Приложение №1

Утверждено приказом директора
ГКУ СО КК «Адлерский
реабилитационный центр»
№ 31 от «09» января 2018 г.

П О Л О Ж Е Н И Е
о порядке обработки персональных данных субъектов персональных данных в ГКУ СО КК «Адлерский реабилитационный центр» Россия, Краснодарский край, г. Сочи, ул. Кирова, 30, кв. 4б.

Общие положения

Настоящее положение о порядке обработки персональных данных субъектов персональных данных, в дальнейшем - Положение, разработано для обеспечения безопасности персональных данных при их обработке в государственном казённом учреждении социального обслуживания Краснодарского края «Адлерский реабилитационный центр», (далее - центр), а также защиты прав граждан при обработке их персональных данных, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящее Положение вступает в силу с момента его утверждения и действует до его отмены.

Все изменения в Положение вносятся приказом директора центра.

Настоящее Положение разработано в соответствии со следующими нормативно-правовыми актами Российской Федерации:

1. Конституция Российской Федерации;
2. Гражданский кодекс Российской Федерации;
3. Уголовный кодекс Российской Федерации;
4. Кодекс об административных правонарушениях Российской Федерации;
5. Трудовой кодекс Российской Федерации;
6. Указ Президента Российской Федерации от 06 марта 1997 года № 188 "Об утверждении перечня сведений конфиденциального характера";
7. Федеральный закон от 19 декабря 2005 года № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных";
8. Федеральный закон от 27 июля 2006 года №152-ФЗ "О персональных данных";
9. Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
10. Федеральный закон от 27 июля 2004 года № 79-ФЗ "О

государственной гражданской службе Российской федерации";

11. Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

12. Постановление Правительства Российской Федерации от 21 марта 2012 года № 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";

13. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Субъектами персональных данных являются:

1. работники учреждения;
2. уволенные сотрудники;
3. агенты/контрагенты по заключенным государственным контрактам, гражданско-правовым договорам и соглашениями;
4. граждане, обратившиеся в учреждение за получением государственных услуг.

Персональные данные субъектов являются конфиденциальной информацией.

Настоящее Положение устанавливает порядок обработки персональных данных субъектов персональных данных в учреждении и предназначено для выявления и предотвращения нарушений законодательства Российской Федерации в сфере персональных данных.

Под обработкой персональных данных понимаются действия (операции) с персональными данными, включающие:

1. сбор, запись, хранение, уточнение: обновление, изменение
2. систематизацию;
3. накопление;
4. использование;
5. извлечение;
6. распространение;
7. передачу;
8. обезличивание;
9. блокирование;
10. удаление;
11. уничтожение.

Настоящее Положение определяет минимальный необходимый набор мер, позволяющий предотвратить утечку сведений, относящихся к персональным данным.

Учреждение является оператором персональных данных субъектов, персональных данных, указанных в этом Положении. На основании соглашения/договора учреждение может поручать обработку персональных данных третьим лицам, с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации. Существенным условием соглашения/договора по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

Учреждение вправе получать и обрабатывать данные о частной жизни работников учреждения только с их письменного согласия в соответствии со статьёй 24 Конституции Российской Федерации.

Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

Основные понятия

В настоящем Положении используются следующие основные понятия:

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

Безопасность персональных данных - состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах.

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

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

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

Несанкционированный доступ (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.

Обработка персональных данных - любое действие/операция или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

Персональные данные - любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу - субъекту персональных данных.

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

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

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

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу.

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.

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.

Цель и содержание персональных данных

Целями обработки и содержанием персональных данных является:

1) выполнение функций, возложенных на учреждение трудовым законодательством, законодательством Российской Федерации о социальных гарантиях - Приложение № 4 «Перечень персональных данных, обрабатываемых в связи с реализацией трудовых отношений»;

2) предоставление (оказание) государственных услуг: выполнение функций, возложенных на учреждение трудовым законодательством, законодательством о государственной социальной обслуживании, законодательством Российской Федерации о социальных гарантиях - Приложение № 4 «Перечень персональных данных, обрабатываемых в связи с оказанием государственных услуг».

Персональные данные сотрудников учреждения обрабатываются в следующих отделах (подразделениях) учреждения в соответствии с исполняемыми функциями:

учреждение;

отделение диагностики и разработки планов социальной реабилитации;

отделение психолого-педагогической реабилитации.

Персональные данные граждан, обратившихся в учреждение, обрабатываются в следующих подразделениях учреждения:

учреждение;

отделение диагностики и разработки планов социальной реабилитации;

отделение психолого-педагогической реабилитации.

Правила обработки персональных данных

Все персональные данные субъектов учреждение получает на законной основе.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе.

Персональные данные ближайших родственников сотрудников необходимые для ведения кадрового учёта, учреждение получает от самих сотрудников, либо от их представителей.

Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных. Типовая форма согласия утверждается приказом.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права

и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

После установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта и с его письменного согласия. Типовая форма согласия утверждается приказом.

Учреждение вправе не осуществлять свои функции по обработке персональных данных в отношении субъекта персональных данных при предоставлении неполных или недостоверных персональных данных, а также в случае письменного отказа на обработку персональных данных.

Персональные данные субъектов учреждения обрабатываются в подразделениях в соответствии с определенными для них функциями.

Доступ лиц к персональным данным, обрабатываемым в информационной системе персональных данных, осуществляется в соответствии со списком, утверждённым приказом.

Уполномоченные лица учреждения имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с утверждённым приказом списком.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённого Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Персональные данные при этом виде обработки должны отделяться от иной информации в специальный подраздел полей форм (бланков), в частности путём фиксации их на отдельных материальных носителях персональных данных.

Хранение персональных данных предусматривает осуществление фиксации их в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии с утверждённым списком.

Персональные данные подлежат уничтожению либо обезличиванию при:

- достижении целей либо утрате необходимости в их достижении;
- отзыва согласия субъекта персональных данных;
- выявления неправомерной обработки персональных данных; если иное не предусмотрено Федеральным законом.

При установлении факта, что персональные данные являются неполными, неточными или неактуальными учреждение вносит необходимые изменения в персональные данные в течение не более 7 рабочих дней со дня предоставления их субъектом, или его представителем, после чего уведомляет субъекта о внесении изменения.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, либо с момента отзыва согласия субъекта, если иное не предусмотрено Федеральными законами.

При выявлении неправомерной обработки персональных данных их уничтожение осуществляется в срок, не превышающий 10 рабочих дней с момента обнаружения. Учреждение уведомляет об этом субъекта или его законного представителя.

Уничтожение персональных данных, являющихся незаконно полученными или не являющимися необходимыми для заявленной цели обработки, осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом или его представителем документов, подтверждающих эти сведения.

Уничтожение персональных данных на бумажных носителях осуществляет комиссией в составе руководителя и сотрудников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого подразделения.

Уничтожение достигается путём измельчения шредером. При этом составляется "Акт уничтожения документов учреждения, содержащих персональные данные субъекта". Форма акта утверждается приказом директора учреждения.

Допускается уничтожение производить в специализированных организациях в присутствии комиссии, ответственной за уничтожение документов, что оформляется актом уничтожения с приложением накладной на передачу уничтожаемых документов.

Уничтожение полей баз данных, содержащих персональные данные субъекта, выполняется по заявке начальника подразделения, обрабатывающего персональные данные субъекта и установившего необходимость их уничтожения. Оно осуществляется комиссией, в состав которой входят лица, ответственные за администрирование автоматизированных систем, в которых обрабатываются базы данных, сотрудники подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных учреждения, содержащих

персональные данные субъекта, достигается физическим разрушением носителя информации, либо затиранием информации на носителях (в том числе и в резервных копиях), исключающим в дальнейшем произвести считывание или - восстановление персональных данных. Об уничтожении нолей баз данных составляется "Акт уничтожения полей баз данных управления, содержащих персональные данные субъекта". Форма акта утверждается приказом. При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путём перезаписи полей баз данных, которые позволяют определить субъекта, данными, исключающими дальнейшее определение субъекта.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и/или договорными документами.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

Обработка биометрических персональных данных (отпечатки пальцев, сетчатки глаза, фотографии, и пр.), допускается при наличии письменного согласия субъекта, в соответствии со статьёй 11 Федерального закона от 27 июля 2006 года № 152- ФЗ "О персональных данных". Типовая форма согласия на обработку биометрических персональных данных утверждается приказом директора учреждения.

Сотрудники учреждения должны быть ознакомлены (под роспись) с требованиями законодательства регламентирующими обработку персональных данных, с настоящим Положением, другими документами учреждения, устанавливающими порядок обработки персональных данных, права и обязанности субъектов.

Передача персональных данных третьим лицам

При обработке персональных данных субъекта оператор должен соблюдать следующие требования:

не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев установленных законодательством. Типовая форма согласия на обработку персональных данных утверждается приказом директора учреждения;

предупреждать лиц, получающих персональные данные субъекта о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных;

при необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной

защиты прав субъектов персональных данных, учреждение запрашивает согласие субъекта в письменной форме.

Права субъектов персональных данных

В целях обеспечения своих интересов субъекты персональных данных имеют право:

получать полную информацию о своих персональных данных и обработке этих данных, в том числе автоматизированной;

осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законодательством;

требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением федерального закона. Субъект персональных данных при отказе учреждения исключить или исправить персональные данные имеет право заявлять в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

требовать от учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них;

обжаловать в суде любые неправомерные действия или бездействие управления при обработке и защите персональных данных субъекта.

Защита персональных данных субъекта

Защиту персональных данных субъектов от их неправомерного использования или утраты учреждение обеспечивает за счёт собственных ресурсов и средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

- руководящими документами ФСТЭК России - "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденными ФСТЭК России приказом № 21 от 18 февраля 2013 года;
- специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утверждёнными приказом

Государственной технической комиссии России от 30 августа 2002 года № 282 внутренними действующими нормативно-правовыми документами управления по обеспечению информационной безопасности.

Защита персональных данных предусматривает предотвращение несанкционированного доступа к персональным данным субъекта.

Доступ к персональным данным устанавливается в соответствие с матрицей доступа, утверждённой руководителем учреждения, при этом допущенные лица имеют право получать только те персональные данные, которые необходимы для выполнения установленных их регламентом действиями над персональными данными, и в целях, которые сообщены оператору персональных данных.

Ответственный за организацию обработки персональных данных, ответственный за администрирование средств защиты, техническое обслуживание информационных систем персональных данных назначаются приказом директора учреждения.

Начальник подразделения учреждения, осуществляющего обработку персональных данных:

несет ответственность за выполнение установленных требований по защите персональных данных в подразделении;

закрепляет за сотрудниками, уполномоченными обрабатывать персональные данные, конкретные носители с персональными данными, которые необходимы для выполнения возложенных на них обязанностей;

организует изучение нормативно-правовой базы по защите персональных данных и требует их неукоснительного исполнения;

обеспечивает режим конфиденциальности персональных данных, обрабатываемых в структурном подразделении;

организует контроль за соблюдением установленного уровня доступа к персональным данным в соответствии с регламентом сотрудников подразделения учреждения, осуществляющих обработку персональных данных.

Обязанности лиц, допущенных к обработке персональных данных

Сотрудники подразделения учреждения, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы управления по защите персональных данных;

2) хранить конфиденциальность персональных данных;

3) контролировать истечение срока действия согласий на обработку персональных данных и своевременно обеспечивать обновление согласий на обработку, или прекращение обработки персональных данных;

4) немедленно доводить до сведения начальник отдела (подразделения) обо всех фактах или попытках несанкционированного

доступа к персональным данным, других нарушениях защиты персональных данных;

5) обеспечивать сохранность закреплённых за ними носителей персональных данных.

Сотрудники, допущенные к персональным данным в установленном порядке дают письменное обязательство о неразглашении персональных данных субъектов обработки.

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и другой гражданско-правовой ответственности на основании судебного решения.

К данным лицам так же могут быть применены следующие дисциплинарные взыскания:

1) замечание;
2) выговор;
3) предупреждение о неполном должностном соответствии;

Порядок действий по запросам надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона от 27 июля 2006 года № 152 "О персональных данных" по запросу уполномоченного органа по защите прав субъектов персональных данных управление представляет информацию, необходимую для осуществления действий указанного органа предусмотренных законодательством Российской Федерации, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных, при необходимости с привлечением сотрудников учреждения.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган.

Заместитель директора
по административно-хозяйственной работе Д.В. Марков