Приложение 1
к Приказу «О проведении работ по защите персональных данных» от 15.08.2016г. №35

УТВЕРЖДАЮ

Директор государственного бюджетного учреждения Самарской области "Реабилитационный центр для инвалидов "Доблесть"

_____Хромцова Ирина Владимировна

"15" августа 2016г.

ПОЛОЖЕНИЕ
по защите персональных данных государственного бюджетного учреждения Самарской области "Реабилитационный центр для инвалидов "Доблесть"

2016г.

СОДЕРЖАНИЕ

1. Общие положения

государственное бюджетное учреждение Самарской области «Реабилитационный центр для инвалидов «Доблесть» - далее «Учреждение», являясь Работодателем (Оператором), осуществляет работу с персональными данными Работников ГБУ СО РЦ «Доблесть» (субъекта персональных данных), руководствуясь соответствующими нормами Конституции РФ (Российской Федерации), Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных", а также общепризнанными принципами и нормами международного права и международных договоров РФ, которые в соответствии с ч. 4 ст. 15 Конституции РФ являются составной частью российской правовой системы. ГБУ СО РЦ «Доблесть» подразделяется на два отделения – стационарное и полустационарное.

Так, в соответствии с частью первой ст. 23 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

1.1. Цель разработанного регламента.

1.1.1. Целью является защита персональных данных от несанкционированного доступа третьих лиц и организация приема, хранения, обработки и передачи персональных данных Работников в соответствии с установленными законодательными требованиями.

1.2. Режим конфиденциальности.

1.2.1. Сбор, хранение, использование и распространение информации о частной жизни Работника без письменного его согласия не допускаются. Персональные данные относятся к категории конфиденциальной информации.

1.2.2. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством РФ.

1.2.3. 1.3. Порядок утверждения данных правил, ввода их в действие и внесенияизменений, утверждаются Директором ГБУ СО РЦ «Доблесть».

Вводятся в действие приказом по учреждению.

2. Основные понятия. Состав персональных данных работников.

2.1. Основные понятия.

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

доступ к информации – возможность получения информации и ее использования.

защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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.

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту 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;

общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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;

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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;

целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.2. Состав персональных данных – документы, из которых могут быть получены Работодателем персональные данные Работника:

2.2.1. Паспорт или иной документ, удостоверяющий личность;

2.2.2. Трудовая книжка;

2.2.3. Страховое свидетельство государственного пенсионного страхования;

2.2.4. Документы воинского учета;

2.2.5. Документ об образовании, о квалификации или о наличии специальныхзнаний или специальной подготовки;

2.2.6. Дополнительные документы (справка о доходах с предыдущего места работы, справка из органов государственной налоговой службы о предоставлении сведений об имущественном положении, медицинское заключение о состоянии здоровья и др.)

2.2.7. Автобиографические данные:

- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- сведения о социальных льготах;
- адрес места жительства;
- место рождения;
- домашний телефон;
- место работы или учебы членов семьи и родственников.

2.2.8. Сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющих идентифицировать его личность.

2.2.9. Сведения о заработной плате.

2.2.10. Дела, содержащие материалы по повышению квалификации и переподготовке Работников, их аттестации, служебным расследованиям.

2.2.11. Основания к приказам по личному составу.

2.2.12. Подлинники и копии приказов по личному составу.

2.2.13. Состав декларируемых сведений о наличии материальных ценностей.

2.2.14. Содержание декларации, подаваемой в налоговую инспекцию.

Персональные данные относятся **к категории конфиденциальной информации,** которые указаны в Перечне сведений конфиденциального характера (утвержден **Указом Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»**).

Работодатель, получающий доступ к персональным данным, должен обеспечить конфиденциальность таких данных.

3.Обязанности работодателя

Правоотношения в сфере персональных данных регулируются федеральным законодательством РФ (Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»), Трудовым кодексом РФ (глава 14), а так же Гражданским кодексом РФ.

Постановлением Правительства РФ от 15 сентября 2008 г. № 687утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации**.**

Рассмотрим обязанности работодателя в ст.18-21 Закона №152-ФЗ от 27 июля 2006г.

3.1.Обязанности работодателя при сборе персональных данных (статья 18)

1. При сборе персональных данных «Работодатель» обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 4 статьи 14 настоящего Федерального закона.

(Часть 4. Статья 14. Субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных «Работодателем», а также цель такой обработки;
2) способы обработки персональных данных, применяемые «Работодателем»,;
3) сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
4) перечень обрабатываемых персональных данных и источник их получения;
5) сроки обработки персональных данных, в том числе сроки их хранения;
6) сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.)

2. Если обязанность предоставления персональных данных установлена федеральным законом, «Работодатель»обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

3. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены «Работодателю» на основании федерального закона или если персональные данные являются общедоступными, «Работодатель» до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование (фамилия, имя, отчество) и адрес «Работодателя» или его представителя;
2) цель обработки персональных данных и ее правовое основание;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных.

3.2. Меры по обеспечению безопасности персональных данных при их обработке (Статья 19)

1. «Работодатель» при обработке персональных данных обязан принимать необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2. Правительство Российской Федерации устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации в соответствии с частью 2 настоящей статьи, осуществляются федеральными органами исполнительной власти, регулирующие вопросы использования и защиты персональных данных:

- Министерство связи и массовых коммуникаций Российской Федерации;

- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

- Федеральная служба по техническому и экспортному контролю

- Федеральная служба безопасности Российской Федерации;

4. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

3.3. Обязанности «Работодателя» при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных (Статья 20.)

1. «Работодатель» обязан в порядке, предусмотренном статьей 14 настоящего Федерального закона, сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту

персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

2. В случае отказа в предоставлении субъекту персональных данных или его законному представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя информации о наличии персональных данных о соответствующем субъекте персональных данных, а также таких персональных данных «Работодатель» обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий семи рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо с даты получения запроса субъекта персональных данных или его законного представителя.

3. «Работодатель» обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4. «Работодатель» обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.

3.4. Обязанности «Работодателя» по устранению нарушений законодательства, допущенных при обработке персональных данных, а также по уточнению, блокированию и уничтожению персональных данных (Статья 21)

1. В случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

2. В случае подтверждения факта недостоверности персональных данных «Работодатель» на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.

3. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными

данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных «Работодатель»обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных «Работодатель»обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных «Работодатель»обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

4. Обязанности работника

В числе обязанностей работника можно назвать обязанность передавать работодателю документы, содержащие персональные данные, перечень которых установлен трудовым и налоговым законодательством, а также своевременно сообщать работодателю об изменении персональных данных.

5. Права работника

(определяются в соответствии со статьей 89 Трудового кодекса Российской Федерации.)

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований настоящего Кодекса или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

6. Сбор, обработка и хранение персональных данных

Всю информацию работодатель собирает и хранит **исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.**

В целях исполнения федерального законодательства в сфере защиты конфиденциальной информации и персональных данных, «Работником» собственноручно подписывается Согласие на обработку персональных данных согласно приложениям №1, №2 к Трудовому договору.

Письменное согласие работника на обработку своих персональных данных включает в себя:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес Работодателя, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва.

До заключения трудового договора необходимо запросить усоискателя (кандидата на должность) необходимые для оформления на работу документы. Основной перечень указанных документов содержит Трудовой кодекс РФ. В соответствии со статьей 65 Трудового кодекса РФ лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

Все персональные данные работника (соискателя) следует получать у него самого. Если персональные данные работника (соискателя) могут быть получены только у третьей стороны, то работник (соискатель) должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Должностное лицо Работодателя должно сообщить работнику (соискателю) о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника (соискателя) дать письменное согласие на их получение.

В соответствии со ст.86 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных Работника должны соблюдать следующие общие требования:

- При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;
- При принятии решений, затрагивающих интересы Работника, **Работодатель не имеет права** основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- Защита персональных данных Работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств, в порядке, установленном федеральным законом;
- Работники не должны отказываться от своих прав на сохранение и защиту тайны;
- Работодатели, Работники и их представители должны совместно вырабатывать меры защиты персональных данных Работника.
- **«Работодатель» не имеет права** получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.
- **«Работодатель» не имеет права** получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

6.1.5. В соответствии с Федеральным законом от 21.07.2014 N 242-ФЗ с 1 сентября 2015 года статья 18 будет дополнена частью 5 следующего содержания:

"5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации **с использованием баз данных, находящихся на территории Российской Федерации**, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.".

6.2. Состав Работников, допущенных к обработке, передаче и хранению персональной информации

6.2.1. Полный доступ: к обработке, передаче и хранению персональных данных Работника могут иметь полный доступ следующие Работники:

- Директор ГБУ СО РЦ «Доблесть»
- главный бухгалтер
- бухгалтер
- инспектор по кадрам
- техник-программист
- сам Работник

6.2.2. Ограниченный доступ: к обработке, передаче и хранению персональных данных Работника могут иметь ограниченный доступ следующие Работники:

Наименование должности	Персональные данные и перечень документов, к которым может быть допущен. А также цели, для которых данное должностное лицо имеет право обрабатывать данные сведения.
Юрисконсульт Экономист	-паспортные данные Работника (сведения о номере паспорта, дате, месте его выдачи, адрес места жительства) – для оформления документов (договоров, контрактов и др.)
Специалист по охране труда	- персональные данные Работника для оформления документов в области охраны труда;
Руководитель структурного подразделения, в котором работает Работник	- сведения о семейном положении, возрасте детей – для предоставления Работнику гарантий, установленных законодательно, в частности для решения вопроса о возможности привлечения к работе сверхурочно, к работе в выходные и праздники, для привлечения к работе ночью, отправления в командировки, тел. конт; - сведения о профессии, квалификации Работника, о его опыте работы и имеющимся профессиональным навыкам – для принятия решений о переводах, возложении дополнительных обязанностей; - медицинские ограничения (группа инвалидности, условия, прописанные в карте реабилитации) – для соблюдения установленных для Работника условий работы, решения вопроса о возможных переводах; - и т.д. указать подробно, исходя из специфики своей организации и особенностей распределения функций.

6.3.Ответственность за разглашение.

6.3.1. Все лица, непосредственно имеющие отношение к персональной базе данных, должны подписывать обязательство о неразглашении персональной информации Работников.

6.3.2. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

6.3.3. Руководитель, разрешающий доступ Работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

6.4.4. Каждый РаботникГБУ СО РЦ «Доблесть», получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

6.3.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

6.3.6. Ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, согласно действующего законодательства может быть дисциплинарной, административной, гражданско-правовой или уголовной в соответствии с федеральными законами.

7. Передача персональных данных работника.

При передаче персональных данных Работника Работодатель должен соблюдать следующие требования (статья 88 Трудового кодекса РФ):

- не сообщать данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные Работника в коммерческих целях без его

письменного согласия;

- предупредить лиц, получающих персональные данные Работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правильно соблюдено. Лица, получающие персональные данные Работника, обязаны соблюдать режим секретности (конфиденциальности).
- осуществлять передачу персональных данных Работника в пределах одной организации в соответствии с данным нормативным актом работодателя;
- разрешать доступ к персональным данным Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции;
- передавать персональные данные Работника представителям Работников в порядке, установленном настоящим Кодексом, и ограничивать эту информацию только теми персональными данными Работника, которые необходимы для выполнения указанными представителями их функций;
- все меры конфиденциальности при сборе, обработке и хранении персональных данных Работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации;
- не отвечать на вопросы, касающиеся персональных данных Работника по телефону или факсу. Передавать по телефону запрошенную третьими лицами, информацию только в присутствии Работника, либо с его письменного согласия.

Исключение – случаи, предусмотренные законодательством (представление сведений о доходах в налоговую, отчет в фонды).

8. Доступ к персональным данным

8.1. **Внутренний доступ.**

8.1.1. Право доступа к персональным данным «Работника», имеют лица, указанные в п.6.2.1 настоящего Положения. Другие Работники учреждения имеют доступ к персональным данным Работника только с письменного согласия самого Работника, субъекта данных.

8.1.2. По письменному заявлению «Работника»,«Работодатель» обязан не позднее трех рабочих дней со дня подачи этого заявления выдать Работнику копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказ об увольнении с работы; выписки из трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и представляться «Работнику» безвозмездно.

8.2. **Внешний доступ.**

8.2.1. К числу лиц, допущенных к персональным данным «Работника» имеют организации (и соответственно должностные лица, данных организаций) осуществляющие контрольные и надзорные функции, а также другие лица, установленные федеральными законами, в частности:

- ✓ инспекции труда (инспектора труда правового департамента и департамента охраны труда);
- ✓ прокуратура РФ;
- ✓ правоохранительные органы;
- ✓ налоговые инспекции;
- ✓ военкоматы;
- ✓ органы, осуществляющие миграционный учет иностранных граждан;
- ✓ органы ФСС РФ;

- ✓ органы Пенсионного фонда РФ;
- ✓ и т.д.

8.2.2. Органы и должностные лица, указанные в п.6.2.1., 8.2.1. настоящего Положения имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

8.2.3. Организации, в которые Работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным Работника только в случае письменного разрешения Работника.

8.2.4. Другие организации: сведения о работающем Работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления Работника с согласием (разрешением, просьбой предоставить сведения о Работнике).

8.2.5. Родственники и члены семей: персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника. В случае развода и отсутствия соглашения сторон об уплате алиментов, справка о заработной плате Работника может быть предоставлена в суд без его согласия, на основании письменного запроса и определения суда.

9. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.

9.1. Внутренняя защита

9.1.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных.

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации.

Для защиты персональных данных Работников Работодатель принимает следующие меры:

- ограничение и регламентация состава Работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между Работниками.
- рациональное размещение рабочих мест, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание Работником требований нормативно - методических документов по защите информации и сохранении тайны. Для этого со всеми Работниками, допущенными к персональным данным проводится при допуске и периодически соответствующий инструктаж и обучение;
- наличие необходимых условий, исключающих несанкционированный доступ в

помещения для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава Работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника.
- организация порядка уничтожения информации. Документы уничтожаются специально созданной комиссией с периодичностью раз в год. Способ уничтожения определяется данной комиссией;
- воспитательная и разъяснительная работа с Работниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами. Данная обязанность возложена на руководителей структурных подразделений, в подчинении которых находятся Работники, допущенные к персональным данным;
- Личные дела могут выдаваться на рабочие места только руководителю организации, Руководителю службы персонала и в исключительных случаях, по письменному разрешению руководителя организации, руководителю структурного подразделения.

9.1.2. Защита персональных данных Работника на электронных носителях: все папки, содержащие персональные данные Работника, защищены паролем, который сообщается руководителю службы персонала и руководителю отдела информационных технологий.

9.1.3. Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные Работника, хранятся в кабинете Отдела кадров, помещении бухгалтерии ГБУ СО РЦ «Доблесть», в специально отведенном для этого месте, с применением специального оборудования (металлические несгораемые шкафы, сейфы).

9.1.4.Ключи от специального оборудования в рабочее время хранятся у директора ГБУ СО РЦ «Доблесть», без права передачи третьим лицам, на время их отсутствия ключи хранятся у лица, исполняющего обязанности руководителя подразделения.

9.2. **Внешняя защита**

9.2.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, посетители, Работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в службе персонала.

9.2.2. Для защиты персональных данных Работников Работодатель соблюдает следующие меры:

- порядок приема, учета и контроля деятельности посетителей. Любой посетитель перемещается по территории ГБУ СО РЦ «Доблесть» только в сопровождении лица, к которому он пришел.
- пропускной режим учреждения. Каждое постороннее физическое лицо обязано зарегистрироваться на пункте охраны сообщив о себе следующие сведения: ф.и.о., причину посещения.

Данные сведения вносятся в журнал учета посетителей, ответственность за хранение которого несут дежурные охранники ООО ЧОО «Единство».

- технические средства сигнализации. Ответственность за их бесперебойной работой лежит на дежурных охранниках ООО ЧОО «Единство».
- порядок охраны территории, зданий, помещений, транспортных средств. Ответственность за охрану лежит на дежурных охранниках ООО ЧОО «Единство».
- требования к защите информации при интервьюировании и собеседованиях.

Контроль за соблюдением данного требования возложен на специалистов ГБУ СО РЦ «Доблесть».

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

11. Заключительные положения

11.1. Настоящее Положение по защите персональных данных Работников вступает в силу с момента его утверждения директором ГБУ СО РЦ «Доблесть» и действует до введения нового Положения по защите персональных данных Работников.

11.2. Ознакомление Работников с условиями настоящего Положения производится под роспись в листе ознакомления, являющимся неотъемлемой частью настоящего Положения по защите персональных данных Работников.

11.3. Роспись Работника в листе ознакомления с Положением по защите персональных данных Работников означает его согласие и обязательство исполнения.

Лист ознакомления

№ п/п	ФИО	Подпись	Дата ознакомления
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			

Лист ознакомления

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления

№ п/п	ФИО	Подпись	Дата ознакомления

Положение по защите персональных данных состоит из _____ листов включая ____ пронумерованных листов ознакомления.

государственное бюджетное учреждение Самарской области
«Реабилитационный центр для инвалидов «Доблесть»

П Р И К А З № 38

от 15.08.2016 г. г.Похвистнево

«О назначении ответственного
за организацию обработки персональных
данных»

Для организации обработки персональных данных и надлежащего контроля за безопасностью персональных данных

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в государственном бюджетном учреждении Самарской области "Реабилитационном центре для инвалидов "Доблесть" (далее Ответственный) следующего сотрудника:
   - Специалиста по кадрам – Черкасову Марину Владимировну

2. Возложить на Ответственного следующие обязанности:
- Контроль соблюдения сотрудниками, обрабатывающими персональные данные правил обеспечения безопасности персональных данных;
- Подготовку и внесение изменений в документы по защите персональных данных;
- Проведение внутренних проверок, согласно Плану.

3. В своей работе Ответственный должен руководствоваться:
- ФЗ «О персональных данных» от 27.07.2006г. № 152-ФЗ;
- Постановлением Правительства от 15.09.2007г. № 687;
- Постановлением Правительства от 01.11.2012г. №1119;
- Нормативными документами ФСТЭК России;
- Руководящими документами и инструкциями по обеспечению безопасности персональных данных государственного бюджетного учреждения Самарской области "Реабилитационного центра для инвалидов "Доблесть".

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор ГБУ СО РЦ "Доблесть" И.В. Хромцова