«УТВЕРЖДАЮ»
Директор ОБУСО «Вичугский КЦСОН»
_____Е.Б. СЛАБНОВА
« 19 » 03.2014 г. Приказ № 252 – Д

Положение по защите персональных данных

I. Общие положения

Бюджетное учреждение социального обслуживания Ивановской области "Вичугский комплексный центр социального обслуживания населения" - далее «Организация», являясь Работодателем, осуществляет работу с персональными данными Работников Организации, 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.

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.

1.2. Основания для разработки

1.2.1. Конституция РФ ст. 24.

В ст. 24 Конституции РФ закреплено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ч. 1), а органы государственной власти и местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом (ч. 2)

1.2.2. Трудовой Кодекс Российской Федерации (ТК РФ):

- ➔ Статья 85. Понятие персональных данных работника. Обработка персональных данных работника.
- ➔ Статья 86. Общие требования при обработке персональных данных работника и гарантии их защиты.
- ➔ Статья 87. Хранения и использование персональных данных работников.
- ➔ Статья 88. Передача персональных данных работника.
- ➔ Статья 89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя.
- ➔ Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

1.2.3. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных":

- ➔ Статья 5. Принципы обработки персональных данных
- ➔ Статья 6. Условия обработки персональных данных
- ➔ Статья 7. Конфиденциальность персональных данных

- ➔ Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных
- ➔ Статья 10. Специальные категории персональных данных
- ➔ Статья 12. Трансграничная передача персональных данных
- ➔ Статья 14. Право субъекта персональных данных на доступ к своим персональным данным
- ➔ Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных
- ➔ Статья 24. Ответственность за нарушение требований настоящего Федерального закона

1.2.4. Федеральный закон от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации» (СЗ РФ, 1995, № 8, ст. 609) в качестве одной из целей защиты
информации закрепил защиту конституционных прав граждан на сохранение
личной тайны и конфиденциальности персональных данных, имеющихся в
информационных системах (ст. 20).

1.2.5. Закон об электронной цифровой подписи (10.01.2002 г. № 1 - ФЗ)

1.2.6. Кодекс РФ «Об административных правонарушениях».

1.2.7. Уголовный кодекс РФ.

1.2.8. Гражданский Кодекс РФ.

1.3. Режим конфиденциальности

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

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

1.4. Порядок утверждения данных правил, ввода их в действие и внесения изменений

1.4.1. Утверждаются директором Организации.

1.4.2. Вводятся в действие приказом по организации.

1.4.3. Изменения вносятся приказом по организации.

II. Понятие и состав персональных данных

2.1. Понятие персональных данных

Персональные данные Работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (Статья 85 ТК РФ.)

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 (Статья 3 152- ФЗ)

Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных Работника.

2.2. Состав персональных данных

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 специальных знаний 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;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье

Сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющих идентифицировать его личность (ст.2, Федерального закона РФ № 24 - ФЗ от 20.02.95).

Сведения о заработной плате.

Содержание трудового договора.

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

Основания к приказам по личному составу.

Подлинники и копии приказов по личному составу.

Состав декларируемых сведений о наличии материальных ценностей.

Содержание декларации, подаваемой в налоговую инспекцию.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

III. Сбор, обработка и хранение персональных данных

3.1. Порядок получения персональных данных

3.1.1. Все персональные данные работника следует получить у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение. (Ст. 86 ТК РФ п. 3.)

3.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия. (Ст. 86 ТК РФ п. 4.)

3.1.3. Работодатель не имеет права получить и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом. (Ст. 86 ТК РФ п. 5.)

3.1.4. Работодатель не имеет права получать и обрабатывать информацию о

национальной принадлежности работника (Ст. 26 Конституции **РФ).**

3.2. Состав работников, допущенных к обработке, передаче и хранению персональной информации

3.2.1. К обработке, передаче и хранению персональных данных работника могут иметь доступ следующие работники:

Сотрудники бухгалтерии Организации;

Сотрудники службы персонала;

Сотрудники административно-хозяйственного отдела Организации.

3.3. Порядок обработки, передачи и хранения персональной информации

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

➔ Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении на службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

➔ 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 и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

➔ 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.

3.3.2. При передаче персональных данных работника работодатель должен соблюдать следующие требования (статья 88 ТК 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). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

➔ осуществлять передачу персональных данных работника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым работник должен быть ознакомлен под расписку;

➔ 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 сотрудника 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.

3.3.3. Порядок хранения и использования персональных данных работников в организации устанавливается работодателем с соблюдением Трудового кодекса. При этом 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 относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

➔ требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса. 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 суде любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

3.4. Ответственность за разглашение

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

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

3.4.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

3.4.4. Каждый сотрудник Организации, получающий для работы конфиденциальный

документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

3.4.5. 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.

3.4.6. Статья 90 ТК РФ устанавливает ответственность лиц, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, которые должны нести дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

IV. Доступ

4.1. Внутренний доступ.

4.1.1. Право доступа к персональным данным работника, за исключением лиц, закрепленных пунктом 3.2. данных правил имеют:

- ➔ Директор;
- ➔ Заместитель директора;
- ➔ Заместитель директора по воспитательно-реабилитационной работе;
- ➔ Работники, в обязанности которых входит ведение кадровой документации.
- ➔ Сотрудники бухгалтерии;
- ➔ Руководители структурных подразделений (имеют доступ к данным только своих сотрудников). При переводах - начальники отделов могут посмотреть личное дело переводимого сотрудника; Сотрудник организации - носитель этих данных;
- ➔ Другие сотрудники Организации имеют доступ к персональным данным работника только с письменного согласия самого работника, носителя данных.

4.1.2. Выдача трудовой книжки и копий документов, связанных с работой, производится в следующем порядке (ст. 62 ТК РФ):

➔ 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.

➔ При прекращении трудового договора работодатель обязан выдать работнику в день увольнения (последний день работы) трудовую книжку и по письменному заявлению работника копии документов, связанных с работой.

➔ В случае если в день увольнения работника выдать трудовую книжку невозможно в связи с отсутствием работника либо его отказом от получения трудовой книжки на руки, работодатель направляет работнику уведомление о необходимости явиться за трудовой книжкой либо дать согласие на отправление ее по почте. Со дня направления уведомления работодатель освобождается от ответственности за задержку выдачи трудовой книжки.

4.2. Внешний доступ

4.2.1. К числу массовых потребителей персональных данных вне Организации можно отнести государственные и негосударственные функциональные структуры:

- инспекции труда
- правоохранительные органы;
- налоговые инспекции;

- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

4.2.3. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции, в порядке, установленном законодательством РФ.

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

4.2.5. Другие организации: сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

4.2.6. Родственники и члены семей: персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. 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.

V. 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 Организации.

5.1. Внутренняя защита

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

Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании. Для защиты персональных данных работников необходимо соблюдать ряд мер: 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; наличие необходимых условий в помещении 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;
- ➔ своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- ➔ воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- ➔ не допускается выдача личных дел сотрудников на рабочие места руководителей. 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.

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

5.1.3. Защита персональных данных на бумажных носителях: все документы, содержащие персональные данные сотрудника, хранятся в кабинете отдела кадров, помещении бухгалтерии Организации, в специально отведенном для этого месте, с применением специального оборудования (металлические несгораемые шкафы, сейфы).

5.1.4. Ключи от специального оборудования в рабочее время хранятся у начальников вышеуказанных подразделений, без права передачи третьим лицам, на время их отсутствия ключи хранятся у лица, исполняющего обязанности руководителя подразделения.

5.2. Внешняя защита

5.2.1. 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 Организации, 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.

5.2.2. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ➔ порядок приема, учета и контроля деятельности посетителей;
- ➔ пропускной режим Организации;
- ➔ учет и порядок выдачи удостоверений;
- ➔ технические средства охраны, сигнализации;
- ➔ порядок охраны территории, зданий, помещений, транспортных средств;
- ➔ требования к защите информации при интервьюировании и собеседованиях.

VI. Видеонаблюдение.

С целью повышения эффективности обеспечения режима комплексной безопасности

Центра, защиты прав и законных интересов проживающих в ОВП и воспитанников

стационарного отделения реабилитации, раннего выявления причин и признаков нестандартных ситуаций, а также предупреждения противоправных действий на территории и в зданиях Центра, ведется режим видеонаблюдения.

Способы осуществления видеонаблюдения.

Видеонаблюдение осуществляется способами адекватным целям безопасности.

Режим видеонаблюдения.

1. Видеонаблюдение осуществляется постоянно.
2. О видеонаблюдении работники и посетители оповещаются надписями на видных местах.
3. Места размещения и перечень устанавливаемых видеокамер утверждаются приказом директора.
4. Отображение процесса видеозаписи производится на экранах, установленных в зданиях в зоне доступного наблюдения с целью своевременного реагирования на возникновение признаков и причин конфликтных, нестандартных и опасных ситуаций.
5. Система видеонаблюдения осуществляет запись информации на жесткий диск видеорегистратора, которая уничтожается автоматически по мере заполнения памяти жесткого диска в течение 20 дней с момента записи.
6. Система видеонаблюдения исключает скрытое видеонаблюдение и установку видеокамер в туалетных комнатах, спальных комнатах, комнатах для переодевания и приема пищи работников.

Просмотр, хранение данных видеонаблюдения и передача данных третьим лицам.

1. Доступ к просмотру записей видеонаблюдения, хранящимся установленный период на жестком диске видеорегистратора, имеют директор, заместители директора, заведующий Отделением, а также другие ответственные лица, утвержденные приказом директора.
2. Периодичность, а также сроки и даты просмотра записей видеонаблюдения, хранящимся установленный период на жестком диске видеорегистратора, устанавливаются приказами директора.
3. Ответственные лица, осуществляющие просмотр записи видеонаблюдения, обязаны:

- соблюдать принцип конфиденциальности;
- оперативно реагировать на выявленные правонарушения, нарушения прав и законных интересов воспитанников, другие нестандартные и опасные ситуации, незамедлительно сообщать о выявленных фактах Директору;
- сообщать Директору о возникших неполадках в системе видеонаблюдения.

4. В случае фиксирования камерами видеонаблюдения конфликтных, нестандартных и опасных ситуаций Директор приказом устанавливает специальный срок их хранения.
5. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях, по запросу следственных и судебных органов, а также по запросу граждан, изображенных на видеозаписи. Вопрос о передаче записей решает директор.

VII. Заключительные положения

7.1. Настоящее Положение по защите персональных данных работников вступает в силу с момента его утверждения директором и действует до введения нового Положения по защите персональных данных работников.

7.2. Ознакомление работников с условиями настоящего Положения производится под роспись в листе ознакомления, являющимся неотъемлемой частью настоящего

Положения по защите персональных данных работников.

7.3.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

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Лист ознакомления:

№ п/п	ФИО	Подпись	Дата ознакомления

Положение по защите персональных данных состоит из 25 листов включая пронумерованные листы ознакомления.