

ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗУЕМЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящая Политика обработки персональных данных и реализуемых требований к защите персональных данных (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, и действует в отношении всей информации, которую государственное автономное учреждение социального обслуживания Оренбургской области «Реабилитационный центр «Проталинка» (далее - оператор), может получить в рамках осуществления своей деятельности. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предназначена для ознакомления неограниченного круга лиц.

В Политике определены требования к персоналу оператора, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных, в информационных системах персональных данных (ИСПДн) оператора.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью настоящей Политики, является обеспечение безопасности объектов защиты оператора в информационных системах от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

1.2. 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.

1.3. Информация и связанные с ней ресурсы должны быть доступны, для субъектов ПДн. Должно осуществляться своевременное обнаружение и реагирование на УБПДн,

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

1.5. Состав объектов защиты представлен в главе II «Правовой режим обработки персональных данных», подлежащих защите.

Область действия:

Требования настоящей Политики распространяются на всех работников оператора (штатных, временных, работающих по контракту и т.п.), а также воспитанников их родителей, (законных представителей) и всех прочих лиц (подрядчики, аудиторы и т.п.).

II. ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Субъекты персональных данных

В Учреждении обрабатываются персональные данные следующих категорий физических лиц (субъектов персональных данных):

- работников (лиц, состоящих в трудовых отношениях с Учреждением);
- работников по гражданско-правовым договорам;
- воспитанников, родителей, законных представителей;
- иных лиц, давших согласие на обработку своих персональных данных, либо сделавших общедоступными свои персональные данные или чьи персональные данные получены из общедоступного источника, а также в других случаях, предусмотренных законодательством Российской Федерации.

2.2. Категории обрабатываемых персональных данных

Учреждение обрабатывает следующие категории персональных данных:

2.2.1. Работники: фамилия, имя, отчество; данные паспорта (серия, номер, кем и когда выдан); дата и место рождения; адрес места жительства и регистрации; индивидуальный номер налогоплательщика (ИНН); страховое свидетельство государственного пенсионного страхования (СНИЛС); контактный телефон; сведения о доходах; информация об образовании; сведения о составе семьи; сведения о социальных льготах и др.

2.2.2. Воспитанники, родители, законные представители: фамилия, имя, отчество; данные свидетельства о рождении воспитанника; данные паспорта (серия, номер, кем и когда выдан); контактная информация (телефон, e-mail), адрес прописки, адрес проживания, место работы.

2.3. Цели обработки персональных данных

Учреждение осуществляет обработку персональных данных в следующих целях:

2.3.1. Работники: содействие в трудовой деятельности, обеспечение личной безопасности, учет результатов исполнения договорных обязательств, осуществление безналичных платежей на счет работника, обеспечение работоспособности и сохранности ресурсов и имущества работодателя, осуществление коллективного взаимодействия и совместного использования информационных ресурсов, аттестация, повышение квалификации, а также наиболее полное исполнение обязательств и компетенций в соответствии с Трудовым кодексом Российской Федерации, и другими нормативно-правовыми актами Российской Федерации в сфере трудовых отношений.

2.3.2. Воспитанники, родители, законные представители: с целью исполнения требований законодательства РФ (Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и других

нормативно-правовых актов Российской Федерации); с целью исполнения договорных отношений.

2.4. Правовое основание обработки персональных данных.

Учреждение осуществляет обработку персональных данных на основании:

2.4.1. Трудового кодекса Российской Федерации;

2.4.2. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

2.4.3. Устава Учреждения;

2.4.4. и иных нормативных актов.

2.5. Перечень действий с персональными данными

Учреждение осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных без использования средств автоматизации.

Учреждение может поручить обработку персональных данных третьим лицам в случаях, если:

— субъект дал согласие на осуществление таких действий (при наличии условий в договоре с третьим лицом о соблюдении им принципов и правил обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

— для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей;

— в других случаях, предусмотренных законодательством Российской Федерации. Трансграничная передача персональных данных не осуществляется.

2.6. Права субъекта

Субъект персональных данных, согласно законодательству Российской Федерации, имеет право:

А) получать информацию, касающуюся обработки своих персональных данных;

Б) 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;

В) требовать прекращения обработки своих персональных данных в случаях, предусмотренных законодательством Российской Федерации;

Г) обжаловать действия или бездействие Учреждения в судебном: порядке в случае нарушения им порядка обработки персональных данных субъекта;

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

2.7. Условия прекращения обработки персональных данных

Срок или условие прекращения обработки персональных данных в Учреждении:

- ликвидация Учреждения или прекращение деятельности;
- истечение 75 лет - хранение персональных данных работников;
- по исполнению обязательств по договорам и в течение срока исковой давности;

- отзыв согласия если иное не предусмотрено Федеральным законодательством, либо в течение срока хранения документов согласно установленным срокам хранения для определенных категорий документов, если иное не предусмотрено Федеральным законодательством.

2.8. Учреждение принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных,

К мерам, применяемым для защиты персональных данных, относятся:

- назначение сотрудника, ответственного за организацию обработки персональных данных;

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;

- разработка документов, определяющие политику Учреждения в отношении обработки, персональных данных, локальные документы по вопросам обработки персональных данных;

- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;

- опубликование в сети Интернет документа, определяющего политику Учреждения в отношении обработки персональных данных;

- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;

- осуществление контроля над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

2.9. Методы защиты персональных данных

Методами защиты персональных данных являются:

- реализация разрешительной системы допуска к обработке персональных данных;

- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также хранятся носители информации;

- разграничение доступа к персональным данным;

- регистрация действий сотрудников, контроль несанкционированного доступа к персональным данным;

- использование защищенных каналов связи.

III. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Сотрудники оператора, являющиеся пользователями информационных систем персональных данных (ИСПДн), должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

3.2. При вступлении в должность нового сотрудника непосредственный начальник, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ПК.

3.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн,

3.4. Сотрудники оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей, логинов и паролей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

3.5. Сотрудники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

3.6. Сотрудники оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

3.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

3.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам,

3.9. При работе с ЦДн на ПК сотрудники оператора обязаны обеспечить исключение возможности просмотра ЦДн третьими лицами с мониторов.

3.10. При завершении работы на ПК сотрудники обязаны защитить монитор с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

3.11. Сотрудники оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его

нарушение. Они должны быть ознакомлены под роспись с ответственностью, предусмотренной законодательством РФ.

3.12. Сотрудники обязаны без промедления сообщать обо всех подозрительных случаях работы ПК, способные повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

3.13. Должностные обязанности сотрудников, обрабатывающих персональные данные.

Должностные обязанности сотрудников, обрабатывающих персональные данные описаны в следующих документах:

— Положение регламентирующее порядок и условия обработки персональных данных, работников Учреждения;

— Должностная инструкция ответственного за организацию обработки персональных данных у оператора.

3.14. Ответственность сотрудников оператора:

3.14.1. Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного Кодекса Российской Федерации).

3.14.2. Сотрудники оператора несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

3.14.3. При нарушениях сотрудниками оператора правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

IV. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Изменение Политики

Учреждение имеет право вносить изменения в настоящую Политику. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.

4.2. Обратная связь

Государственное автономное учреждение социального обслуживания Оренбургской области «Реабилитационный центр «Проталинка» (ГАУСО «РЦ «Проталинка»), юридический адрес: 460051, г. Оренбург, пр. Гагарина, дом 43а, телефон: (3532) 43-10-12.