «О конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации»;
- Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;
- Постановление Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства Российской Федерации от 31.03.2018 №397 «Об утверждении единой методики проведения конкурсов на замещение вакантных должностей государственной гражданской службы Российской Федерации и включение в кадровый резерв государственных органов»;
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Распоряжение Правительства Российской Федерации от 15.08.2007 г. № 1055-Р «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;
- Приказ Роскомнадзора от 30.05.2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».

1. Общие положения.

В соответствии с требованиями ч. 1 ст. 18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Закон) оператор обязан осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Согласно требованиям пп. д. п. 1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденных Постановлением Правительства РФ от 21.03.2012 № 211 (далее – Перечень мер), в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуется проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе.

Проверки условий обработки персональных данных проводятся оператором, в том числе в целях:

- оценки выполнения требований законодательства о персональных данных оператором;

- выявления и предотвращения нарушений законодательства в сфере персональных данных.

2. Рекомендованный порядок осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства.

Периодические проверки условий обработки персональных данных рекомендуется проводить не реже одного раза в год.

Проверки подразделяются на:

плановые;

внеплановые.

Проверки соответствия обработки персональных данных установленным требованиям рекомендуется проводить на основании утвержденного руководителем ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (Приложение №1) или на основании поступившего письменного

заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Проверки осуществляются ответственным за организацию обработки персональных данных либо комиссией, образуемой руководителем государственного или муниципального органа.

Оператором, являющимся государственным и муниципальным органом, должен быть утвержден локальный акт, регламентирующий процедуру проведения внутреннего контроля соответствия обработки персональных данных установленным требованиям законодательства о персональных данных.

При проведении проверки оператору рекомендуется установить:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;

состояние учета машинных носителей персональных данных;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

осуществление мероприятий по обеспечению целостности персональных данных;

наличие правовых оснований по сбору копий документов, содержащих персональные данные;

соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки персональных данных.

Также оператору рекомендуется предусмотреть обязанность лиц, проводивших проверку, в отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, обеспечивать конфиденциальность персональных данных.

3. Предмет внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства.

Предметом периодических проверок условий обработки персональных данных может являться:

1. Уведомление об обработке персональных данных.

При проведении проверки оператору рекомендуется оценить актуальность сведений, указанных в реестре операторов, осуществляющих обработку персональных данных, а именно их соответствие локальным актам и фактической деятельности.

Часто операторы не указывают сведения об обработке персональных данных таких категорий субъектов персональных данных, как пользователи сайта, участники конкурсов, посетители, а также не указывают все цели обработки персональных данных, например, изготовление визитных карточек, обеспечение добровольным медицинским страхованием.

Особое внимание при проведении проверки соответствия обработки персональных данных установленным требованиям рекомендуется обратить на актуальность адресов баз данных, указанных в уведомлении об обработке персональных данных.

В случае если оператор начал осуществлять обработку персональных данных в новых целях, необходимо отразить данную цель в уведомлении об обработке персональных данных путем направления информационного письма в адрес уполномоченного органа по защите прав субъектов персональных данных.

При прекращении обработки персональных данных в рамках той или иной цели, соответствующие положения должны быть исключены из уведомления об обработке персональных данных.

Вышеуказанные положения также распространяются на категории субъектов, чьи персональные данные обрабатываются, перечень обрабатываемых персональных данных, перечень действий с персональными данными и пр.

2. Локальные акты оператора.

В рамках проверки оператору рекомендуется оценить наличие, а также содержание документов, установленных пп. б п. 1 Перечня мер.

Документы должны быть утверждены актом руководителя государственного или муниципального органа.

Оператор должен удостовериться, что правила обработки персональных данных изданы в отношении каждой категории субъектов персональных данных, например в отношении пользователей сайта, практикантов, соискателей на вакантные должности, посетителей и пр.

Также оператору рекомендуется поддерживать в актуальном состоянии перечень информационных систем персональных данных.

В ходе проведения проверки условий обработки персональных данных оператору рекомендуется оценить соответствие локальных актов

фактической действительности, а также сведениям, указанным в уведомлении об обработке персональных данных.

Локальные акты оператора должны содержать сведения обо всех целях обработки персональных данных, категориях субъектов персональных данных, перечне обрабатываемых персональных данных, сроках хранения персональных данных, а также порядке их уничтожения.

В случае обработки оператором новой категории персональных данных или в случае прекращения соответствующей обработки, оператором должны быть внесены изменения в локальный акт, определяющий политику обработки персональных данных.

При проведении проверки оператору рекомендуется оценить соответствие локального акта, определяющего политику в отношении обработки персональных данных, «Рекомендациям по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», изданным Роскомнадзором (Приложение №2).

При проведении проверки соответствия обработки персональных данных установленным требованиям оператору необходимо проанализировать должностной регламент или должностную инструкцию ответственного за организацию обработки персональных данных в государственном или муниципальном органе на предмет наличия положений, закрепляющих обязанности лица, ответственного за организацию обработки персональных данных, в соответствии с ч. 4 ст. 22.1 Закона.

Оператору рекомендуется в рамках проверки проанализировать типовую форму согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных.

Форма согласия должна быть издана в отношении каждой категории субъектов, чьи персональные данные обрабатываются оператором. Получение согласия субъекта на обработку персональных данных должно осуществляться до момента начала обработки его персональных данных.

В соответствии с пп. г Перечня мер при обработке персональных данных, осуществляемой без использования средств автоматизации, государственные и муниципальные органы выполняют требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

В ходе проведения проверки условий обработки персональных данных оператору рекомендуется удостовериться в том, что в соответствии с требованиями п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 (далее – Положение), типовая форма или связанные с ней документы содержат сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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, общее описание используемых оператором способов обработки персональных данных

Также оператору рекомендуется проверить наличие локальных актов, закрепляющих:

места хранения персональных данных (материальных носителей) и перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ (п. 13 Положения);

условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ, а также перечень лиц, ответственных за реализацию указанных мер (п. 15 Положения).

3. Ознакомление служащих государственного или муниципального органа с положениями законодательства Российской Федерации о персональных данных.

В соответствии с пп. е Перечня мер государственный или муниципальный орган осуществляет обучение служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, а также ознакомление служащих 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.

В ходе проведения проверки условий обработки персональных данных оператору рекомендуется оценить ознакомлены ли все лица, осуществляющие обработку персональных данных, с положениями законодательства о персональных данных и локальных актов.

Оператору рекомендуется знакомить работников с изменениями, внесенными в нормативные правовые акты, регулирующие отношения, связанные с обработкой персональных данных, путем проведения соответствующего обучения и обеспечения условий для самостоятельного изучения служащими государственного или муниципального органа нормативных правовых актов с использованием системы «Консультант +».

В рамках проверки оператору рекомендуется обратить особое внимание на ознакомление лиц, осуществляющих обработку персональных данных без использования средств автоматизации, со следующими положениями (п. 6 Положения):

- факт обработки персональных данных, обработка которых осуществляется оператором без использования средств автоматизации;

- категории обрабатываемых персональных данных;

- особенности и правила осуществления такой обработки, установленные нормативными правовыми актами, а также локальными актами оператора.

4. Информационные системы персональных данных (далее – ИСПДн).

Оператор в рамках внутреннего контроля должен оценить актуальность локального акта, закрепляющего перечень лиц, имеющих доступ к ИСПДн, а также обратить особое внимание на наличие правового основания обработки персональных данных.

Оператору рекомендуется оценить соответствие объема обрабатываемых персональных данных в кадровых информационных системах заявленным целям обработки.

В рамках внутреннего контроля оператору рекомендуется уделить особое внимание локализации баз данных на территории Российской Федерации.

В соответствии с ч. 4 ст. 21 Закона в случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных

Обработка персональных данных уволенных служащих государственного или муниципального органа, а также лиц, замещающих должности, не относящиеся к должностям государственной гражданской службы, должна осуществляться в ИСПДн не более 5 лет с момента увольнения во исполнение требований законов о бухгалтерском и налоговом учете.

5. Официальный сайт в сети «Интернет».

В соответствии с п. 2 Перечня мер документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.

Оператору в ходе проведения проверки рекомендуется проверить соблюден ли срок размещения документа, определяющего политику в отношении обработки персональных данных, на официальном сайте, а также актуальность размещенной версии документа.

Также оператору в рамках проверки условий обработки персональных данных рекомендуется проверить наличие правовых оснований обработки персональных данных пользователей сайта.

Например, при сборе персональных данных пользователей сайта посредством метрических программ, оператору рекомендуется убедиться, что согласие пользователя сайта на обработку его персональных данных с использованием метрических программ получено.

6. Документы лиц, претендующих на замещение вакантных должностей.

В ходе проведения проверки условий обработки персональных данных оператору рекомендуется оценить срок хранения персональных данных лиц, претендующих на замещение вакантных должностей.

Согласно п. 25 Указа Президента РФ от 01.02.2005 № 112 «О конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации» (далее – Указ Президента Российской Федерации), документы претендентов на замещение вакантной должности гражданской службы, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, могут быть им возвращены по письменному заявлению в течение трех лет со дня завершения конкурса. До истечения этого срока документы хранятся в архиве государственного органа, после чего подлежат уничтожению.

На основании изложенного, а также в соответствии с ч. 4 ст. 21 Закона обработка персональных данных лиц, претендующих на замещение вакантных должностей, должна быть прекращена, а персональные данные уничтожены в течение 30 дней после достижения цели, а именно истечения сроков хранения документов, установленных Указом Президента Российской Федерации.

Документы лиц, претендующих на замещение вакантных должностей, не относящихся к должностям государственной гражданской службы, должны быть уничтожены в течение 30 дней с момента принятия положительного решения или решения об отказе в приеме на работу.

7. Обработка персональных данных служащих государственного или муниципального органа, а также работников, не являющихся государственными гражданскими служащими.

Передача персональных данных служащих государственного или муниципального органа, а также работников, не являющихся государственными гражданскими служащими, должна осуществляться с письменного согласия.

Требования к содержанию письменного согласия установлены ч. 4 ст. 9 Закона.

Оператору при проведении проверки рекомендуется проверить наличие правового основания передачи персональных данных служащих государственного или муниципального органа, а также работников, не являющихся государственными гражданскими служащими, в адрес третьих лиц, а также соответствие письменной формы согласия требованиям ч. 4 ст. 9 Закона.

Согласно ч. 3 ст. 6 Закона оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Поручение обработки персональных данных всегда предполагает передачу персональных данных в адрес третьего лица, однако передача персональных данных работника в адрес третьего лица не означает поручение обработки персональных данных.

Типовыми примерами поручения обработки персональных данных служащих государственного или муниципального органа, а также работников, не являющихся государственными гражданскими служащими, являются передача (предоставление, доступ) оператором персональных данных в адрес третьих лиц в целях организации командирования, сопровождения информационных систем персональных данных и пр.

Необходимо отметить, что согласие на обработку персональных данных в письменной форме должно содержать наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора.

Оператору в ходе проведения проверки рекомендуется удостовериться в наличии правового основания поручения третьим лицам обработки персональных данных служащих государственного или муниципального органа, а также работников, не являющихся государственными гражданскими служащими.

8. Основная деятельность.

В ходе мероприятия внутреннего контроля оператору рекомендуется оценить соответствие объема обрабатываемых персональных данных в рамках основной деятельности заявленным целям обработки, наличие правовых оснований обработки персональных данных и сроки хранения персональных данных субъектов.

Например, обработка документов, содержащих персональные данные лиц, обратившихся за государственной услугой, может осуществляться в течение сроков, установленных нормативными правовыми актами.

Обработка документов, содержащих персональные данные лиц, обратившихся за государственной услугой, может осуществляться без согласия в объеме, установленном административным регламентом предоставления государственной услуги.

Оператору в ходе проведения периодических проверок условий обработки персональных данных рекомендуется оценить соответствие договоров-поручений на обработку персональных данных требованиям ч. 3 ст. 6 Закона.

4. Порядок закрепления результатов проведенного мероприятия внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям законодательства.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии.

Результаты проведенной проверки рекомендуется оформлять в виде акта (Приложение №3).

После оформления результатов мероприятия внутреннего контроля, оператору рекомендуется приступить к устранению нарушений, выявленных по результатам внутреннего контроля.

Оператору рекомендовано издать документ, определяющий план мероприятий по устранению нарушений, выявленных по результатам проверки условий обработки персональных данных (Приложение №4).

Оператору рекомендуется определить срок устранения каждого нарушения, выявленного в ходе проверки условий обработки персональных данных.

Также Оператору рекомендуется внести сведения о проведенной проверке в журнал проведения внутреннего контроля соответствия

обработки персональных данных требованиям законодательства, а также локальным актам.

Приложение к Программе №1

утверждено Руководителем_____

План проведения периодической проверки условий обработки персональных данных

№ п/п	Мероприятие внутреннего контроля и (или) аудита соответствия обработки персональных данных установленным требованиям	Дата

Приложение №2 к Программе

РЕКОМЕНДАЦИИ

ПО СОСТАВЛЕНИЮ ДОКУМЕНТА, ОПРЕДЕЛЯЮЩЕГО ПОЛИТИКУ ОПЕРАТОРА

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, В ПОРЯДКЕ,

УСТАНОВЛЕННОМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ ОТ 27 ИЮЛЯ

2006 ГОДА N 152-ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

1. Настоящие Рекомендации разработаны в целях выработки унифицированных подходов к структуре и форме документа, определяющего политику оператора в отношении обработки персональных данных (далее - Политика).

2. Основные понятия, используемые в Рекомендациях:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. В Политику рекомендуется включить следующие структурные компоненты:

3.1 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.

3.2 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 оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным

подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

3.3 Правовые основания обработки персональных данных

Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных.

В качестве правового основания обработки персональных данных могут быть указаны:

- федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью оператора;
- уставные документы оператора;
- договоры, заключаемые между оператором и субъектом персональных данных;
- согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" не может служить правовым основанием обработки персональных данных оператором, поскольку указанный Закон регулирует отношения, связанные с обработкой персональных данных, а также закрепляет требования, предъявляемые к операторам при обработке персональных данных.

3.4 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:

- работники оператора, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников;
- клиенты и контрагенты оператора (физические лица);
- представители/работники клиентов и контрагентов оператора (юридических лиц).

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

3.5 Порядок и условия обработки персональных данных

В данном разделе рекомендуется указывать перечень действий, совершаемых оператором 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 <2>), в том числе, находящихся за пределами Российской Федерации (трансграничная передача). При этом рекомендуется указать конкретное наименование и местонахождение соответствующих третьих лиц, цели осуществляемой (трансграничной) 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 Федерального закона "О персональных данных", а также информацию о принятии оператором мер, предусмотренных ч. 2 ст. 18.1, ч. 1 ст. 19 Федерального 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.

При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона "О персональных данных".

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

3.6 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 <4>.

При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

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

- оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;

- 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 <5>.

Рекомендуется включить в Политику регламент(ы) реагирования на запросы/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/обращений.

Приложение №3 к Программе

АКТ

мероприятия внутреннего контроля соответствия обработки персональных данных установленным требованиям

На основании: приказа руководителя …

было проведено плановое мероприятие внутреннего контроля в целях:…

Продолжительность проверки:…

Лица, уполномоченные на проведение мероприятия:…

В ходе мероприятия внутреннего контроля было проверено соблюдение:
1. порядка обработки персональных данных и его соответствие требованиям законодательства о персональных данных, а именно:…

2. условий обработки и защиты персональных данных в информационных системах персональных данных, а именно:…

3. условий обработки персональных данных без использования средств автоматизации, а именно:…

4. …

В ходе проведения мероприятия было выявлено:…

Прилагаемые документы: 1. Описание проведенного мероприятия по внутреннему контролю….

Подписи лиц, проводивших проверку:

Приложение №4 к Программе

План мероприятий по устранению нарушений, выявленных по результатам периодической проверки условий обработки персональных данных

№ п/п	Мероприятие	Срок выполнения	Ответственный	Отметка о выполнении	Примечания