|  |
| --- |
| УТВЕРЖДЕНО |
| Приказом директора  КГАУСО «ПЦСОН» |
| № 68 от 05.11.2014г. |

**ПОЛОЖЕНИЕ**

**ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

**КГАУСО «ПЦСОН»**

**г.Владивосток**

**2014г.**

**ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящем документе используются следующие термины и их определения:

1) *персональные данные* — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) *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;

3) *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;

4) *автоматизированная обработка персональных данных* — обработка персональных данных с помощью средств вычислительной техники;

5) *распространение персональных данных* — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) *предоставление персональных данных* — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) *блокирование персональных данных* — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) *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;

9) *обезличивание персональных данных* — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) *информационная система персональных данных* — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1.Настоящее Положение определяет порядок и условия обработки ПДн в КГАУСО «ПЦСОН» (далее – Учреждение), включая порядок передачи ПДн третьим лицам, случаи взимания согласий субъектов ПДн и уведомления органа по защите прав субъектов ПДн, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиту ПДн, порядок внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.2. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом

1.3.3. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

**2. ЦЕЛИ ОБРАБОТКИ ПДн**

2.1. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2.Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.3. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Целями обработки персональных данных является оказание услуг клиентам Учреждения, а также ведение кадрового и бухгалтерского делопроизводства.

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

**3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

3.1. Защита ПДн представляет собой процесс, организуемый и поддерживаемый в Учреждении, с целью предупреждения несанкционированного доступа к охраняемой информации и исключения ее разглашения и утечки через различные каналы.

3.2. Защита ПДн предусматривает:

* определение уровня защищенности ПДн и мероприятий по их защите;
* ограничение свободного доступа к ПДн, путем установления порядка обращения с этой информацией и осуществление контроля за его соблюдением;
* договорное регулирование отношений с контрагентами по вопросам условий передачи и использования ПДн;
* применение при необходимости средств и методов технической защиты конфиденциальности ПДн;
* принятие иных мер, не противоречащих законодательству Российской Федерации.

3.3. Обеспечение защиты ПДн предусмотрено действующим законодательством Российской Федерации и является обязательной неотъемлемой составной частью деятельности как Учреждения в целом, так и всех его отделов и работников.

3.4. Защита ПДн от несанкционированного доступа или утечки по техническим каналам, обеспечение сохранности информации, создаваемой, обрабатываемой, передаваемой и хранящейся в электронном виде в информационно-вычислительных и телекоммуникационных сетях Учреждения осуществляется в соответствии с действующим законодательством Российской Федерации.

3.5. Работа с документами, содержащими ПДн, не допускает их свободной рассылки, публикации в СМИ, размещения в информационных системах общего пользования, в том числе в сети Интернет, разглашения сторонним юридическим и физическим лицам без согласия владельца ПДн.

3.6. Обезличивание или уничтожение ПДн производится по достижению целей обработки ПДн. Обезличивание или уничтожение ПДн производится ответственным за работу с ПДн

**4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В УЧРЕЖДЕНИИ**

4.1. В Учреждении обрабатываются ПДн следующих субъектов ПДн:

* работники
* кандидаты для приема на работу;
* клиенты (потребители услуг).
* иные физические лица, ПДн которых обрабатываются в Учреждении.

Данный перечень может пересматриваться по мере необходимости.

**5.УВЕДОМЛЕНИЕ В РОСКОМНАДЗОР ОБ ОБРАБОТКЕ ПДн**

5.1. В соответствии с Законом РФ «О персональных данных» Учреждение является оператором ПДн.

5.2. В соответствии с п.1 ст.22 ФЗ «О персональных данных» оператор ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн (в настоящее время Роскомнадзор) об обработке ПДн. Форма уведомления и порядок заполнения и направления в Роскомнадзор установлены в приложении к настоящему Положению. Форма уведомления разработана в соответствии с Приказом Роскомнадзора от 19 августа 2011 г. N 706

5.3. В случае неполноты или изменения сведений, указанных в уведомлении, Учреждение обязано уведомить об изменениях уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) в порядке, установленном Роскомнадзором.

5.4. Учреждение вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

**6. СОГЛАСИЕ НА ОБРАБОТКУ ПДн. СЛУЧАИ И ПОРЯДОК ПОЛУЧЕНИЯ СОГЛАСИЯ**

6.1. Обработка персональных данных допускается без согласия субъекта ПДН в следующих случаях:

1) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

2) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее — исполнение судебного акта);

3) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

4) обработка персональных данных необходима для исполнения договора (гражданско-правового или трудового), стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.2. Соискатели на вакансии Учреждения при заполнении анкет, должны предоставлять согласие на обработку персональных данных, указанных в анкетах, поскольку на момент прохождения собеседования и заполнения анкеты трудовые отношения между Учреждением и соискателем еще не возникли.

6.3. Получения согласия на обработку ПДн клиентов по гражданско-правовым договорам не требуется, если персональные данные передаются в момент и после заключения договора. В случае получения от субъекта ПДн заявки на бронирование до момента подтверждения бронирования и заключения договора, договорные отношения между Учреждением и субъектом не возникают, в связи с чем необходимо получение согласия на обработку ПДн.

6.4. В случае, если гражданско-правовой договор, заключаемый между Учреждением и клиентом (субъектом ПДн), предусматривает предоставление услуг иным, кроме клиента, подписавшего договор, лицам (родственники, сопровождающие и т. п.), то должно быть получено согласие от этих физических лиц на обработку ПДн. Клиент обязан оказывать Учреждению содействие на получение такого согласия на обработку ПДн от указанных лиц.

6.5. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением, в частности следующих случаев (полный перечень установлен п.2 ст. 10 Закона РФ «О защите персональных данных»,

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2.1) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

2.2) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

6.6. В случае трансграничной передачи ПДн сотрудников или клиентов Учреждения необходимо получать согласие субъектов ПДн на обработку ПДн. Трансграничная обработка осуществляется в соответствии с положениями ст. 12 Закона РФ «О персональных данных».

6.7. Порядок получения согласия на обработку ПДн:

6.7.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

6.7.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных, если это необходимо в целях исполнения заключенного договора с субъектом ПДн, а также в иных случаях, установленных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Закона РФ «О персональных данных».

6.7.3. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

6.8. Получение письменного согласия на обработку ПДн осуществляется сотрудником Учреждения, при получении ПДн от субъекта ПДн, путем оформления письменного согласия по форме, установленной в Учреждении.

**7. ПРАВА СУБЪЕКТА В ОТНОШЕНИИ ПДн, ОБРАБАТЫВАЕМЫХ В УЧРЕЖДЕНИИ**

7.1. Субъект персональных данных имеет право на получение информации (далее — сведения), касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

7.2. Субъект персональных данных вправе требовать от оператора уточнения его 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, а также принимать предусмотренные законом меры по защите своих прав.

7.3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7.4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Срок ответа на запрос — 30 дней.

7.5. В случае, если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.6.Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.7. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого

7.8. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены Учреждению на основании федерального закона или если персональные данные являются общедоступными, Учреждение до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

* наименование (фамилия, имя, отчество) и адрес субъекта или его представителя;
* цель обработки персональных данных и ее правовое основание;
* предполагаемые пользователи персональных данных;
* установленные настоящим Федеральным законом права субъекта персональных данных.

7.9. Если обязанность предоставления персональных данных установлена федеральным законом, Учреждение обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

**8. ПОРЯДОК ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

8.1. Учреждение, обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

8.2. В Учреждении в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» осуществлено определение уровня угроз и уровня защищенности ИСПДн Учреждения.

8.3. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн в Учреждении разработана частная модель угроз на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

8.4. В Учреждении в соответствии с нормативно-методическим документом ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» разработан и внедрен комплекс мер по защите и обеспечению безопасности ПДн.

8.5. Требования к работникам в связи с обработкой ПДн

8.5.1. Должностные обязанности работников установлены в должностных инструкциях, руководствах пользователей.

8.5.2. Обеспечение конфиденциальности ПДн, обрабатывающихся в Учреждении, является обязательным требованием для всех сотрудников, которым ПДн стали известны.

8.5.3. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения, а также должны подписать «Соглашение об обеспечении конфиденциальности персональных данных сотрудниками Учреждения», приведенного в Приложении к настоящему Положению.

8.5.4. В Учреждении организован процесс обучения использования средств защиты ПДн, эксплуатируемых в Учреждении. Обучение по данному направлению рекомендовано лицам, имеющим постоянный доступ к ПДн, и лицам, эксплуатирующим технические и программные средства ИСПДн и средств защиты ИСПДн. В обязательном порядке обучение должны проходить лица, ответственные за эксплуатацию средств защиты информации ИСПДн.

8.5.5. ПДн поступают в Учреждение при приеме новых сотрудников, заключении договоров, проведении собеседований, а также в иных случаях.

Сотрудники Учреждения, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

8.5.6. В случае нарушения установленного порядка обработки ПДн работники Учреждения несут ответственность в соответствии с разделом 12 настоящего Положения.

8.6. Доступ к ПДн.

8.6.1. В Учреждении установлен разрешительный порядок доступа к ПДн. Сотрудникам предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании решения Директора.

8.6.2. Сотрудники Учреждения, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей на основании перечня лиц, допущенных к работе с ПДн, который утверждается Директором.

8.6.3. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

8.6.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником по согласованию с Директором или председателем комиссии по ПДн.

8.6.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками Учреждения, без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома Директора Учреждения.

В случае, если сотруднику сторонней Организации необходим доступ к ПДн Учреждения, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней Организации и ее сотрудников по соблюдению требований текущего законодательства в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками Учреждения, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Учреждением с субъектом ПД.

8.6.6. Доступ сотрудника Учреждения к ПДн прекращается с даты прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы в Учреждении, должны быть переданы соответствующему должностному лицу Учреждения.

8.6.7. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Учреждения об утрате или недостаче носителей информации, составляющей ПДн, а также о причинах и условиях возможной утечки ПДн. В случае попытки посторонних лиц получить от работника ПДн, обрабатываемых в Учреждении, незамедлительно известить об этом соответствующее должностное лицо Учреждения.

8.7. ПДн субъектов на бумажных носителях, обрабатываемые Учреждением, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

8.7.1. Места хранения документов, содержащих ПДн:

* ПДн клиентов Учреждения (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн клиентов Учреждения, носители информации (флеш-карты, CD-диски, и т.п.)) хранятся в основном офисе Учреждения и филиалах, размещаются на полках и запираются на ключ. Ответственное лицо, осуществляющее контроль — Заместители директора по филиалам.
* ПДн сотрудников Учреждения — документы, носители информации (флеш-карты, СD-диски и т.п.) хранятся в шкафу кадровой службы и запираются на ключ. Ответственное лицо, осуществляющее контроль — Начальник отдела кадров и делопроизводства.
* Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

8.7.2.Места и порядок хранения иных носителей информации.

Иные носители информации могут храниться в в основном офисе Учреждения и его филиалах, размещаются на полках и запираются на ключ или же в шкафу (сейфе).

8.8. При работе с программными средствами автоматизированной системы Учреждения, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

8.9. При получении персональных данных сотрудником Учреждения, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника иного лица в обязательном порядке проводится проверка достоверности ПДн. Ввод персональных данных, полученных Учреждением, в автоматизированную систему осуществляется сотрудниками имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

8.10. Сотрудники, осуществляющие обработку ПДн должны быть ознакомлены с настоящими Правилами.

8.11. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется компьютер) установлены в соответствии с Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации")

8.11.1. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

8.11.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

* не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
* персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

8.11.3.При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее — типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, — при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8.12. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

8.13. Случаи уничтожения, блокирования и уточнения ПДн.

* В случае выявления недостоверных персональных данных или неправомерных действий с ними Учреждение при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных обязана осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки. Блокирование осуществляется на основании распоряжения (приказа) Директора Учреждения путем прекращения каких-либо действий с ПДн.
* В случае подтверждения факта неточности персональных данных Учреждение на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные (внести изменения) и снять их блокирование. Снятие блокирования осуществляется на основании приказа Директора.
* В случае выявления неправомерных действий с персональными данными Учреждение в срок, не превышающий трех рабочих дней с даты такого выявления, обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Учреждение в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязано уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано 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.
* В случае достижения цели обработки персональных данных Учреждение обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором с субъектом ПДн и уведомить об этом субъекта персональных данных или его законного представителя.
* В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней, с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом персональных данных. Об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных.
* 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).
* Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

8.13.1. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

* ПДн на бумажных носителях уничтожается путем использования Шредера (уничтожители документов), установленного в офисе Учреждения.
* ПДн, размещенная в памяти ПЭВМ уничтожается путем удаления её из памяти ПЭВМ.
* ПДн, размещенная на флеш-карте, CD-диске, ином носителе информации уничтожается путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

Об уничтожении носителя информации составляется Акт.

8.14. Требования к помещениям, в которых обрабатываются ПДн.

8.14.1. Доступ в помещения, в которых располагаются средства обработки ПДн, должен контролироваться.

8.14.2. Офис, и помещения филиалов Учреждения, по окончании рабочего дня и отсутствия сотрудников в офисе, помещениях, должны запираться, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

8.14.3. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

8.14.4. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

8.15. Требования к администраторам ИСПДн.

8.15.1. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в обязанности администраторов ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

8.15.2. В обязанности администраторов ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

8.15.3. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица не рекомендуется совмещать роли администратора ИСПДн и администратора ИСПДн в лице одного сотрудника.

8.15.4. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях, с которыми сотрудники, назначаемые на данные роли должны быть ознакомлены под роспись.

8.16. Организация внутреннего контроля обработки и обеспечения безопасности ПДн

8.16.1. Организация внутреннего контроля процесса обработки ПДн в Учреждении осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

8.16.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

* Обеспечение соблюдения сотрудниками Учреждения требований настоящего Положения и нормативно-правовых актов, регулирующих сферу персональных данных.
* Оценка компетентности персонала, задействованного в обработке ПДн.
* Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.
* Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.
* Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.
* Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.
* Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

8.16.3. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

**9. ОСОБЕННОСТИ ОБРАБОТКИ ПДН СОТРУДНИКОВ УЧРЕЖДЕНИЯ**

В настоящем разделе установлены дополнительные права и обязанности Учреждения и работников при обработке Пдн работников.

9.1. Персональные данные работника — информация, необходимая Учреждению в связи с трудовыми отношениями и касающаяся конкретного работника.

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

9.3. Учреждение не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами;

9.4. При принятии решений, затрагивающих интересы работника, Учреждение не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

9.5. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

9.6. Учреждение обязуется не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

9.7. Учреждение обязуется предупредить сотрудников, третьих лиц, получающих персональные данные работника (при его согласии), о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Режим конфиденциальности обеспечивается подписанием с лицом соглашения (Приложение к настоящему Положению). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном настоящим Кодексом и иными федеральными законами;

9.8. Доступ к персональным данным работников предоставляется сотрудникам Учреждения, указанным в Приложении к настоящему положению в целях исполнения ими должностных обязанностей по ведению кадрового делопроизводства, выполнения административно-хозяйственных и организационно-распорядительных функций.

9.9. Организация обязуется не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

9.10. Организация обязуется передавать персональные данные работника представителям работников в порядке, установленном настоящим Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

9.11. Работник имеет право на определение своих представителей для защиты своих персональных данных.

9.12. Учреждение обязано осуществлять передачу персональных данных сотрудников в пределах Учреждения в соответствии с настоящим Положением.

**10. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ**

10.1. Руководство Учреждения несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

10.2. Работники Учреждения несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

10.3. Работник Учреждения может быть привлечен к ответственности в случаях:

* умышленного или неосторожного раскрытия ПДн;
* утраты материальных носителей ПДн;
* нарушения требований настоящего Положения и других нормативных документов Учреждения в части вопросов доступа и работы с ПДн.

10.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Учреждению, его работникам, клиентам и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Юридическое лицо, нарушившее договорные обязательства по защите ПДн несет ответственность в соответствии с законодательством Российской Федерации.

**ЛИСТ ОЗНАКОМЛЕНИЙ  
с Положением об обработке и защите персональных данных  
КГАУСО «ПЦСОН»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№**  **п/п** | **Ф.И.О.** | **Должность** | 1. **Дата** | **Подпись** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | **Приложение № 1** |

**Согласие на обработку персональных данных**

Я (далее - Субъект), \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(фамилия, имя, отчество)*

документ удостоверяющий личность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ серия\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(кем и когда)*

проживающий(ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, даю свое согласие КГАУСО «ПЦСОН» (далее Опрератор), расположенному по адресу: Приморский край, г.Владивосток, ул.Иртышская, 8, на обработку своих персональных данных, на следующих условиях:

1.Оператор осуществляет обработку персональных данных Субъекта исключительно в целях (интересах) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

2. Перечень персональных данных передаваемых Оператору на обработку (ненужное вычеркнуть):

- фамилия, имя, отчество;

- дата и место рождения;

- пол;

- место жительства и регистрация;

- реквизиты документа, удостоверяющего личность;

- социальный статус;

- номер телефона;

- номер страхового свидетельства государственного пенсионного страхования;

- информация о трудовой деятельности, о трудовом стаже;

- номера лицевых счетов в банке;

- сведения о составе семьи;

- сведения о воинском учете;

- сведения о доходах граждан;

- сведения об актах гражданского состояния;

- сведения о зарегистрированных лицах в жилых помещениях, принадлежащих клиенту на праве собственности, или занимаемых им на ином законном праве (поквартирная карточка, выписка из домовой книги, похозяйственной книги);

- информация о состоянии здоровья (наличие инвалидности)

- иные данные, необходимые для получения мер социальной поддержки и субсидий.

3.Субъект дает согласие на обработку своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ №152 от 27.07.2006 г., а также на передачу такой информации в организации, задействованные в реализации мер социальной поддержки и помощи, в организации совершающие контроль за целевым использованием денежных средств, а так же в другие организации, в случаях, установленных федеральным законодательством, законодательством Приморского края, нормативными правовыми актами органов местного самоуправления.

Настоящие письменное согласие действует пожизненно и может быть отозвано, путем подачи письменного заявления в адрес КГАУСО «ПЦСОН».

Дата\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сведения о законном представителе или представителе по доверенности:

Фамилия\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Имя\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Отчество\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Адрес места жительства (пребывания)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Реквизиты документа, удостоверяющего личность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Реквизиты документа, удостоверяющего полномочия\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Согласие зарегистрировано в журнале регистрации заявлений №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_г.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Приложение № 2** |

**Отзыв согласия на обработку персональных данных**

|  |  |
| --- | --- |
|  | Наименование оператора  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Адрес оператора  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Ф.И.О. субъекта персональных данных  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Адрес, где зарегистрирован субъект  персональных данных  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Номер основного документа, удостоверяющего  его личность  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Дата выдачи указанного документа  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Наименование органа, выдавшего документ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Заявление**

Прошу Вас прекратить обработку моих персональных данных в связи с\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать причину)

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (расшифровка подписи)

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Приложение № 3** |

Директору

КГАУСО «ПЦСОН»

В.А.Логачеву

**Заявление-согласие**

субъекта на получение его персональных данных у третьей стороны.

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_, выданный\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии со статьей 86 Трудового Кодекса Российской Федерации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(согласен/не согласен)

на получение моих персональных данных, а именно:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.)

для обработки в целях\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указать цели обработки)

У следующих лиц \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

« \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

|  |  |  |
| --- | --- | --- |
|  |  | **Приложение № 4** |

Директору

КГАУСО «ПЦСОН»

В.А.Логачеву

**Заявление-согласие**

субъекта на передачу его персональных данных третьей стороне.

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_, выданный\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в соответствии со статьей 88 Трудового Кодекса Российской Федерации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(согласен/не согласен)

на получение моих персональных данных, а именно:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.)

для обработки в целях\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указать цели обработки)

У следующих лиц \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

« \_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Приложение № 5** |

**УТВЕРЖДЕНО**

Приказом директора

КГАУСО «ПЦСОН»

№ 68 от 05.11.2014 г.

**ИНСТРУКЦИЯ**

**о порядке доступа в помещения, где обрабатываются персональные данные и к информационным системам персональных данных**

1. Общие положения

1.1. Настоящая инструкция определяет порядок доступа в помещения, где обрабатываются персональные данные и к информационным системам персональных данных (далее – ИСПДн) в подразделениях КГАУСО «ПЦСОН» (далее по тексту – Учреждение).

1.2. Перечень сотрудников, допущенных к работе с персональными данными в ИСПДн определяется приказом Директора

1.3. В своей работе сотрудники, допущенные к обработке персональных данных, должны строго руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и последующих нормативных правовых документов Правительства РФ, ФСТЭК России, ФСБ России, а также настоящей Инструкцией.

1.4. Ответственность за обеспечение безопасности персональных данных и надлежащего режима доступа к ИСПДн возлагается на руководителя структурного подразделения.

1.5. Помещения, в которых обрабатываются персональные данные, должны быть защищены от физического проникновения посторонних лиц. Доступ лиц, не причастных к непосредственной обработке персональных данных в эти помещения должен быть ограничен, а к рабочему месту оператора, обрабатывающего персональные данные исключен.

1.6. В помещениях, где обрабатываются персональные данные, должны быть установлены шкафы (сейфы) для хранения электронных носителей и машинных документов (распечаток). Ключи от шкафов (сейфов) хранятся у ответственных лиц, назначаемых приказом Директора.

1.7. Доступ к персональным данным и средствам их обработки должен контролироваться и быть только авторизованным. Должны применяться средства аутентификации. Вся информация о доступе в ИСПДн должна протоколироваться.

1.8.Запрещается хранение персональных данных на дисках с общим доступом (сетевом диске).

1.9. Права доступа должны подвергаться регулярному анализу и обновлению.

1.10. Оборудование должно располагаться с учетом требований минимизации доступа в рабочее помещение лиц, не связанных с обслуживанием этого оборудования.

1.11. Системы обработки и хранения персональных данных должны быть расположены так, чтобы исключить возможность случайного или преднамеренного доступа к ним неуполномоченных лиц в процессе их обработки.

1.12. Пользователи ПЭВМ, занятые обработкой персональных данных, обязаны:

* пройти инструктаж о выполнении правил разграничения доступа к защищаемой информации;
* знать и соблюдать требования по безопасности персональных данных, в части их касающихся;
* строго следить за соблюдением режима разграничения доступа, незамедлительно информировать непосредственного руководителя и о всех случаях утечки или разрушения обрабатываемой на ПЭВМ защищаемой информации;
* перед началом обработки на ПЭВМ персональных данных убедиться в отсутствии в помещении посторонних лиц.

1.13. Для осуществления контроля и поддержания надлежащего режима обработки персональных данных, руководитель Подразделения обязан систематически проводить воспитательную работу с лицами, осуществляющими обработку на ПЭВМ защищаемой информации, с целью повышения их бдительности и персональной ответственности.

**Приложение № 6**

**УТВЕРЖДЕНО**

Приказом директора

КГАУСО «ПЦСОН»

№ 68 от 05.11.2014 г.

**ИНСТРУКЦИЯ**

**пользователю автоматизированных систем, предназначенных для обработки персональных данных, в структурных подразделениях**

**КГАУСО «ПЦСОН»**

1. Общие обязанности пользователей по обеспечению безопасности персональных данных:

1.1. Каждый пользователь, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению (далее АС), несет персональную ответственность за свои действия и обязан:

1.1.1. Знать и выполнять требования нормативных правовых актов, затрагивающие вопросы защиты информации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

1.1.2. Выполнять указания ответственных за обеспечение безопасности информации.

1.1.3. Соблюдать режим допуска в помещения, где проводится обработка персональных данных.

1.1.4. Соблюдать режим разграничения доступа к персональным данным.

1.1.5. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами АС.

1.1.6. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АС.

1.1.7. Хранить в тайне от других свой пароль и менять его с установленной периодичностью.

1.1.8. В случаях убытия в отпуск (командировку) передавать для хранения установленным порядком свое устройство личной идентификации, личную ключевую дискету и другие реквизиты разграничения доступа (при необходимости их использования) только ответственному лицу за обеспечение безопасности персональных данных, назначенному приказом Директора.

1.1.9. Выполнять установленные требования по организации антивирусной защиты в части, касающейся действий пользователей АС.

1.1.10. Обращаться за помощью и консультациями к администратору вычислительной сети в случаях нарушения нормального режима работы средств вычислительной техники АС, а также в случаях возникновения трудностей при выполнении работ.

1.1.11. Для обеспечения целостности персональных данных, руководствоваться Регламентом по организации антивирусной защиты.

1.1.12. При передаче персональных данных по открытым каналам связи использовать средства криптографической защиты информации.

1.1.13. Соблюдать требования по учету, хранению и использованию электронных носителей информации и материальных носителей, предназначенных для хранения персональных данных.

1.1.14. Незамедлительно информировать непосредственного руководителя обо всех случаях несанкционированного доступа или нарушения целостности персональных данных.

1.1.15. Немедленно поставить в известность руководителя своего подразделения в случаях:

1. утери персональной ключевой дискеты, устройства личной идентификации;
2. при подозрении компрометации личных ключей и паролей;
3. при обнаружении: изменений в размещении средств вычислительной техники АС;
4. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС;
5. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПВЭМ, выхода из строя или неустойчивого функционирования узлов ПВЭМ или периферийных устройств (дисководов, принтера и.т.п), а также перебоев в системе электроснабжения;
6. некорректного функционирования установленных на ПВЭМ технических средств защиты;
7. непредусмотренных формуляром на ПВЭМ отводов кабелей и подключенных устройств.

1.2. Пользователь несет персональную ответственность за полноту и своевременное выполнение требований федеральных законов, нормативных документов в области безопасности персональных данных и настоящей Инструкции.

1.3. Пользователям запрещается:

1.3.1. Использовать компоненты средств вычислительной техники АС в неслужебных целях.

1.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПВЭМ или устанавливать дополнительно любые программные и аппаратные средства.

1.3.3. Осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц.

1.3.4. Записывать и хранить персональные данные на неучтенных носителях информации.

1.3.5. Оставлять включенной без присмотра на любое время АС, не активировав средства защиты от НСД (временную блокировку экрана и клавиатуры).

1.3.6. Передавать третьим лицам свою персональную ключевую дискету и личные идентификаторы кроме, ответственного лица за обеспечение безопасности персональных данных.

1.3.7. Создавать неучтенные копии ключевой дискеты и личных идентификаторов.

1.3.8. Снимать с дискеты защиту записи и вносить какие-либо изменения в файлы ключевой дискеты и личных идентификаторов.

1.3.9. Использовать свою ключевую дискету и личные идентификаторы для формирования цифровой подписи любых электронных документов, кроме как регламентированных технологическим процессом на рабочем месте.

1.3.10. Оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету и личный идентификатор, машинные носители и распечатки, содержащие персональные данные.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | **Приложение № 7** |

**Соглашение**

**о неразглашении персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, понимаю, что получаю доступ к персональным данным работников КГАУСО «ПЦСОН».

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных работников КГАУСО «ПЦСОН» и лиц связанных с Учреждением договорными отношениями.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения, о работниках КГАУСО «ПЦСОН» и лицах связанных с Учреждением договорными отношениями:

* 1. анкетные и биографические данные;
  2. сведения об образовании;
  3. сведения о трудовом и общем стаже;
  4. сведения о составе семьи;
  5. паспортные данные;
  6. сведения о воинском учете;
  7. сведения о заработной плате сотрудника;
  8. сведения о социальных льготах;
  9. специальность;
  10. занимаемая должность;
  11. наличие судимостей;
  12. адрес места жительства;
  13. домашний телефон;
  14. место работы или учебы членов семьи и родственников;
  15. характер взаимоотношений в семье;
  16. содержание трудового договора;
  17. состав декларируемых сведений о наличии материальных ценностей;
  18. содержание декларации, подаваемой в налоговую инспекцию;
  19. подлинники и копии приказов по личному составу;
  20. личные дела и трудовые книжки сотрудников;
  21. основания к приказам по личному составу;
  22. дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
  23. копии отчетов, направляемые в органы статистики.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать лицу ответственному за организацию обработки персональных данных.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации. Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2014г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись) (расшифровка подписи)

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Приложение № 8** |

**УТВЕРЖДАЮ**

Директор КГАУСО «ПЦСОН»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/В.А. Логачёв

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года

**АКТ № \_\_\_\_\_\_**

**Определения уровня защищенности информационной системы персональных данных КГАУСО «ПЦСОН»**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование информационной системы персональных данных)

Комиссия в составе:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Председатель: |  | | Должность, Фамилия, Имя, Отчество | |
| члены комиссии: | - | Должность, Фамилия, Имя, Отчество | |
|  | - | Должность, Фамилия, Имя, Отчество | |

рассмотрев исходные данные информационной системы персональных данных (ИСПДн) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование информационной системы персональных данных)\*

в соответствии с требованиями Постановления Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определили:

1. Уровень защищенности ИСПДН «\_\_\_\_\_\_\_\_»: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Информационные системы персональных данных, по заданным оператором характеристикам безопасности относятся к: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Структура информационной системы: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Местонахождения информационных систем персональных данных: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена:

(имеются/ не имеются)\*

1. Режим обработки персональных данных в информационной системе:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(однопользовательский / многопользовательский)\*

1. Разграничение прав доступа пользователей:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(с разграничением / без разграничения)\*

По результатам анализа исходных данных информационной системы

(наименование информационной системы персональных данных)\*

комиссией присвоен \_\_\_\_\_\_\_\_ класс АС и \_\_\_\_\_\_ уровень защищенности.

|  |  |  |
| --- | --- | --- |
| Председатель: |  | Фамилия, инициалы |
| Члены комиссии: |  | Фамилия, инициалы |
|  |  | Фамилия, инициалы |

\*- при заполнении бланка не указываются

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | **Приложение № 9** |

**Журнал учета передачи персональных данных**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Отметка о передаче или отказе в передаче персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | **Приложение № 10** |

**Журнал учета обращений субъектов персональных данных о выполнении их законных прав**

**в области защиты персональных данных**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Сведения о запрашивающем лице | Краткое содержание обращения | Цель получения информации | Отметка о предоставлении или отказе в предоставлении информации | Дата передачи/отказа в предоставлении информации | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Приложение № 11** |

**УТВЕРЖДЕНО**

Приказом директора

КГАУСО «ПЦСОН»

№ 68 от 05.11.2014 г.

**ИНСТРУКЦИЯ**

**по использованию и хранению съемных носителей информации, содержащих персональные данные**

1. Основные термины, сокращения и определения

* 1. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
  2. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
  3. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
  4. Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.
  5. ПК – персональный компьютер.
  6. ПО – Программное обеспечение вычислительной техники.
  7. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
  8. Пользователь – работник КГАУСО «ПЦСОН» (далее по тексту – Учреждение), использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.
  9. Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2. Порядок использования носителей информации

2.1. Под использованием носителей информации в ИС структурного подразделения понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

2.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Учреждения и подвергаются регулярной ревизии и контролю.

2.3. К предоставленным носителям персональных данных предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

2.4. Носители персональных данных предоставляются сотрудникам структурных подразделений по инициативе Руководства Учреждения в случаях:

1. необходимости выполнения вновь принятым работником своих должностных обязанностей;
2. возникновения у сотрудника структурного подразделения производственной необходимости.

**3. Порядок учета, хранения и обращения со съемными носителями ПДн (персональных данных), твердыми копиями и их утилизации**

3.1. Все находящиеся на хранении и в обращении съемные носители с персональными данными в структурном подразделении подлежат учёту.

3.2. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.3. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники отдела, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей ПДн.

3.4. Сотрудники структурного подразделения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

**4. Использование носителей ПДн**

При использовании сотрудниками носителей ПДн необходимо:

4.1. Соблюдать требования настоящей Инструкции.

4.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

4.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции.

4.4. Бережно относится к носителям ПДн.

4.5.Обеспечивать физическую безопасность носителей информации всеми разумными способами.

4.6. Извещать администраторов ИС о фактах утраты (кражи) носителей ПДн.

**5. При использовании носителей ПДн Пользователям запрещается:**

5.1. Использование носителей ПДн в личных целях.

5.2. Передача носителей ПДн другим лицам (за исключением администраторов ИС).

5.3.Хранение съемных носителей с ПДн вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

5.4 Вынос съемных носителей с ПДн (персональными данными) из служебных помещений для работы с ними на дому и т. д.(если на это нет соответствующего разрешения Руководства).

**6. Организация контроля**

6.1.Любое взаимодействие (обработка, прием/передача информации), инициированное сотрудником Учреждения, между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.

6.2. Информация об использовании сотрудником структурного подразделения носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена руководству Учреждения.

6.3. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей ПДн инициализируется служебная проверка, проводимая комиссией, состав которой определяется Директором.

6.4. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Учреждения и действующему законодательству.

6.5. Информация, хранящаяся на носителях ПДн, подлежит обязательной проверке на отсутствие вредоносного ПО (проверка установленным в Учреждении антивирусным ПО).

6.6. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

6.7. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.8. В случае утраты или уничтожения съемных носителей персональных данных, либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

6.9. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

Уничтожение съемных носителей с ПДн осуществляется комиссией назначенной приказом. По результатам уничтожения носителей составляется акт по прилагаемой форме.

6.10.В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители ПДн изымаются.

**7. Ответственность**

7.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Учреждения.

**УТВЕРЖДАЮ**

Директор КГАУСО «ПЦСОН»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/В.А. Логачёв

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года

**АКТ**

**уничтожения съемных носителей персональных данных**

Комиссия, наделенная полномочиями приказом от \_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_ в составе:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должности, ФИО)

провела отбор съемных носителей конфиденциальной информации (персональных данных), не подлежащих дальнейшему хранению:

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Дата | Учетный номер съемного носителя | Примечание |
|  |  |  |  |
|  |  |  |  |

Всего съемных носителей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(цифрами и прописью).

На съемных носителях уничтожены ПДн путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(разрезания, демонтажа и т.п.)

Председатель комиссии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены комиссии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение № 13**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование структурного подразделения)

Начат «\_\_\_» \_\_\_\_\_\_\_\_\_ \_\_\_\_

Окончен «\_\_\_» \_\_\_\_\_\_\_\_\_ \_\_\_\_

На \_\_\_\_\_\_ листах

**ЖУРНАЛ**

**учета электронных носителей персональных данных**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Учетный номер | Дата постановки на учет | Вид  электронного носителя,  место его хранения (размещения) | Ответственный за использование и хранение | | |
| Ф.И.О. | подпись | дата |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Приложение № 14**

**УТВЕРЖДЕНО**

Приказом директора

КГАУСО «ПЦСОН»

№ 68 от 05.11.2014 г.

**ИНСТРУКЦИЯ**

**администратора безопасности информационной системы персональных данных**

**КГАУСО «ПЦСОН»**

**1. Общие положения**

1.1. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом Директора КГАУСО «ПЦСОН» (далее по тексту – Учреждение).

1.2. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения.

1.3. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

**2. Администратор обязан:**

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

1) программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);

2) аппаратных средств;

3) аппаратных и программных средств защиты.

2.3.Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персональных паролей Операторами ИСПДн.

2.9.Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности ПДн.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11.Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12.Обеспечивать строгое выполнение требований по обеспечению безопасности ПДн при организации обслуживания технических средств и отправке их в ремонт. (При проведении технического обслуживания и ремонта узлы и блоки с элементами накопления и хранения информации вынимаются и передаются на хранение в отдел ИТ.)

2.13. Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

2.14. Не допускать к работе на рабочих станциях и серверах Учреждения посторонних лиц.

2.15. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

2.18. При изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС.

**Приложение № 15**

**ПЕРЕЧЕНЬ**

**персональных данных, обрабатываемых в ИСПДн КГАУСО «ПЦСОН»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Наименование персональных данных** | **Способ обработки** | **Наименование ИСПДн, в которой обрабатываются ПДн** | |
| 1. **Персональные данные кандидатов на работу** | | | | |
|  | Ф.И.О. | Неавтоматизированный | Неавтоматизированная ИСПДн БиК | |
|  | Предыдущие Ф.И.О., причины их изменения | Неавтоматизированный | Неавтоматизированная ИСПДн БиК | |
|  | Паспортные данные: пол, серия, номер, кем и когда выдан | Неавтоматизированный | Неавтоматизированная ИСПДн БиК | |
|  | Адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона или сведения о других способах связи; реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; реквизиты страхового медицинского полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о трудовой деятельности; сведения о воинском учете и реквизиты документов воинского учета; сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании); сведения об ученой степени; | Неавтоматизированный | Неавтоматизированная ИСПДн БиК | |
| 1. **Персональные данные работников** | | | | |
| 2.1. | Ф.И.О. | Смешанный | | ИСПДн БиК, неавтоматизированная ИСПДн «Кадровое делопроизводство |
| 2.2. | Предыдущие Ф.И.О., причина их изменения | Неавтоматизированный | | Неавтоматизированная ИСПДн «Кадровое делопроизводство» |
| 2.3. | Паспортные данные: пол, серия, номер, кем и когда выдан | Смешанный | | ИСПДн «БиК», неавтоматизированная ИСПДн «Кадровое делопроизводство» |
| 2.4. | Информация о гражданстве (в том числе предыдущие гражданства, иные гражданства); вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; адрес места жительства (адрес регистрации, фактического проживания); номер контактного телефона или сведения о других способах связи; реквизиты страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика; реквизиты страхового медицинского полиса обязательного медицинского страхования; реквизиты свидетельства государственной регистрации актов гражданского состояния; семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших); сведения о трудовой деятельности; сведения о воинском учете и реквизиты документов воинского учета; сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании); сведения об ученой степени; информация о владении иностранными языками, степень владения; фотография; информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору; информация о наличии или отсутствии судимости; информация об оформленных допусках к государственной тайне; государственные награды, иные награды и знаки отличия; сведения о профессиональной переподготовке и (или) повышении квалификации; информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания; сведения о доходах, об имуществе и обязательствах имущественного характера; номер расчетного счета; номер банковской карты; | Неавтоматизированный | | ИСПДн «БиК», неавтоматизированная ИСПДн «Кадровое делопроизводство» |
| 1. **Персональные данные клиентов (при наличии действующих договоров)** | | | | |
| 3.1. | Фамилия, имя, отчество; число, месяц, год рождения; пол; адрес по прописке; номер и дата свидетельства о рождении; фамилия, имя, отчество законного представителя; контактные телефоны законного представителя; серия, номер паспорта законного представителя; дата выдачи и орган, выдавший паспорт законного представителя; | автоматизированный | ИСПДН УСЛУГИ | |