

Приложение № 5 к приказу  
Департамента социальной политики от  
25 апреля 2014 года № 175  
«Об утверждении организационно-  
распорядительных документов по  
защите персональных данных»

## **ПОЛОЖЕНИЕ об обработке персональных данных**

### **I. ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящее Положение об обработке персональных данных (далее — Положение) Департамента социальной политики Администрации города Кургана (далее - Департамент) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

Цели разработки Положения:

-определение порядка обработки персональных данных сотрудников Департамента и обратившихся в Департамент граждан, а также иных субъектов, персональные данные которых подлежат обработке на основании полномочий Департамента;

-обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников Департамента и обратившихся в Департамент граждан, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

-установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

-обезличенных персональных данных;

-общедоступных персональных данных.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии Департамента, если иное не определено законом Российской Федерации.

### **II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую

информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

**Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**Обработка персональных данных без использования средств автоматизации** – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 N 687).

**Оператор** – Департамент социальной политики.

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

### **III. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Состав персональных данных, обрабатываемых в Департаменте, определяется «Перечнем сведений, содержащих персональные данные».

Документы со сведениями, содержащими персональные данные, обрабатываются в следующих структурных подразделениях Департамента:

- отдел опеки и попечительства;
- отдел документационного обеспечения;
- управление образования;
- управление экономики и финансов.

### **IV. ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

Перед началом обработки персональных данных необходимо получить у субъекта согласие в письменном виде в соответствии, с утвержденной в Департаменте формой такого согласия.

В ИС ПДн «Бухгалтерия» обрабатываются документы - лицевые счета сотрудников Департамента, содержащие персональные данные сотрудников в единичном или сводном виде:

Информация, представляемая гражданам, либо их представителями в структурные подразделения Департамента необходима в рамках предоставления муниципальной услуги и должна иметь документальную форму. Граждане, либо их представители предъявляют документы, определяемые регламентом соответствующей муниципальной услуги.

Данные из документов вносятся сотрудниками в электронном виде в ИСПДн в соответствии с регламентом предоставляемой муниципальной услуги.

## **V. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Хранение бумажных документов, электронных носителей (дисков, флэш накопителей и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

Обработка персональных данных в Департаменте осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в Департаменте определяются «Перечнем сведений, содержащих персональные данные».

Срок хранения документов, содержащих персональные данные, определяется «Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденный Приказом Министерства культуры РФ от 25.08.2010 № 558.

По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Eraser») без уничтожения материального носителя.

Обезличивания персональных данных в Департаменте не предполагается.

## **VI. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Обработка персональных данных в Департаменте может осуществляться исключительно в целях предоставления муниципальных услуг, обработки обращений граждан и в случаях, установленных законодательством Российской Федерации.

При определении объема и содержания, обрабатываемых персональных данных Департамент должен руководствоваться Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 N 210-ФЗ и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

## **VII. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

Предоставление персональных данных допускается в случаях передачи налоговой бухгалтерской и иной отчетности, передачи сведений о заработной плате в банковские и иные кредитные организации при официальном запросе, раскрытии данных правоохранительным органам при наличии законных оснований, а также в иных случаях, установленным законодательством РФ.

Не допускается распространение персональных данных субъекта.

## **VIII. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Департаментом за счет своих средств.

В Департаменте защите подлежат все сведения, содержащие персональные данные субъектов, в том числе:

- зафиксированные в бумажных документах;
- зафиксированные в электронных документах на технических средствах, включая внешние носители;
- речевая (акустическая) информация, содержащая персональные данные;
- текстовая и графическая видовая информация, содержащая персональные данные;

Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

Проведение организационных мероприятий:

- разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;
- ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;
- проведение обучения сотрудников вопросам защиты персональных данных.

Программно-аппаратная защита:

- разработка модели угроз безопасности персональным данным;
- внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;
- организация учёта носителей персональных данных.

Инженерно-техническая защита:

- установка сейфов или запирающихся шкафов для хранения носителей персональных данных;
- установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Департамента.

Организацию и контроль защиты персональных данных в структурных подразделениях Департамента осуществляют их непосредственные руководители.

## **IX. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

Допуск к персональным данным субъекта могут иметь только те сотрудники Департамента, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких сотрудников отражен в «Приказе об утверждении списка должностных лиц, которым доступ которых к персональным данным, необходим для выполнения служебных (трудовых) обязанностей №124 от 27.03.2014.

Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

-ознакомление сотрудника под роспись с настоящим Положением, «Инструкцией о порядке работы с персональными данными» и другими локальными нормативно-правовыми актами Департамента, касающимися обработки персональных данных;

-истребование с сотрудника «Обязательства о неразглашении конфиденциальной информации»;

Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

## **X. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ**

Типовые формы Департамента и иные документы, предполагающие включение в них персональных данных:

-заявление граждан;

-формы, определяемые Регламентами муниципальных услуг.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Департамента или лица, осуществляющие такую обработку по договору с Департаментом), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Департаментом без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Департамента.

Ведение журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения Департамента или в иных аналогичных целях не предполагается.

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

Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

## **XI. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Состав информационных систем персональных данных Департамента и их характеристика определяется «Перечнем информационных систем персональных данных» (Приложение 1 к Приказу Департамента №124 от 27.03.2014).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

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, а также иных несанкционированных действий.

Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

Информационные системы в Департаменте классифицируются на основании приказа директора Департамента, в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки информационных систем персональных данных - администратор безопасности ИСПДн.

При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

- своевременное обнаружение фактов несанкционированного доступа к персональным данным;

- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянный контроль над обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты персональных данных.

Иные требования по обеспечению безопасности информации и средств защиты информации в Департаменте выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Курганской области.

## **ХII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности ИСПДн и ответственного за организацию обработки персональных данных Департамента.

Сотрудники Департамента, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленные настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) Департамента, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения.

Сотрудник Департамента, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Департаменту (в соответствии с п.7 ст. 243 Трудового кодекса РФ).