Приложение № 7
к Приказу № 147
от 30.12.2021г.

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Муниципального бюджетного учреждения социальной защиты «Комплексный центр социального обслуживания населения» Коркинского муниципального района (далее – КЦСОН), представляющих собой совокупность персональных данных, содержащихся в базах данных КЦСОН, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

1.2. 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.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.2. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.3. 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.

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

2.5. 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.

3. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных». Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

3.4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

3.5. В информационных системах персональных данных КЦСОН устанавливаются уровни защищенности персональных данных в зависимости от угроз безопасности этих данных в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства РФ от 1 ноября 2012г. № 1119.

3.6. 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.

3.7. В КЦСОН организован режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

3.8. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивают ответственный за обеспечение безопасности персональных данных и администратор безопасности.

4. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

4.1. При обработке персональных данных в информационной системе должно быть обеспечено:

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

4.1.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

4.1.3. предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

4.1.6. постоянный контроль над обеспечением уровня защищенности персональных данных.

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

4.2.1. определение угроз безопасности персональных данных при их обработке в ИСПДн;

4.2.2. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

4.2.3.оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

4.2.4.учет машинных носителей персональных данных;

4.2.5.установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

4.2.6.контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн;

4.2.7.ознакомление работников КЦСОН, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику КЦСОН в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе возлагается на администратора безопасности.

4.4. Список лиц, имеющих право доступа к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается директором КЦСОН.

4.5. Работники КЦСОН, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими трудовых обязанностей, для получения доступа к информационной системе направляют письменный запрос на имя ответственного за обеспечение безопасности персональных данных.

4.6. При обнаружении нарушений порядка предоставления персональных данных администратор безопасности незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

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

5. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ ИСПДН

5.1. В ИСПДн подлежат регистрации следующие события:

5.1.1. вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

5.1.2. подключение машинных носителей информации и вывод информации на носители информации;

5.1.3. запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

5.1.4. попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

5.1.5. попытки удаленного доступа.

5.2. Сроки хранения событий безопасности определяются заданными настройками средств защиты информации от несанкционированного доступа.

5.3. Состав и содержание информации о событиях безопасности:

5.3.1. типы события;

5.3.2. дата и время события;

5.3.3. идентификационной информации источника события безопасности;

5.3.4. результат события безопасности (успешно или неуспешно);

5.3.5. субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

5.4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения предусматривает:

5.4.1. возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени: обеспечивается возможностями операционной системы и средств защиты информации от несанкционированного доступа;

5.4.2. генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с п. 5.1 настоящего Положения с составом и содержанием информации, определенными в соответствии с п. 5.3 настоящего Положения.

5.4.3. хранение информации о событиях безопасности в течение времени, установленного в соответствии с п. 5.2 настоящего Положения.

5.5. Доступ к записям регистрации событий и функциям управления механизмами регистрации предоставляется только администратору безопасности и обслуживающему персоналу под контролем администратора безопасности.

Приложение № 8
к Приказу № 147
от 30.12.2021г.

ПОЛОЖЕНИЕ
о порядке обработки персональных данных 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 Муниципального бюджетного учреждения социальной защиты «Комплексный центр социального обслуживания населения» Коркинского муниципального района (далее – КЦСОН).

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, осуществляемой без использования средств автоматизации».

1.3. Перечень персональных данных, обрабатываемых в КЦСОН, утверждается директором КЦСОН.

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

1.5. Ответственный за организацию обработки персональных данных КЦСОН ответственен 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 субъект 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 ответственного за организацию обработки персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

2.2. 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.

2.3. 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.

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

3.1. Персональные данные при их обработке, осуществляемой 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, осуществляемой без использования средств автоматизации, наименование и адрес КЦСОН, 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 КЦСОН 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, осуществляемую 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 КЦСОН 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, осуществляемой 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. 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).

3.7. 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, 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 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.

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.

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 КЦСОН, далее 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.