

Приложение 11 к Приказу № 0602-102 от « 6 » февраля 2023 г.
о вводе в действие организационно-распорядительной документации в
области защиты информации в ФГБУ «ИНФОРМАВТОДОР»

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ИНФОРМАЦИОННЫЙ ЦЕНТР ПО АВТОМОБИЛЬНЫМ ДОРОГАМ
«ИНФОРМАВТОДОР» ФЕДЕРАЛЬНОГО ДОРОЖНОГО АГЕНТСТВА»**

**ПОЛОЖЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ
ДАнных**

Содержание

1. Общие положения.....	3
2. Термины и определения	4
3. Перечень используемых сокращений	4
4. Принципы обработки ПДн.....	5
5. Система защиты персональных данных	6
5.1. Организация СЗПДн.....	6
5.2. Мониторинг СЗПДн.....	7
6. Правила обработки ПДн.....	8
6.1. Сбор ПДн	8
6.2. Порядок отзыва согласия субъекта ПДн на обработку ПДн	12
6.3. Хранение персональных данных.....	13
6.4. Использование, извлечение и уточнение персональных данных	13
6.5. Передача ПДн.....	14
6.6. Блокирование ПДн.....	15
6.7. Сроки обработки ПДн	15
6.8. Уничтожение персональных данных	16
6.9. Особенности неавтоматизированной обработки ПДн	18
7. Обучение работников Учреждения правилам обработки ПДн	18
8. Управление доступом к ПДн	19
9. Актуализация и пересмотр.....	20

1. Общие положения

Настоящее Положение о порядке обработки и защите персональных данных (далее – Положение) устанавливает требования по организации и непосредственному функционированию процессов обработки персональных данных (далее – ПДн) в Федеральном государственном бюджетном учреждении «Информационный центр по автомобильным дорогам «ИНФОРМАВТОДОР» Федерального дорожного агентства» (далее – ФГБУ «ИНФОРМАВТОДОР», Учреждение) в соответствии с требованиями нормативных правовых актов Российской Федерации в области обработки и защиты ПДн.

Настоящий документ распространяет свое действие на структурные подразделения Учреждения и отдельных должностных лиц, принимающих участие в процессах обработки ПДн.

Требования настоящего Положения распространяются на все процессы обработки ПДн, независимо от формы их представления.

В Учреждении для реализации настоящего Положения приказом директора назначаются Ответственный за организацию обработки ПДн и Ответственный за обеспечение безопасности ПДн. Допускается объединение указанных ролей.

Контроль за соблюдением требований настоящего Положения осуществляет Ответственный за организацию обработки ПДн.

Настоящее Положение разработано в соответствии со следующими нормативными правовыми документами:

- Конституция Российской Федерации;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден Приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК) России от 18 февраля 2013 г. № 21).

При работе с ПДн во всех случаях, не урегулированных внутренними документами Учреждения, необходимо руководствоваться действующим законодательством Российской Федерации.

Работники Учреждения, получившие доступ к ПДн, обязаны соблюдать конфиденциальность таких данных, не разглашать и иным образом не делать доступными ПДн субъекта без его согласия.

Настоящее Положение должно быть доведено до всех работников Учреждения, осуществляющих обработку ПДн, под подпись. Подпись работника в листе ознакомления означает его согласие со всеми требованиями, указанными в настоящем Положении.

2. Термины и определения

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь – лицо, обладающее постоянным или временным доступом к ИС, в рамках выполнения своих должностных обязанностей.

3. Перечень используемых сокращений

АРМ	Автоматизированное рабочее место
ИС	Информационные системы
ИСПДн	Информационные системы персональных данных
ПДн	Персональные данные
СЗИ	Средство защиты информации
СЗПДн	Система защиты персональных данных
Учреждение	Федеральное государственное бюджетное учреждение «Информационный центр по автомобильным дорогам «ИНФОРМАВТОДОР» Федерального дорожного агентства»

4. Принципы обработки ПДн

Обработка ПДн в Учреждении должна осуществляться в соответствии со следующими принципами:

- обработка ПДн должна осуществляться на законной и справедливой основе;
- обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями их сбора;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке ПДн должны быть обеспечены их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Необходимо принимать меры по удалению или уточнению неполных или неточных данных;
- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- не допускается использовать ПДн в целях причинения имущественного и (или) морального вреда субъектам ПДн, затруднения реализации их прав и свобод;
- все работники должны быть ознакомлены под подпись с документами Учреждения, устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области в соответствии с действующими нормативными документами.

В Учреждении должен проводиться регулярный анализ соответствия процессов обработки ПДн указанным выше принципам. Данный анализ проводится в следующих случаях:

- создание новых или внесение изменений в существующие процессы обработки ПДн;
- создание новых или внесение изменений в существующие ИС, в которых осуществляется обработка ПДн;

- изменение нормативной базы, затрагивающей принципы и (или) процессы обработки ПДн в Учреждении;
- проведение внутренних контрольных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

5. Система защиты персональных данных

5.1. Организация СЗПДн

С целью выполнения требований законодательства Российской Федерации в области ПДн, важнейшей задачей является обеспечение конфиденциальности, целостности и доступности ПДн при их обработке.

Для решения данной задачи в Учреждении введена, функционирует и проходит периодический пересмотр (контроль) система защиты персональных данных (далее – СЗПДн), которая состоит из следующих компонентов:

- организационная структура (участники обработки и ответственные лица);
- организационно-распорядительная документация;
- средства обработки ПДн;
- меры и средства обеспечения безопасности ПДн.

СЗПДн Учреждения основана на следующих принципах:

- вовлеченность руководства – деятельность по обеспечению безопасности ПДн инициирована и контролируется руководством Учреждения;
- соответствие мер и средств защиты актуальным угрозам безопасности ПДн;
- соответствие мер и средств защиты требованиям нормативных документов Российской Федерации в области обработки и обеспечения безопасности ПДн;
- комплексность – с целью обеспечения безопасности ПДн в Учреждении используется совокупность организационных и технических мер;
- удобство персонала – при построении и модернизации СЗПДн в Учреждении учитываются и, по возможности, сводятся к минимуму возможные затруднения персонала в работе со средствами защиты и при выполнении основных процедур обеспечения безопасности ПДн;
- законность организационных и технических мер по обеспечению безопасности ПДн;
- непрерывность повышения уровня знаний работников Учреждения в сфере обеспечения безопасности ПДн;
- стремление к постоянному совершенствованию СЗПДн.

В соответствии с принципами обработки ПДн в Учреждении определены правила обработки ПДн, а также методы и способы обеспечения безопасности ПДн.

Учреждение самостоятельно либо с привлечением организаций, обладающих лицензией на техническую защиту конфиденциальной информации, не реже одного раза в 3 года проводит аудит соответствия обработки и защиты ПДн требованиям законодательства Российской Федерации и подзаконных актов.

5.2. Мониторинг СЗПДн

Мониторинг СЗПДн осуществляется с целью актуализации существующей СЗПДн в соответствии с текущими процессами обработки ПДн, элементами ИТ- и ИБ-инфраструктуры, и требованиями по безопасности ПДн.

В ходе мониторинга СЗПДн обеспечивается контроль отсутствия несанкционированного доступа к ПДн.

В процессе мониторинга СЗПДн решаются задачи по актуализации:

- сведений о процессах обработки ПДн:
 - перечень ПДн, обрабатываемых в Учреждении;
 - объем обрабатываемых ПДн;
 - категории субъектов, чьи ПДн обрабатываются в Учреждении;
 - пользователи ПДн (структурные подразделения и отдельные работники) и третьи стороны (контрагенты, аутсорсинговые и обслуживающие организации и т. п.), имеющие доступ к ПДн;
 - структура и состав ИСПДн;
 - мероприятия и технические меры обеспечения безопасности ПДн;
- уровня защищенности ПДн при их обработке в ИСПДн, в т. ч.:
 - вреда, который может быть причинен субъектам ПДн в случае нарушения безопасности ПДн, и соответственно показателя опасности угроз безопасности в ИСПДн;
 - угроз безопасности ПДн;
- требований к СЗПДн;
- документации на СЗПДн;
- вариантов реализации СЗПДн (в т. ч. проведение дополнительных мероприятий по защите ПДн).

Мониторинг СЗПДн организуется и контролируется Ответственным за обеспечение безопасности ПДн с привлечением подразделений, обеспечивающих функционирование ИСПДн и подразделений, обрабатывающих ПДн в ИСПДн.

6. Правила обработки ПДн

6.1. Сбор ПДн

Учреждение осуществляет обработку ПДн в целях:

- выполнения требований трудового законодательства;
- ведения кадрового и бухгалтерского учета;
- ведения кадрового резерва;
- организации мероприятий;
- соблюдения пропускного и внутриобъектового режимов.

В целях выполнения требований трудового законодательства и ведения кадрового и бухгалтерского учета Учреждение осуществляет обработку ПДн работников Учреждения:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- гражданство;
- реквизиты документа, удостоверяющего личность;
- адрес проживания и прописки;
- семейное положение;
- сведения о месте работы и должности, профессии;
- сведения о финансовом положении;
- доходы;
- страховой номер индивидуального лицевого счета (СНИЛС);
- данные воинского учета;
- сведения об образовании, о квалификации или наличии специальных знаний, ученой степени;
- сведения о повышении квалификации и профессиональной переподготовке;
- стаж работы, сведения о предыдущих местах работы и занимаемых должностях, указанные в трудовой книжке;
- сведения о наличии инвалидности;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования;

- сведения из реестра дисквалифицированных лиц;
- сведения об участии в органах управления других организаций;
- идентификационный номер налогоплательщика (ИНН);
- сведения о наличии льгот при исчислении налогов и уплате страховых взносов;
- сведения о праве на получение налоговых вычетов;
- реквизиты документа, содержащего сведения о смерти;
- реквизиты банковского счета;
- номер телефона;
- адрес электронной почты.

В целях организации мероприятий Учреждение осуществляет обработку ПДн работников Учреждения:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- гражданство;
- реквизиты документа, удостоверяющего личность;
- адрес проживания и прописки;
- семейное положение;
- сведения о месте работы и должности, профессии;
- сведения об образовании, о квалификации или наличии специальных знаний, ученой степени;
- сведения о повышении квалификации и профессиональной переподготовке;
- номер телефона;
- адрес электронной почты.

В целях соблюдения пропускного и внутриобъектового режимов Учреждение осуществляет обработку ПДн работников Учреждения:

- фамилия, имя, отчество;
- отпечатки пальцев.

Приведенный перечень обрабатываемых данных является исчерпывающим. При этом в исключительных случаях допускается сбор дополнительных данных о субъекте, что в обязательном порядке отражается в согласии субъекта на обработку его ПДн либо в составе договора, заключаемого с субъектом. Сбор специальных категорий ПДн не производится. Обработка ПДн субъектов в целях рекламы и политической агитации, ПДн, разрешенных субъектом для распространения, не производится.

Сбор ПДн организуется исключительно на законных основаниях. При сборе ПДн до или в момент их получения необходимо осуществлять сбор согласий на обработку ПДн.

Учреждение может осуществлять сбор согласий на обработку ПДн в письменной форме.

Согласие в письменной форме должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта ПДн.

Учреждение может получать ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов Российской Федерации;
- от другого субъекта ПДн в целях реализации его законных прав.

Если в соответствии с федеральным законом предоставление ПДн и (или) получение Учреждением согласия на обработку ПДн являются обязательными, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку, в частности, указать на положения законодательных актов Российской Федерации, предусматривающих сбор ПДн и последствия отказа в предоставлении ПДн.

При сборе ПДн Учреждение обязано предоставить субъекту ПДн при обращении или получении запроса следующую информацию:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- перечень ПДн;
- применяемые в Учреждении способы обработки ПДн;
- наименование и фактический адрес Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Учреждением обязанностей, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных».

Указанные выше сведения предоставляются субъекту ПДн или его представителю Учреждением в течение 10 дней с момента обращения либо получения запроса. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 10 дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Учреждением в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Ответственность за организацию приема и обработки обращений субъектов ПДн или их представителей и уполномоченного органа по защите прав субъектов ПДн возлагается на Ответственного за организацию обработки ПДн.

Если субъект ПДн по какой-либо причине не может получить доступ к документам Учреждения в области обеспечения безопасности ПДн, либо указанных в них сведений

недостаточно для удовлетворения просьбы субъекта ПДн, то предоставление указанных сведений осуществляется напрямую субъекту по его запросу.

Если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн необходимо предоставить субъекту ПДн следующую информацию:

- наименование Учреждения;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения ПДн.

Указанная информация может не предоставляться в следующих случаях:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- предоставление субъекту ПДн указанных сведений нарушает права и законные интересы третьих лиц.

Ответственность за сбор и хранение согласий возлагается на работников Учреждения, осуществляющих сбор ПДн субъектов ПДн. Хранение согласий субъектов ПДн осуществляется в бумажном и/или электронном виде.

6.2. Порядок отзыва согласия субъекта ПДн на обработку ПДн

Субъект ПДн в праве отозвать согласие на обработку его ПДн.

В случае отзыва субъектом ПДн согласия на обработку ПДн работники Учреждения осуществляют в срок до 10 календарных дней удаление ПДн на всех носителях, при необходимости оставляя обезличенные сведения, необходимые для ведения статистики и реализации законных интересов Учреждения. При отзыве согласия субъектом не удаляются сведения, обработка которых производится во исполнение требований законодательства Российской Федерации.

В случае обращения субъекта ПДн с требованием о прекращении обработки ПДн Учреждение прекращает обработку его ПДн в срок, не превышающий 10 календарных дней с даты получения Учреждением соответствующего требования. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока обработки ПДн.

Если право или обязанность обработки ПДн субъекта ПДн Учреждением установлена законом, то субъект ПДн обязан не препятствовать реализации Учреждением этого права или исполнению этой обязанности.

6.3. Хранение персональных данных

В Учреждении обеспечивается раздельное хранение ПДн, цели обработки которых несовместимы между собой, и не допускается на одном бумажном носителе фиксация ПДн, цели обработки которых заведомо несовместимы.

Хранение ПДн в Учреждении осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов Российской Федерации, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

Работники Учреждения, имеющие доступ к ПДн субъектов ПДн в связи с исполнением трудовых обязанностей, обязаны обеспечивать хранение информации, содержащей ПДн субъектов ПДн, исключаящее неправомерный или случайный доступ к ним.

В случае необходимости работник обязан передать документы и иные носители, содержащие ПДн субъектов ПДн, работнику, на которого организационно-распорядительным актом (приказом, распоряжением) или должностной инструкцией возложено исполнение его трудовых обязанностей, включающих обработку ПДн.

В случае увольнения работника, имеющего доступ к ПДн субъектов ПДн, документы и иные носители, содержащие ПДн субъектов ПДн, передаются другому работнику, имеющему доступ к ПДн субъектов ПДн, по указанию руководителя структурного подразделения.

6.4. Использование, извлечение и уточнение персональных данных

Обработка ПДн субъектов в целях выполнения требований трудового законодательства, ведения кадрового и бухгалтерского учета и ведения кадрового резерва, организации мероприятий, соблюдения пропускного и внутриобъектового режима осуществляется с использованием и без использования средств автоматизации.

В Учреждении запрещено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

При использовании ПДн допускается:

- извлечение ПДн из баз данных или иных электронных хранилищ данных;

- формирование документов (как в электронном виде, так и на бумажных носителях), содержащих ПДн, в случаях, предусмотренных технологическими процессами обработки ПДн;
- передача таких документов как внутри Учреждения между работниками, в том числе различных структурных подразделений, так и третьим лицам.

Субъект ПДн обязан предоставлять Учреждению достоверные сведения о себе и своевременно сообщать ей об изменении своих ПДн.

Учреждение обязано уточнять обрабатываемые ПДн и вносить в них необходимые изменения (при выявлении неполных или неточных ПДн субъекта ПДн) в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий.

Учреждение обязано уведомить субъекта ПДн или его представителя о внесенных изменениях и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта ПДн были переданы.

Лицом, ответственным за организацию и контроль своевременного внесения изменений в ПДн субъектов ПДн и направления уведомлений субъектам ПДн, их представителям и третьим лицам, является Ответственный за организацию обработки ПДн.

6.5. Передача ПДн

Передачу ПДн с использованием съемных носителей информации разрешается осуществлять только в случае служебной необходимости.

При необходимости передачи ПДн другим работникам Учреждения для исполнения ими своих трудовых обязанностей, допускается осуществлять передачу только работникам, имеющим доступ к ПДн субъектов ПДн в соответствии с «Перечнем лиц, допущенных к обработке персональных данных».

Предоставление Учреждением доступа к ПДн субъекта ПДн третьим лицам осуществляется при соблюдении следующих условий:

- передача ПДн, в том числе поручение Учреждением обработки ПДн третьим лицам осуществляется с согласия субъекта ПДн или без такового согласия при наличии правовых оснований, предусмотренных федеральным законодательством, в частности, статьей 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- в том случае, если Учреждение поручает обработку ПДн третьему лицу на основании договора, в условиях такого договора определяется:

- обязанность лица, осуществляющего обработку ПДн по поручению Учреждения, по соблюдению принципов и правил обработки ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн по поручению;
- цели обработки ПДн;
- обязанность лица, осуществляющего обработку ПДн по поручению Учреждения, по соблюдению конфиденциальности ПДн и обеспечению безопасности ПДн;
- требования по обеспечению безопасности ПДн, которые должны быть выполнены лицом, осуществляющим обработку ПДн по поручению Учреждения.

ПДн субъекта могут быть предоставлены его законному представителю в порядке, установленном действующим законодательством Российской Федерации.

Предоставление ПДн субъекта государственным органам и органам местного самоуправления производится в соответствии с требованиями действующего законодательства Российской Федерации и настоящим Положением.

Ответственность за соблюдение порядка предоставления ПДн субъекта третьим лицам несет Ответственный за организацию обработки ПДн, а также руководитель структурного подразделения, осуществляющего передачу ПДн субъекта ПДн третьему лицу.

В Учреждении не осуществляется трансграничная передача ПДн (передача ПДн на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу).

6.6. Блокирование ПДн

Учреждение блокирует обрабатываемые ПДн при выявлении их недостоверности или правонарушений в отношении субъекта ПДн на период проверки в следующих случаях:

- по требованию субъекта ПДн;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий.

6.7. Сроки обработки ПДн

Обработка ПДн субъектов ограничивается определенным в локальных актах Учреждения сроком обработки либо наступлением определенных законодательством обстоятельств для каждой цели обработки ПДн: достижение целей обработки ПДн либо утрата необходимости достижения этих целей.

Обработка ПДн сотрудника осуществляется до момента прекращения его трудовых отношений с Учреждением. После увольнения сотрудника обработке и хранению подлежат только

те документы, содержащие ПДн уволенного сотрудника, срок хранения которых установлен законодательством Российской Федерации.

Срок обработки ПДн субъектов в целях ведения кадрового резерва составляет 2 года.

Обработка ПДн сотрудников в целях организации мероприятий осуществляется до момента окончания мероприятия.

Обработка ПДн сотрудника в целях соблюдения пропускного и внутриобъектового режимов осуществляется до момента прекращения его трудовых отношений с Учреждением.

По окончании срока обработки либо хранения ПДн субъектов подлежат уничтожению (удалению) либо обезличиванию.

6.8. Уничтожение персональных данных

Учреждение уничтожает ПДн в случае:

- достижения целей обработки ПДн или утраты необходимости в их достижении;
- выявления неправомерной обработки;
- отзыва согласия субъекта на обработку его ПДн, если отзыв согласия влечет за собой уничтожение ПДн;
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или по его поручению, в срок, не превышающий 3 рабочих дней с даты этого выявления, необходимо прекратить неправомерную обработку ПДн. В случае, если обеспечить правомерность обработки ПДн невозможно, необходимо уничтожить такие ПДн в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки.

При уничтожении ПДн субъектов составляется документ, подтверждающий уничтожение ПДн.

В случае, если обработка ПДн Учреждением осуществляется без использования средств автоматизации, документом, подтверждающим уничтожение ПДн субъектов, является акт об уничтожении ПДн.

В случае, если обработка ПДн Учреждением осуществляется с использованием средств автоматизации или с использованием и без использования средств автоматизации, документами, подтверждающими уничтожение ПДн, являются акт об уничтожении ПДн и выгрузка из журнала событий в ИСПДн.

Акт об уничтожении ПДн должен содержать:

- наименование Учреждения;

- наименование юридического лица или фамилию, имя, отчество физического лица, адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка была поручена такому лицу;
- фамилию, имя, отчество субъекта (субъектов) или иную информацию, относящуюся к определенному физическому лицу (лицам), чьи ПДн были уничтожены;
- фамилию, имя, отчество, должность лица (лиц), уничтожившего ПДн, и его подпись;
- перечень категорий уничтоженных ПДн субъектов;
- наименования уничтоженного материального носителя (носителей), содержащего ПДн субъекта, с указанием количества листов в отношении каждого материального носителя (в случае обработки ПДн без использования средств автоматизации);
- наименование ИСПДн, из которой были уничтожены ПДн субъекта (в случае обработки ПДн с использованием средств автоматизации);
- способ уничтожения ПДн;
- причину уничтожения ПДн;
- дату уничтожения ПДн.

Акт об уничтожении ПДн в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается равнозначным акту об уничтожении ПДн на бумажном носителе, подписанному собственноручной подписью.

Выгрузка их журнала регистрации событий ИСПДн должна содержать:

- фамилию, имя, отчество субъекта (субъектов) или иную информацию, относящуюся к определенному физическому лицу (лицам), чьи ПДн были уничтожены;
- перечень категорий уничтоженных ПДн субъектов;
- наименование ИСПДн, из которой были уничтожены ПДн субъекта;
- причину уничтожения ПДн;
- дату уничтожения ПДн.

В случае если выгрузка из журнала не позволяет указать предусмотренные сведения, недостающие сведения вносятся в акт об уничтожении ПДн.

Акт об уничтожении ПДн и выгрузка из журнала событий ИСПДн подлежат хранению в течение 3 лет с момента уничтожения ПДн.

Проверка наличия в ИСПДн ПДн, которые должны быть уничтожены и контроль удаления таких данных осуществляется ответственным работником Отдела кадров или Администратором ИС под контролем Ответственного за организацию обработки ПДн не реже 1 раза в 3 месяца.

Учреждение может заключать договоры с третьими сторонами на оказание услуг по уничтожению материальных носителей. При этом Учреждение и третья сторона соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

6.9. Особенности неавтоматизированной обработки ПДн

При использовании внутренних типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны выполняться следующие условия:

- в типовые формы или в связанные с ними документы (инструкция по ее заполнению, карточки, реестры и журналы) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Учреждения, фамилия, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Учреждении способов обработки ПДн;
- в случае необходимости получения письменного согласия на обработку ПДн, в типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации;
- типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, чьи ПДн содержатся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;
- в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

В Учреждении обеспечивается раздельное хранение материальных носителей ПДн, обработка которых осуществляется для различных целей.

7. Обучение работников Учреждения правилам обработки ПДн

В Учреждении все работники, участвующие в обработке ПДн, в обязательном порядке должны проходить внутренний инструктаж по следующим темам:

- общие вопросы обеспечения информационной безопасности в Учреждении;
- правила автоматизированной и неавтоматизированной обработки ПДн;
- правила использования средств защиты информации, входящих в состав СЗПДн Учреждения;
- ответственность за нарушение правил обработки и обеспечения безопасности ПДн.

Новые работники в обязательном порядке проходят вводный инструктаж по указанным темам.

Ответственным за организацию проведения инструктажа работников Учреждения, участвующих в обработке и обеспечении безопасности ПДн, является Ответственный за организацию обработки ПДн.

8. Управление доступом к ПДн

Для определения перечня работников Учреждения, допущенных к работе с ПДн, разрабатывается «Перечень лиц, допущенных к обработке персональных данных», в котором указываются структурное подразделение и должность работника.

Работник допускается к обработке ПДн только после:

- ознакомления с требованиями настоящего Положения и иными организационно-распорядительными документами на СЗПДн, выполнение требований которых обязательно для соответствующих работников;
- прохождения инструктажа по правилам обработки и обеспечения безопасности ПДн;
- ознакомления с видами ответственности за нарушение установленных в Учреждении правил обработки и обеспечения безопасности ПДн.

При получении работником доступа к ИСПДн, за ним закрепляется роль Пользователя ИСПДн.

Пользователи ИСПДн должны иметь права доступа к ИСПДн, минимально необходимые для исполнения ими своих должностных обязанностей.

Инициатором внесения изменений в «Перечень лиц, допущенных к обработке персональных данных», выступают:

- руководители вновь созданных структурных подразделений, предполагающих участие их работников в обработке ПДн;
- руководители структурных подразделений, внутри которых произошли изменения организационно-штатной структуры, касающиеся работников, должностные обязанности которых связаны с обработкой ПДн;
- руководители структурных подразделений, внутри которых произошли изменения в должностных обязанностях работников, связанных с допуском или отменой допуска к ПДн, обрабатываемым в Учреждении.

Руководители перечисленных структурных подразделений оформляют служебные записки на имя Ответственного за организацию обработки ПДн, в которых указывают работников и категории субъектов ПДн, доступ к которым указанным работникам необходимо изменить или предоставить для выполнения ими своих функциональных (должностных) обязанностей. Ответственный за организацию обработки ПДн подготавливает новую редакцию «Перечня лиц,

допущенных к обработке персональных данных», с внесенными на основании служебной записки изменениями, которая утверждается директором Учреждения.

9. Актуализация и пересмотр

Сведения, содержащиеся в настоящем Положении, могут уточняться и дополняться по мере необходимости не реже одного раза в год.

Настоящее Положение должно быть пересмотрено в обязательном порядке в случаях изменений в законодательстве РФ в области защиты ПДн.

При необходимости к пересмотру настоящего Положения могут привлекаться на договорной основе юридические лица и (или) индивидуальные предприниматели, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Ответственным за актуализацию и пересмотр настоящего Положения является Ответственный за организацию обработки ПДн.