

**ИСПДн «Учреждение социального обслуживания»  
Положение о персональных данных**

**1. Общие положения**

1.1. Настоящее Положение о персональных данных (далее - Положение):

- а) Является основополагающим внутренним документом КГКУ «Бикинский психоневрологический интернат» (далее – Учреждение), регулирующим вопросы и правила обработки персональных данных (далее - ПДн);
- б) Устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн;
- в) Определяет категории обрабатываемых ПДн, а также цели их обработки.

1.2. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми актами РФ:

- а) Конституция Российской Федерации (от 25.12.1993);
- б) Федеральный закон «Об информации, Информационных технологиях и о защите информации» (N 149-ФЗ от 27.07.2006);
- в) Федеральный закон «О персональных данных» (N 152-ФЗ от 27.07.2006);
- г) Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (N 1119 от 01.11.2012);
- д) Постановление Правительства РФ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (N 687 от 15.09.2008);
- е) Постановление Правительства РФ «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» (N 211 от 21.03.2012);

ж) Иные нормативно-правовые акты, разработанные в соответствии с федеральным законом «О персональных данных».

1.3. ПДн относятся к категории конфиденциальной информации.

1.4. Учреждение обрабатывает следующие категории персональных данных:

- а) Персональные данные физических лиц, работающих по трудовому договору с Учреждением (далее - Работники);
- б) Персональные данные физических лиц, являющихся стороной договора гражданско-правового характера (далее - Контрагенты);
- в) Персональные данные физических лиц детей-инвалидов в возрасте от 4 до 18 лет с отклонениями в умственном развитии, нуждающихся по состоянию здоровья в постороннем уходе, бытовом обслуживании, социально-трудовой реабилитации, обучении и воспитании и их законных представителей (далее - Воспитанники и их законные представители);
- г) Персональные данные физических лиц законных представителей воспитанника.

1.5. Учреждение осуществляет обработку ПДн Работников 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.

1.6. Учреждение осуществляет обработку ПДн Контрагентов исключительно в целях исполнения договора гражданско-правового характера.

1.7. Учреждение осуществляет обработку ПДн Воспитанников и их законных представителей исключительно в целях осуществления социальной защиты детей-инвалидов, создания наиболее адекватных их возрасту и состоянию здоровья условий жизнедеятельности, осуществление мероприятий реабилитационного, адаптационного, медицинского, социального и лечебно-трудового характера, организации их отдыха и досуга, лечебно-оздоровительных и профилактических мероприятий, улучшения качества обслуживания, содержания и ухода детей-инвалидов, проведения санитарно-гигиенических и противоэпидемических мероприятий, создания условий для получения образования.

1.8. Настоящее Положение вступает в силу на основании приказа директора Учреждения.

1.9. Все изменения в Положение вносятся приказом директора Учреждения.

## **2. Основные термины и понятия**

2.1. Основные термины и понятия, указанные в п. 2 настоящего положения используются в иных локальных документах Учреждения, принимаемых по вопросу обработки персональных данных в информационной системе персональных данных «Учреждение социального обслуживания» (далее - ИСПДн).

2.2. Для целей настоящего положения используются следующие термины и понятия:

- а) Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- б) Субъект - субъект персональных данных;
- в) Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.3. Персональные данные Работников - информация, необходимая Учреждению для 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.

2.4. Персональные данные Контрагентов - информация, необходимая Учреждению для исполнения договора гражданско-правового характера.

2.5. Персональные данные Воспитанников и их законных представителей - информация, необходимая Учреждению в целях осуществления социальной защиты детей-инвалидов, создания наиболее адекватных их возрасту и состоянию здоровья условий жизнедеятельности, осуществление мероприятий реабилитационного, адаптационного, медицинского, социального и лечебно-трудового характера, организации их отдыха и досуга, лечебно-оздоровительных и профилактических мероприятий, улучшения качества обслуживания, содержания и ухода детей-инвалидов, проведения санитарно-гигиенических и противоэпидемических мероприятий, создания условий для получения образования.

### **3. Общие правила обработки персональных данных**

3.1. В Учреждении устанавливаются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

3.2. К обработке персональных данных допускаются только штатные работники, внесенные в список лиц, допущенных к обработке персональных данных и соответствующие должности, внесенной в перечень должностей работников, допущенных к обработке персональных данных.

3.3. При работе с персональными данными, в том числе при обработке персональных данных в ИСПДн, работники, допущенные к обработке персональных данных, руководствуются инструкцией пользователя ИСПДн.

3.4. Приказом директора Учреждения для ИСПДн назначается лицо, ответственное за организацию обработки персональных данных.

3.5. Лицо, ответственное за организацию обработки персональных данных, в своей деятельности руководствуется инструкцией лица, ответственного за организацию обработки персональных данных.

3.6. Лицом ответственным за организацию обработки персональных данных определяется список лиц, допущенных в помещения, в которых производится обработка персональных данных.

3.7. Лицом, ответственным за организацию обработки персональных данных, производится учет обращений субъектов персональных данных или их законных представителей.

3.8. Каждое лицо, допущенное к обработке персональных данных, обязуется не разглашать информацию конфиденциального характера, в том числе персональные данные, полученные в результате исполнения своих должностных обязанностей.

3.9. Все места хранения носителей информации должны быть учтены.

3.10. Все нормативные акты, указанные в п. 3.1-3.7 вступают в силу с момента их утверждения директором Учреждения и действуют бессрочно до замены их новыми актами.

#### **4. Правила обработки персональных данных в ИСПДн**

4.1. В Учреждении устанавливаются и соблюдаются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, обрабатываемых в ИСПДн.

4.2. Приказом директора Учреждения утверждается перечень информационных систем персональных данных.

4.3. Определение необходимого уровня защищенности ИСПДн осуществляется комиссией, утвержденной приказом директора Учреждения. В комиссию должны входить не менее трех человек из числа Работников Учрежде-

ния. По завершении процедуры классификации составляется Акт определения требуемого уровня защищенности ИСПДн.

4.4. Состав персональных данных, обрабатываемых в ИСПДн, а также цели их обработки определяются в перечне персональных данных.

4.5. Для ИСПДн приказом директора Учреждения назначается администратор информационной безопасности (далее – Администратор).

4.6. Администратор в своей деятельности руководствуется инструкцией администратора информационной безопасности.

4.7. К техническому обслуживанию средств и систем ИСПДн допускаются только лица, внесенные в список лиц, допущенных к техническому и программному обслуживанию ИСПДн.

4.8. К управлению конфигурацией ИСПДн и системы защиты персональных данных допускаются только лица, внесенные в список лиц, допущенных к управлению конфигурацией ИСПДн и системы защиты персональных данных.

4.9. Любые изменения в конфигурации ИСПДн, влияющие на защищенность персональных данных, обрабатываемых в ИСПДн должны быть учтены Администратором в журнале регистрации изменений в конфигурации ИСПДн

4.10. Администратор в согласовании с лицом, ответственным за организацию обработки персональных данных, составляет технический паспорт ИСПДн.

4.11. Для предотвращения возможных потерь информации с носителей, содержащих персональные данные, Администратором разрабатывается инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.12. Для защиты автоматизированных рабочих мест (далее – АРМ) лиц, допущенных к обработке персональных данных, от вирусов и шпионских программ, Администратором разрабатывается инструкция по организации антивирусной защиты.

4.13. Для защиты автоматизированных рабочих мест лиц, производящих обработку персональных данных от несанкционированного доступа, Администратором разрабатывается инструкция по организации парольной защиты.

4.14. Все съемные и машинные носители персональных данных подлежат учету. Администратором разрабатывается инструкция по порядку учета и хранения машинных и съемных носителей информации.

4.15. В случае если в информационной системе персональных данных имеется разграничение прав доступа пользователей к защищаемой информа-

ции, Администратор разрабатывает разрешительную систему доступа к информационным ресурсам.

4.16. Приказом директора Учреждения утверждается перечень регистрируемых событий безопасности. Администратор обеспечивает сбор, обработку, хранение и конфиденциальность таких событий.

4.17. Для определения вероятных нарушителей и актуальных угроз безопасности в ИСПДн Администратором оператора разрабатывается модель угроз безопасности персональных данных, обрабатываемых ИСПДн.

4.18. Ежегодно, не позднее 1 марта комиссия, указанная в п.4.3 разрабатывает план мероприятий по обеспечению защиты персональных данных на текущий год.

4.19. Лицо, ответственное за организацию обработки персональных данных производит учет всех мероприятий, направленных на обеспечение безопасности персональных данных, обрабатываемых в Учреждении в журнале учета мероприятий по защите персональных данных.

4.20. Все субъекты персональных данных, данные которых обрабатываются в ИСПДн, подтверждают свое согласие на обработку персональных данных в письменном виде.

4.21. Лицо, ответственное за организацию обработки персональных данных направляет и поддерживает в актуальном состоянии уведомление об обработке персональных данных в Учреждение Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Хабаровскому краю и Еврейской автономной области.

4.22. Все нормативные акты, указанные в п. 4.1-4.21 вступают в силу с момента их утверждения директором Учреждения и действуют бессрочно до замены их новыми актами.

4.23. Не допускается обработка персональных данных в ИСПДн:

- а) При отсутствии установленных и настроенных сертифицированных средств защиты информации;
- б) При отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.

4.24. При обработке персональных данных запрещается:

- а) Обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- б) Осуществлять ввод персональных данных под диктовку.

## **5. Правила обработки персональных данных без использования средств автоматизации**

5.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях.

5.2. При неавтоматизированной обработке персональных данных:

- а) Не допускается фиксация на одном бумажном носителе персональных данных, цели, обработки которых заведомо не совместимы;
- б) Персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- в) Документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- г) Дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.3. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание)

5.4. Факт уничтожения персональных данных оформляется внутренним актом, в котором указывается какие персональные данные, когда, кем и каким образом уничтожены.

## **6. Правила обработки персональных данных с применением средств криптографической защиты информации**

6.1. Двери помещений, где размещены средства криптографической защиты информации (далее - СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения) должны быть оснащены замками.

6.2. Двери Помещений должны быть постоянно закрыты на замок, за исключением необходимости санкционированного прохода.

6.3. Двери Помещений должны опечатываться по окончанию рабочего дня или оборудоваться соответствующим техническим устройством, сигнализирующем о несанкционированном вскрытии.

6.4. Администратором разрабатываются правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

6.5. Все пользователи, применяющие СКЗИ для обработки персональных данных в ИСПДн, должны быть ознакомлены с инструкцией по работе с СКЗИ, сертификатами ключей подписи, открытыми и закрытыми ключами электронной цифровой подписи.

6.6. К работе с СКЗИ допускаются только лица, внесенные в список лиц, допущенных к работе СКЗИ.

6.7. Перед внесением пользователя ИСПДн в списки лиц, допущенных к работе с СКЗИ, Администратор проводит инструктаж по работе с СКЗИ с записью в журнал учета проведения инструктажа пользователя, допущенного к работе с СКЗИ.

6.8. Администратор обязан вести учет всех СКЗИ, эксплуатационной и технической документации к ним и ключевых документов, используемых в ИСПДн.

6.9. Администратор обязан вести учет носителей с ключевой информацией.

## **7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

7.1. Лицо, ответственное за организацию обработки персональных данных, а также иные руководители Учреждения, разрешающие доступ Работников к документу, содержащему персональные данные, несут персональную ответственность за данное разрешение.

7.2. Защита прав субъектов персональных данных осуществляется судом, в целях пресечения неправомерного использования этих персональных данных, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального вреда.

7.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

## **8. Заключительные положения**

8.1. Администратор, лицо, ответственное за организацию обработки персональных данных, пользователи ИСПДн обязаны не реже одного раза в полгода ознакомляться с настоящим документом.

8.2. Администратор, совместно с лицом, ответственным за организацию обработки персональных данных, обязаны не реже одного раза в год пересматривать и приводить в соответствие законодательству и иных нормативных актов положения настоящего документа.