ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ

УПРАВЛЕНИЕ ПО ХАНТЫ-МАНСИЙСКОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ

(УФСИН РОССИИ ПО ХАНТЫ-МАНСИЙСОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ)

П Р И К А З

Сургут

01 апреля 2016 г. № 151

Об утверждении Положения о правилах обработки и порядке защиты персональных данных в информационных системах персональных данных

В соответствии с требованиями постановления Правительства Российской Федерации от 21 марта 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», п р и к а з ы в а ю:

1. Утвердить Положение о правилах обработки и порядке защиты персональных данных в информационных системах персональных данных (далее – Положение) Управления Федеральной службы исполнения наказаний по Ханты-Мансийскому автономному округу – Югре (далее – УФСИН России по Ханты-Мансийскому автономному округу – Югре) (приложение).

2. Ответственному за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре заместителю начальника полковнику внутренней службы Амелишко Михаилу Михайловичу:

взять с работников, непосредственно осуществляющих обработку персональных данных, обязательства о соблюдении конфиденциальности персональных данных;

довести до работников, непосредственно осуществляющих обработку персональных данных, требования Положения.

3. Сотрудникам, ответственным за обеспечение безопасности персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре:

обеспечить обработку и защиту персональных данных в соответствии с Положением;

определить лиц непосредственно осуществляющих обработку персональных данных в информационных системах персональных данных УФСИН России по Ханты-Мансийскому автономному округу – Югре по направлению деятельности;

организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

4. Контроль за исполнением настоящего приказа возложить на заместителя начальника Управления Федеральной службы исполнения наказаний по Ханты-Мансийскому автономному округу – Югре полковника внутренней службы Амелишко Михаила Михайловича.

Начальник
полковник внутренней службы Д.Н. Безруких

Исп. Сбоев В.Г.
тел. (3462)21-95-51, вн.151

Приложение

к приказу УФСИН России по
Ханты-Мансийскому
автономному округу – Югре
от _____ № _____

ПОЛОЖЕНИЕ
о правилах обработки и порядке защиты
персональных данных в информационных системах персональных данных
Управления Федеральной службы исполнения наказаний
по Ханты-Мансийскому автономному округу – Югре

Сургут, 2016

Содержание

	Термины и определения	3
1.	Общие положения	5
2.	Работники, участвующие в обработке персональных данных	6
3.	Цели обработки персональных данных	7
4.	Правила обработки персональных данных	8
5.	Правила рассмотрения запросов субъектов персональных данных или их представителей	10
6.	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных»	11
7.	Правила работы с обезличенными персональными данными	13
8.	Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных	13
9.	Типовое обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей	19
10.	Типовая форма согласия на обработку персональных данных	20
11.	Типовая форма согласия на обработку персональных данных иных субъектов персональных данных	21
12.	Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	22
13.	Порядок доступа работников в помещения, в которых ведётся обработка персональных данных	23
14.	Особенности и правила обработки персональных данных, осуществляемой без использования средств автоматизации	24

Термины и определения

В настоящем документе используются следующие термины и их определения.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы без использования средств автоматизации (неавтоматизированная) – такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1. Общие положения

Положение о правилах обработки и порядке защиты персональных данных в информационных системах персональных данных (далее – Положение) Управления Федеральной службы исполнения наказаний по Ханты-Мансийскому автономному округу – Югре (далее – УФСИН России по Ханты-Мансийскому автономному округу – Югре) разработано в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Положение разработано с учетом положений:

Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

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, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211;

положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденного приказом ФСБ России от 10 июля 2014 г. № 378;

других нормативных и методических документов, регламентирующих вопросы обработки персональных данных.

Положение о правилах обработки и порядке защиты персональных данных при их обработке в информационных системах персональных данных УФСИН России по Ханты-Мансийскому автономному округу - Югре предназначено для организации и выполнения мероприятий по обеспечению безопасности информации при обработке ПДн в УФСИН России по Ханты-Мансийскому автономному округу – Югре от всех видов угроз (внешних и внутренних, умышленных и непреднамеренных), минимизации ущерба от возможной реализации угроз безопасности ПДн. Требования настоящего Положения распространяются на всех работников (сотрудников и служащих) УФСИН России по Ханты-Мансийскому автономному округу – Югре (штатных, временно исполняющих обязанности).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным,

результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности ПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Работники, участвующие в обработке персональных данных

В информационных системах персональных данных УФСИН России по Ханты-Мансийскому автономному округу – Югре можно выделить следующие группы работников, участвующих в обработке ПДн:

лицо, ответственное за организацию обработки ПДн в УФСИН России по Ханты-Мансийскому автономному округу – Югре;

лица, ответственные за обеспечение безопасности ПДн (администраторами безопасности) при их обработке в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре;

пользователи, обрабатывающие ПДн (пользователи) в УФСИН России по Ханты-Мансийскому автономному округу – Югре.

Данные об уровне доступа и информированности должны быть отражены в инструкциях администратора безопасности персональных данных и пользователя, обрабатывающего ПДн.

Лицо, ответственное за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре назначается из числа руководства Управления, отвечает за соблюдение и выполнение своих должностных обязанностей, администраторов безопасности и пользователей, координирует их деятельность.

Администратор безопасности, сотрудник УФСИН России по Ханты-Мансийскому автономному округу – Югре, ответственный за функционирование ИСПДн.

Администратор безопасности обладает следующим уровнем доступа и знаний:

обладает полной информацией о ПДн в обрабатываемых в ИСПДн по направлению деятельности;

имеет доступ к средствам криптографической защиты информации и к ключевым элементам автоматизированной системы ПДн;

не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных);

имеет возможность ознакомления и обработки ПДн в ИСПДн по направлению деятельности.

Пользователь - работник УФСИН России по Ханты-Мансийскому автономному округу – Югре, осуществляющий обработку ПДн. Обработка ПДн включает:

возможность просмотра ПДн, изменение, формирование справок и отчетов по информации, полученной из информационной системы персональных данных.

Пользователь обладает следующим уровнем доступа и знаний:

обладает всеми необходимыми атрибутами (например – паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

располагает конфиденциальными данными, к которым имеет доступ.

3. Цели обработки персональных данных

1. В УФСИН России по Ханты-Мансийскому автономному округу – Югре, персональные данные могут обрабатываться для:

осуществления статистических или иных исследовательских целей, за исключением целей, указанных в статье 15 Федерального закона «О персональных данных»;

обеспечения доступа неограниченного круга лиц к общедоступным персональным данным, который предоставлен субъектом персональных данных либо по просьбе субъекта персональных данных;

реализация социальных программ, гарантий и мероприятий связанных с действующими и бывшими работниками, в целях обеспечения льгот и гарантий, обеспечение личной безопасности работников;

осуществление программ в области профессиональной подготовки, переподготовки и повышению квалификации работников УФСИН России по Ханты-Мансийскому автономному округу – Югре;

формирование общедоступных источников персональных данных работников, содержащих контактную и другую информацию делового характера;

осуществление политики сотрудничества с органами государственной власти и местными органами власти;

организации кадрового учета в УФСИН России по Ханты-Мансийскому автономному округу – Югре и ведения кадрового делопроизводства;

исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение заполнения первичной статистической документации, в соответствии с законодательством Российской Федерации;

реализации уголовно – исполнительного законодательства;

реализации Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации»;

обеспечения пропускного режима;

осуществление других видов деятельности для реализации задач и функций, установленных действующим законодательством и Положением об УФСИН России по Ханты-Мансийскому автономному округу – Югре в рамках законодательства Российской Федерации с обязательным выполнением требований в области персональных данных.

2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей.

3. Обработка персональных данных, несовместимых с целями сбора персональных данных, не допускается.

4. 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.

4. Правила обработки персональных данных

1. Обработка персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре должна осуществляться на законной основе.

2. Не допускается обработка ПДн, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. 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.

6. При обработке ПДн должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Работники, осуществляющие обработку персональных данных в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу - Югре, должны принимать необходимые меры по удалению или уточнению неполных или неточных персональных данных.

7. Мерами, направленными на выявление и предотвращение нарушений, предусмотренных законодательством, являются:

осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятым в соответствии с ним нормативным правовым актам;

оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

ознакомление работников, осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, и их обучение.

8. Обеспечение безопасности персональных данных достигается, в частности:

определением угроз безопасности ПДн при их обработке в информационных системах персональных данных;

применением организационных и технических мер по обеспечению безопасности

ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по их недопущению;

восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установлением разграничения прав доступа пользователей к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе персональных данных.

9. Хранение ПДн должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения ПДн не установлен действующим законодательством, по согласованию с субъектом персональных данных. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

10. В случае выявления неправомерной обработки персональных данных, осуществляемой УФСИН России по Ханты-Мансийскому автономному округу – Югре в срок, не превышающий трех рабочих дней с даты этого выявления, УФСИН России по Ханты-Мансийскому автономному округу – Югре обязан прекратить неправомерную обработку ПДн.

В случае, если обеспечить правомерность обработки персональных данных невозможно, УФСИН России по Ханты-Мансийскому автономному округу – Югре в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных УФСИН России по Ханты-Мансийскому автономному округу - Югре обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом

по защите прав субъектов персональных данных, также указанный орган.

11. В случае достижения цели обработки персональных данных УФСИН России по Ханты-Мансийскому автономному округу – Югре обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого является субъект персональных данных, либо иным

соглашением между УФСИН России по Ханты-Мансийскому автономному округу – Югре и субъектом персональных данных.

12. В случае отзыва субъектом ПДн согласия на обработку своих персональных данных УФСИН России по Ханты-Мансийскому автономному округу – Югре обязан прекратить обработку персональных данных и уничтожить ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между УФСИН России по Ханты-Мансийскому автономному округу – Югре и субъектом персональных данных, а также действующим законодательством.

13. В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных выше, УФСИН России по Ханты-Мансийскому автономному округу – Югре осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий шесть месяцев, если иной срок не установлен действующим законодательством.

5. Правила рассмотрения запросов субъектов персональных данных

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки ПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре;

правовые основания и цели обработки ПДн;

цели и применяемые УФСИН России по Ханты-Мансийскому автономному округу – Югре способы обработки ПДн;

наименование и место нахождение УФСИН России по Ханты-Мансийскому автономному округу – Югре, сведения о лицах, которые имеют доступ к ПДн или которым могут быть раскрыты персональные данные на основании Федерального закона № 152-ФЗ;

обрабатываемые ПДн, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

сроки обработки ПДн, в том числе сроки их хранения.

2. Субъект ПДн вправе требовать от УФСИН России по Ханты-Мансийскому автономному округу – Югре уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту ПДн УФСИН России по Ханты-Мансийскому автономному округу - Югре в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для

раскрытия таких персональных данных.

4. Сведения предоставляются субъекту ПДн или его представителю УФСИН России по Ханты-Мансийскому автономному округу – Югре при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо сведения, иным образом подтверждающие факт обработки персональных данных УФСИН России по Ханты-Мансийскому автономному округу – Югре, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством о защите персональных данных

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в УФСИН России по Ханты-Мансийскому автономному округу – Югре организовывается проведение периодических проверок условий обработки ПДн.

2. Проверки осуществляются ответственным за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо комиссией образуемой приказом начальника УФСИН России по Ханты-Мансийскому автономному округу – Югре.

3. В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в ее результатах.

4. Проверки соответствия обработки ПДн установленным требованиям в УФСИН России по Ханты-Мансийскому автономному округу – Югре проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в УФСИН России по Ханты-Мансийскому автономному округу – Югре письменного заявления о нарушениях правил обработки ПДн (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

5. При проведении проверки соответствия обработки ПДн установленным требованиям должны быть полностью, объективно и всесторонне определены:

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

порядок и условия применения средств защиты информации;

состояние учета машинных носителей ПДн;

соблюдение правил доступа к ПДн;

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

мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности ПДн.

6. Ответственный за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо комиссия имеет право:

требовать от ответственных за обеспечение безопасности персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить начальнику УФСИН России по Ханты-Мансийскому автономному округу – Югре предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

вносить начальнику УФСИН России по Ханты-Мансийскому автономному округу – Югре предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства о защите ПДн.

7. В отношении ПДн, ставших известными ответственному за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность ПДн.

8. Проверка должна быть завершена не позднее чем через десять дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений ответственный за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо председатель комиссии докладывает начальнику УФСИН России по Ханты-Мансийскому автономному округу - Югре в форме письменного заключения.

Контроль за своевременностью, полнотой и объективностью проведения проверки возлагается на ответственного за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре, либо на председателя комиссии, назначенной приказом УФСИН России по Ханты-Мансийскому автономному округу – Югре.

7. Правила работы с обезличенными персональными данными

1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения класса ИСПДн и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством о защите персональных данных.

2. Способы обезличивания при условии дальнейшей обработки ПДн:

замена части сведений идентификаторами;

обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

другие способы.

3. Решение о необходимости обезличивания персональных данных принимает начальник УФСИН России по Ханты-Мансийскому автономному округу – Югре.

4. Ответственные за обеспечение безопасности персональных данных в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и способ обезличивания.

5. Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

6. Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

7. При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используются);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

8. При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

8. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных

1. Настоящие Требования и методы по обезличиванию персональных данных, обрабатываемых в ИСПДн, (далее - Требования и методы) разработаны в соответствии с подпунктом «з» пункта 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, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

2. В соответствии со ст. 3 Федерального закона № 152-ФЗ под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

3. Обезличивание ПДн должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых ПДн.

4. К свойствам обезличенных данных относятся:

полнота (сохранение всей информации о конкретных субъектах ПДн или группах субъектов ПДн, которая имелась до обезличивания);

структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта ПДн или группы субъектов ПДн, соответствующих связям, имеющимся до обезличивания);

релевантность (возможность обработки запросов по обработке ПДн и получения ответов в одинаковой семантической форме);

семантическая целостность (сохранение семантики ПДн при их обезличивании);

применимость (возможность решения задач обработки ПДн, стоящих перед УФСИН России по Ханты-Мансийскому автономному округу - Югре, осуществляющим обезличивание ПДн, обрабатываемых в ИСПДн, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, без предварительного деобезличивания всего объема записей о субъектах);

анонимность (невозможность однозначной идентификации субъектов ПДн, полученных в результате обезличивания, без применения дополнительной информации).

5. К характеристикам (свойствам) методов обезличивания ПДн (далее - методы обезличивания), определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:

обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность ПДн конкретному субъекту, устранить анонимность);

вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию субъекта персональных данных);

возможность косвенного деобезличивания (возможность проведения

деобезличивания с использованием информации других операторов);

совместимость (возможность интеграции ПДн, обезличенных различными методами);

параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

6. Требования к методам обезличивания подразделяются на:

требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;

требования к свойствам, которыми должен обладать метод обезличивания.

7. К требованиям к свойствам получаемых обезличенных данных относятся:

сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых ПДн);

сохранение структурированности обезличиваемых ПДн;

сохранение семантической целостности обезличиваемых ПДн;

анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

8. К требованиям к свойствам метода обезличивания относятся:

обратимость (возможность проведения деобезличивания);

возможность обеспечения заданного уровня анонимности;

увеличение стойкости при увеличении объема обезличиваемых ПДн.

9. Выполнение приведенных в пунктах 7 и 8 требований обязательно для обезличенных данных и применяемых методов обезличивания.

10. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных информационных системах и позволять решать поставленные задачи обработки ПДн.

11. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

метод введения идентификаторов (замена части сведений (значений ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

метод изменения состава или семантики (изменение состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления части сведений);

метод декомпозиции (разбиение множества (массива) ПДн на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

метод перемешивания (перестановка отдельных записей, а также групп записей в массиве ПДн).

12. Метод введения идентификаторов реализуется путем замены части ПДн,

позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

семантическая целостность;

применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);

изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых ПДн);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием ПДн, имеющихся у других операторов);

совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);

параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах ПДн, подлежащих обезличиванию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется установить атрибуты ПДн, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

13. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

Метод обеспечивает следующие свойства обезличенных данных:

структурированность;

релевантность;

применимость;

анонимность.

Оценка свойств метода:

обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);

вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых ПДн);

возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием ПДн, имеющихся у других операторов);

совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);

параметрический объем (параметры метода определяются набором правил изменения состава или семантики ПДн);

возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения ПДн).

Для реализации метода требуется выделить атрибуты ПДн, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта.

При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

14. Метод декомпозиции реализуется путем разбиения множества записей ПДн на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

релевантность;

семантическая целостность;

применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);

параметрический объем (определяется числом подмножеств и числом субъектов

персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

15. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

релевантность;

семантическая целостность;

применимость;

анонимность.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);

возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием ПДн, имеющихся у других операторов);

совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);

параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

9. Типовое обязательство работника, непосредственно осуществляющего обработку персональных данных, в случае увольнения со службы прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____,
(фамилия, имя, отчество полностью)
являясь работником _____,
_____
_____,
(указать наименование структурного подразделения)
обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае увольнения со службы.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ «___» _____ 20___ г.
(фамилия, инициалы) (подпись)

10. Типовая форма согласия на обработку персональных данных

Я,_____,
(фамилия, имя, отчество)

зарегистрированный по адресу: _____,

_____

основной документ, удостоверяющий личность

_____
(наименование документа, удостоверяющего личность,

_____
серия и номер, сведения о дате выдачи документа и выдавшем его органе)

даю согласие _____
(наименование организации)

_____
(адрес организации)

на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, представление, доступ), обезличивание, блокирование, удаление, уничтожение, содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а именно:

Фамилия, имя, отчество; дата рождения; место рождения; пол; гражданство; знание иностранного языка; образование, повышение квалификации, профессиональная переподготовка, стажировка, присвоение ученой степени, ученого звания (если таковое имеется) или наличие специальных знаний; профессия (специальность); трудовой и общий стаж, сведения о приемах, перемещениях и увольнениях по предыдущим местам работы, размер денежного содержания (оклад, надбавки, премии); состояние в браке, состав семьи, место работы или учебы членов семьи и родственников; паспортные данные, адрес места жительства, дата регистрации по месту жительства; номер телефона (домашнего, мобильного); идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; сведения, включенные в трудовую книжку; сведения о воинском учете; фотография; сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовой функции, водительское удостоверение (в связи с выполнением трудовой функции работника), заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на службу или ее прохождению, материалы по аттестации, содержание трудовых договоров и занимаемая должность, сведения о доходах, имуществе и обязательствах имущественного характера, документы о награждении (грамоты, дипломы, удостоверения о награждении), антропометрические данные, данные о психофизиологическом состоянии.

Настоящее согласие действует со дня его подписания до дня отзыва письменной форме в случаях, предусмотренных действующим законодательством.

Об ответственности за достоверность представленных сведений предупрежден(а).

_____ _____
(дата) (подпись)

11. Типовая форма согласия на обработку персональных данных иных субъектов персональных данных

Я, _____,
паспорт серии _____, номер _____,
выданный _____
«___» _____ _____ года, даю согласие УФСИН России по Ханты-Мансийскому автономному округу - Югре на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных п. 3 ч. 1 ст. 3 Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных» (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, представление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных) и содержащихся в настоящем заявлении, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижения по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, а именно:

Фамилия, имя, отчество; дата рождения; место рождения; пол; гражданство; знание иностранного языка; образование, повышение квалификации, профессиональная переподготовка, стажировка, присвоение ученой степени, ученого звания (если таковое имеется) или наличие специальных знаний; профессия (специальность); трудовой и общий стаж, сведения о приемах, перемещениях и увольнениях по предыдущим местам работы, размер денежного содержания (оклад, надбавки, премии); состояние в браке, состав семьи, место работы или учебы членов семьи и родственников; паспортные данные, адрес места жительства, дата регистрации по месту жительства; номер телефона (домашнего, мобильного); идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; сведения, включенные в трудовую книжку; сведения о воинском учете; фотография; сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовой функции, водительское удостоверение (в связи с выполнением трудовой функции работника), заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на муниципальную службу или ее прохождению, материалы по аттестации, содержание трудовых договоров и занимаемая должность, сведения о доходах, имуществе и обязательствах имущественного характера, документы о награждении (грамоты, дипломы, удостоверения о награждении), антропометрические данные, данные о психофизиологическом состоянии.

Для обработки в целях _____
_____
(указать цели обработки)

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

_____ _____
(дата) (подпись)

12. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

_____.

(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:

_____.

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи, иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;

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

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____	_____	_____
(дата)	(подпись)	(расшифровка)

13. Порядок доступа работников в помещения, в которых ведётся обработка персональных данных

1. Настоящий Порядок доступа в помещения, в которых ведется обработка персональных данных (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов ПДн, обрабатываемых в УФСИН России по Ханты-Мансийскому автономному округу – Югре, и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми работниками УФСИН России по Ханты-Мансийскому автономному округу – Югре.

3. Помещения, в которых ведется обработка ПДн, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранно-пожарной сигнализацией.

4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

5. Бумажные носители персональных данных и электронные носители персональных данных хранятся в металлических шкафах, оборудованных опечатывающими устройствами.

6. Помещения, в которых ведется обработка персональных данных, запираются на ключ, а в нерабочее время подключаются к охранной сигнализации.

7. Вскрытие и закрытие (опечатывание) помещений, в которых ведется обработка персональных данных, производится работниками, имеющими право доступа в данные помещения.

8. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

убрать бумажные носители персональных данных и электронные носители персональных данных в шкафы, закрыть и опечатать шкафы;

отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

закрыть окна;

сдать помещение под охрану.

9. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:

провести внешний осмотр с целью установления целостности двери и замка;

открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

10. При обнаружении неисправности двери и запирающих устройств работники обязаны:

не вскрывая помещение, в котором ведется обработка ПДн, доложить

ответственному за обеспечение безопасности персональных данных в ИСПДн;

в присутствии не менее двух иных работников, включая ответственного за обеспечение безопасности персональных данных в ИСПДн, вскрыть помещение и осмотреть его;

составить акт о выявленных нарушениях и передать его ответственному за обеспечение безопасности персональных данных в ИСПДн для организации служебной проверки.

11. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные лица имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, доступ к ней иных лиц, не имеющих права, должен быть исключен.

13. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

14. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на ответственного за обеспечение безопасности персональных данных в ИСПДн.

14. Особенности и правила обработки персональных данных, осуществляемой без использования средств автоматизации

1. Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также требований предусмотренных действующим законодательством.

2. Обработка персональных данных, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

4. При фиксации персональных данных на материальных носителях ПДн

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

5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных действующим законодательством, а также указаниями и распоряжениями УФСИН России по Ханты-Мансийскому автономному округу – Югре.

6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес оператора, фамилию, 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 УФСИН России по Ханты-Мансийскому автономному округу – Югре способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

7. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем ПДн, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе ПДн, а если это не допускается техническими особенностями материального носителя ПДн, – путем фиксации на том же материальном носителе ПДн сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя ПДн с уточненными персональными данными.

9. Обработка ПДн, осуществляемая без использования средств автоматизации,

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

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

11. При хранении материальных носителей ПДн 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 приказом УФСИН России по Ханты-Мансийскому автономному округу – Югре.