



Управление социальной
защиты населения
 администрации
города Трехгорного

Приказ № 120

29.12.2015

Об утверждении и введение в действие
Положения о порядке обработки персональных
данных в УСЗН без использования средств автоматизации

Во исполнение «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, а также иных нормативных документов по защите информации

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение о порядке обработки персональных данных в УСЗН без использования средств автоматизации (Приложение).
2. Делопроизводителю Шаргородской М. М. ознакомить сотрудников УСЗН с данным приказом под подпись.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник УСЗН

Ю. А. Полуконова

Утверждено приказом
начальника УСЗН

№ _____ от _____ 20 ____ г.

Положение
о порядке обработки персональных данных в УСЗН
без использования средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о порядке обработки персональных данных без использования средств автоматизации (далее - Положение) определяет порядок работы с документами, содержащими персональные данные, в УСЗН.

1.2. Положение разработано в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации».

1.3. Перечень персональных данных, обрабатываемых в УСЗН, утверждается начальником УСЗН.

1.4. Список лиц, доступ которых к персональным данным необходим для выполнения трудовых обязанностей, утверждается начальником УСЗН.

1.5. Ответственный за организацию обработки персональных данных УСЗН отвечает за подбор лиц, допускаемых к информации ограниченного доступа (персональным данным), и обязан обеспечить систематический контроль за тем, чтобы к этой информации получали доступ только работники, которым данная информация необходима для выполнения своих трудовых обязанностей.

1.6. Лица, допущенные к персональным данным, обязаны:

- а) обеспечивать сохранность и конфиденциальность персональных данных;
- б) информировать субъекта персональных данных об обращении посторонних лиц о предоставлении его персональных данных.

1.7. Запрещается выносить документы и дела, содержащие персональные данные, из помещений, а также передавать их по открытым каналам связи, за исключением случаев, предусмотренных законодательством Российской Федерации или по согласованию с субъектом персональных данных.

1.8. Во время пребывания в помещениях работник несет личную ответственность за защиту информации в данном помещении и обязуется соблюдать требования Инструкции по физической охране и контролю доступа в помещения.

1.9. Неконтролируемое пребывание в помещении посторонних лиц исключено.

1.10. Контроль за исполнением требований настоящего Положения возлагается на ответственных за организацию обработки персональных данных в информационных системах УСЗН, администратора информационных систем и информационной безопасности в УСЗН.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Муниципальные информационные системы – информационные системы, созданные на основании решения органа местного самоуправления.

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), 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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных

в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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.

3. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Персональные данные при их обработке, осуществляющейся без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

3.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

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

3.3.1. типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляющейся без использования средств автоматизации, наименование и адрес УСЗН, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых УСЗН способов обработки персональных данных;

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

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

3.4. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимых для однократного пропуска субъекта персональных данных в помещение УСЗН или в иных аналогичных целях, должны соблюдаться следующие условия:

3.4.1. необходимость ведения такого журнала должна быть предусмотрена актом, содержащим сведения о цели обработки персональных данных, осуществляющейся без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

3.4.2. копирование содержащейся в таких журналах информации не допускается;

3.4.3. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

3.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.6. В случае утери (кражи) или порчи носителя материальных данных должно быть проведено расследование причин, составлен соответствующий акт, данные следует восстановить путем изготовления нового материального носителя, виновное лицо должно быть привлечено к ответственности в соответствии с законодательством Российской Федерации.

3.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

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

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ И ПЕРЕДАЧЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

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

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

4.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. В этих целях необходимо осуществлять хранение персональных данных в запираемых шкафах или ящиках, ключ от которых должен находиться у работника, имеющего право доступа к персональным данным, находящимся в этих шкафах (ящиках), дубликаты ключей должны храниться у заведующего хозяйством УСЗН.

4.4. Шкафы или ящики, в которых хранятся документы, содержащие персональные данные, по окончании рабочего дня запираются работниками, ответственными за учет и хранение документов.

4.5. Конфиденциальные документы должны пересылаться (доставляться) между организациями в соответствующим образом оформленных запечатанных пакетах.

4.6. Размножение и отправка документов, содержащих персональные данные, осуществляется только с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

4.7. Проверки наличия конфиденциальных документов проводятся не реже одного раза в год комиссией, назначаемой начальником УСЗН.

4.8. Проверками должны быть охвачены дела, документы, и иные носители информации.

4.9. По результатам проверок составляется акт.

4.10. При обнаружении утраты документов, разглашения информации и признаков несанкционированного ознакомления с конфиденциальными документами, работник обязан доложить ответственному за организацию обработки персональных данных УСЗН, далее по распоряжению начальника УСЗН проводится служебное расследование.

4.11. Утрата конфиденциальных документов, разглашение информации ограниченного доступа, незаконное ознакомление с информацией ограниченного доступа, влечет ответственность, предусмотренную действующим законодательством Российской Федерации.

Приложение
к Положению о порядке
обработки персональных данных в УСЗН
без использования средств автоматизации

**Список мест хранения
материальных носителей персональных данных**

№	Физическое место расположения	Должность допущенного должностного лица	Кому принадлежат персональные данные
1		<i>Ответственный за организацию обработки персональных данных, ответственный за обеспечение безопасности персональных данных, администратор безопасности ИСПДн, руководитель, главный бухгалтер, бухгалтер</i>	<i>Персональные данные работников (автоматизированная обработка, обработка без использования средств автоматизации)</i>
2			