|  |  |  |
| --- | --- | --- |
| Санкт-Петербургское государственное |  | Приложение N 1 |
| бюджетное учреждение социального |  |  |
| обслуживания населения «Комплексный |  | УТВЕРЖДЕНО |
| центр социального обслуживания населения |  | приказом СПб ГБУСОН |
| Невского района Санкт-Петербурга» |  | «КЦСОН Невского района» |
| (СПб ГБУСОН «КЦСОН Невского района») |  | от 22.11.2018 № 183 |
|  |  |  |
| **ПОЛОЖЕНИЕ** |  |  |
| Санкт-Петербург |  |  |
| **об обработке и защите персональных данных** |  |  |
|  |  |  |

**1. Общие положения**

 1.1. Настоящее Положение об обработке и защите персональных данных (далее **-** Положение) Санкт**-**Петербургского государственного бюджетного учреждения социального обслуживания населения «Комплексный центр социального обслуживания населения Невского района Санкт**-**Петербурга» (СПб ГБУСОН «КЦСОН Невского района») разработано в соответствии Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 28.12.2013 №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Законом Санкт-Петербурга от 26.12.2014 №717-135 «О социальном обслуживании населения в Санкт-Петербурге» и иными нормативными правовыми актами.

 1.2. Цель разработки Положения - определение порядка сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения и защиты персональных данных в Санкт**-**Петербургском государственном бюджетном учреждении социального обслуживания населения «Комплексный центр социального обслуживания населения Невского района Санкт-Петербурга» (СПб ГБУСОН «КЦСОН Невского района») (далее – Учреждение) и установление ответственности должностных лиц Учреждения, непосредственно осуществляющих обработку персональных данных и (или) имеющих доступ к персональным данным Учреждения за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

 1.3. Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Учреждения.

1.4. Формы документов, необходимых для организации обработки и защиты персональных данных, разработанные в Учреждении, являются неотъемлемой частью настоящего Положения. Работники Учреждения обязаны оформлять документы по утвержденным формам.

1.5. Настоящее Положение является обязательным для исполнения всеми работниками Учреждения, непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным субъектов персональных данных. Все работники Учреждения, непосредственно осуществляющие обработку персональных данных и (или) имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

При приеме на работу работник должен быть ознакомлен под роспись с настоящим Положением до подписания трудового договора.

1.6. В настоящем Положении используются следующие понятия, термины и сокращения:

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

 **информация** - сведения (сообщения, данные) независимо от формы их представления;

 **доступ к информации** - возможность получения информации и ее использования;

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

 оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

 **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

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

 **субъект персональных данных** - это физическое лицо, персональные данные которого обрабатываются Учреждением (работники, бывшие работники, близкие родственники работника, соискатели на замещение вакантных должностей, лица, проходящие различного рода практику (стажировку) в Учреждении, граждане, состоящие с Учреждением в гражданско-правовых отношениях, граждане, персональные данные которых необходимы для оказания социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения);

 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;

 **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

 **обработка персональных данных без использования средств автоматизации (неавтоматизированная)** – обработка (использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных), содержащихся в информационной системе персональных данных либо извлеченных из такой системы персональных данных, осуществляемая при непосредственном участии человека;

 **использование персональных данных** - действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

 распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

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

 **уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

 **конфиденциальность персональных данных –** обязанность лица, получившего доступ к персональным данным, не раскрывать третьим лицам и не распространять их без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

 1.7. Обозначения и сокращения:

**ПЭВМ** - персональные электронные вычислительные машины

**АРМ**  - автоматизированное рабочее место

 **ИСПДн** - информационная система персональных данных

**МЭ** - межсетевой экран

**НСД**  - несанкционированный доступ

**ПДн** - персональные данные

**ПО** - программное обеспечение

**СВТ** - средства вычислительной техники

**СЗИ**  - средства защиты информации

# **2. Обработка персональных данных**

#  2.1. Обработка персональных данных в Учреждении осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных.

 2.2. Обработка персональных данных в Учреждении осуществляется в целях обеспечения кадровой и бухгалтерской работы, обучения и должностного роста работников, учета результатов исполнения работниками Учреждения должностных обязанностей, обеспечения работникам Учреждения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, оформления договорных отношений в соответствии с законодательством Российской Федерации, предоставления социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения.

 **2.3. Общие требования при обработке персональных данных.**

 2.3.1. Работники Учреждения при обработке персональных данных обязаны соблюдать следующие общие требования:

 при определении объема и содержания обрабатываемых персональных данных, работники Учреждения должны руководствоваться Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 28.12.2013 №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации» и иными федеральными законами;

 обработка специальных категорий персональных данных, касающихся состояния здоровья, допускается на основании ст.10 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

 Учреждение не обрабатывает биометрические персональные данные. Сканирование фотографий в документах, идентифицирующих личность субъектов персональных данных (например, в паспортах), в Учреждении не осуществляется. Передаваемые в рамках трудового законодательства, а также в рамках договоров, копии паспортов субъектов персональных данных, не используются в целях идентификации личности. В случае, если обработка биометрических персональных данных субъекта персональных данных Учреждения необходима по действующему законодательству или для осуществления деятельности Учреждения, то такая обработка осуществляется с письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных;

 в целях информационного обеспечения могут создаваться общедоступные источники персональных данных. Сведения о работнике Учреждения должны быть в любое время исключены из общедоступных источников персональных данных по запросу работника либо по решению суда или иных уполномоченных государственных органов;

 обработка персональных данных в Учреждении осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом директора Учреждения, при этом указанные в приказе работники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей;

 работники Учреждения, осуществляющие обработку персональных данных, должны быть проинформированы о факте такой обработки, об особенностях и правилах такой обработки, установленных нормативно-правовыми актами и внутренними документами Учреждения, об ответственности за разглашение конфиденциальной информации, к которой относится, в том числе информация, содержащая персональные данные;

 в рамках информирования работников Учреждения о факте обработки персональных данных, Учреждение обязывает работников самостоятельно изучать и соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с персональными данными, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой персональных данных субъектов персональных данных Учреждения.

 2.4. Субъекты персональных данных и состав персональных данных.

 2.4.1. В целях, указанных в пункте 2.2. настоящего Положения, в Учреждении обрабатываются персональные данные следующих субъектов персональных данных:

 а) работников, состоящих или состоявших в трудовых отношениях с Учреждением, соискателей на замещение вакантных должностей, лиц, проходящих различного рода практику (стажировку) в Учреждении, близких родственников работника в объеме, предусмотренном унифицированной формой №Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05.01.2004 №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление социальных выплат);

 б) граждан, состоящих с Учреждением в гражданско-правовых отношениях;

 в) граждан, персональные данные которых необходимы для оказания социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения.

 2.4.2. К персональным данным лиц, указанным в подпункте «а» п.2.4.1. настоящего Положения, относятся следующие сведения:

 фамилия, имя, отчество;

 информация о смене фамилии, имени, отчества;

 дата рождения; место рождения;

 пол;

 информация о гражданстве;

 документ, удостоверяющий личность (вид, серия, номер документа, наименование органа, выдавшего его, дата выдачи);

 адрес места жительства (адрес регистрации, фактического проживания); дата регистрации по месту жительства;

 почтовый адрес;

 номер контактного телефона;

 семейное положение, состав семьи и сведения о близких родственниках;

 реквизиты идентификационного номера налогоплательщика (ИНН);

 реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);

 сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка, степень знания);

 сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору;

 характер, вид работы;

 табельный номер;

 подразделение;

 профессия, специальность, категория;

 сведения о трудовой деятельности, общем трудовом стаже;

 сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификации, специальность по документу об образовании);

 сведения об ученой степени;

 отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах;

 сведения о замещаемой должности;

 сведения о приеме на работу и переводах на другие должности;

 сведения о прохождении аттестации;

 сведения в документах, связанные с оформлением доступа к работе с конфиденциальной информацией, если исполнение обязанностей по замещаемой должности связано с использованием такой информации;

 сведения о профессиональной переподготовке и (или) повышении квалификации;

 информация о награждении (поощрении), почетных званиях;

 материалы служебных проверок, расследований;

 сведения о взысканиях;

 сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

 сведения о командировках;

 сведения о состоянии здоровья и его соответствием выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности;

сведения о социальных льготах, на которые сотрудник имеет право в соответствии с законодательством;

 сведения о доходах;

 сведения о налогах;

 сведения о страховых взносах;

 данные о нетрудоспособности;

 фотография;

 номер расчетного счета;

 номер банковской карты.

2.4.3. К документам (в бумажном и (или) электронном виде), содержащим персональные данные работников Учреждения, относятся:

 документы, необходимые для расчета и начисления заработной платы и иных выплат сотрудникам (табель учета использования рабочего времени, карточка-справка, заявления, расчетные ведомости по начислению заработной платы работникам, документы о выплате пособий, оплате листков нетрудоспособности, командировочное удостоверение);

 документы, необходимые для ведения расчетно-кассовой деятельности (приходно-кассовый ордер, расходно-кассовый ордер, квитанции);

 документы, необходимые для расчета с Федеральной налоговой службой и различными фондами (регистр налогового учета, листок нетрудоспособности, сведения о сумме выплат и иных вознаграждений, о начисленных и уплаченных страховых взносах на обязательное пенсионное страхование и страховом стаже застрахованного лица);

 справки (по форме 2-НДФЛ, о заработной плате, с места работы);

 договоры о материальной ответственности материально-ответственного лица;

заявление о приеме на работу, протоколы по определению стажа работы, личные карточки работников (форма №Т-2);

приказы по личному составу;

трудовые договоры (в том числе срочные), дополнительные соглашения к ним;

графики предоставления отпусков;

заявления работников о предоставлении отпусков, отгулов;

документы по учету командировок (приказы, командировочные удостоверения);

трудовые книжки;

справки;

документы о представлении к награждению государственными, ведомственными наградами, присвоении званий, присуждении премий (представление, наградные листы, ходатайства, характеристики, автобиографии, выписки из решений, постановлений, протоколов);

списки работников;

документы по воинскому учету граждан;

журналы учета, регистрации по вопросам кадрового учета.

 2.4.4. В целях информационного обеспечения Учреждением могут создаваться общедоступные источники персональных данных (в том числе справочники, информационные стенды для получателей социальных услуг). В общедоступные источники персональных данных с письменного согласия работника Учреждения или в силу прямого указания закона, могут включаться следующие сведения, к которым обеспечен свободный доступ:

 фамилия, имя, отчество;

 дата рождения;

 должность;

 сведения об образовании и квалификации;

 сведения о наградах;

 фотография.

 Форма согласия на общедоступность персональных данных приведена в Приложении N 1 к настоящему Положению.

 2.4.5. К персональным данным граждан, состоящих с Учреждением в гражданско-правовых отношениях, относятся следующие сведения:

 фамилия, имя, отчество;

 адрес места жительства; дата регистрации по месту жительства;

 документ, удостоверяющий личность (вид, серия, номер документа, наименование органа, выдавшего его, дата выдачи);

 сведения об образовании;

 реквизиты идентификационного номера налогоплательщика (ИНН);

 номер расчетного счета;

 номер банковской карты;

 сумма к зачислению.

2.4.6. К документам (в бумажном и (или) электронном виде), содержащим персональные данные граждан, состоящих с Учреждением в гражданско-правовых отношениях, относятся:

 договоры гражданско-правового характера.

2.4.7. К персональным данным граждан, персональные данные которых необходимы для оказания социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения, относятся следующие сведения:

 фамилия, имя, отчество;

 дата рождения;

 пол;

 место жительства и адрес регистрации по месту жительства;

 почтовый адрес;

 контактные телефоны;

 данные документа, удостоверяющего личность (вид, серия, номер документа, наименование органа, выдавшего его, дата выдачи);

 реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);

 семейное положение;

 сведения о состоянии здоровья;

 сведения о наличии (отсутствии) судимости;

 сведения о пенсии;

 сведения о материально-бытовых условиях;

 сведения из документов, подтверждающих право на получение мер социальной поддержки;

 сведения об инвалидности;

 сведения о составе семьи;

 сведения о доходах;

 сведения, необходимые для оказания социальных услуг.

2.4.8. К документам (в бумажном и (или) электронном виде), содержащим персональные данные граждан, персональные данные которых необходимы для оказания социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения, относятся:

 личные дела получателей социальной помощи;

 журналы учета/ регистрации по вопросам основной деятельности.

 2.4.9. Обработка персональных данных работников, состоящих или состоявших в трудовых отношениях с Учреждением, соискателей на замещение вакантных должностей, лиц, проходящих различного рода практику (стажировку) в Учреждении, близких родственников работника, граждан, состоящих с Учреждением в гражданско-правовых отношениях, осуществляется отделом кадров и бухгалтерией Учреждения и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. При сборе персональных данных работник отдела кадров, осуществляющий сбор (получение) персональных данных непосредственно от соискателей на замещение вакантных должностей, лиц, проходящих различного рода практику (стажировку) в Учреждении, граждан, состоящих с Учреждением в гражданско-правовых отношениях, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

 2.4.10. Обработка персональных данных граждан, персональные данные которых необходимы для оказания социальных услуг, выполнения возложенных на Учреждение функций, полномочий и обязанностей в сфере социального обслуживания населения, осуществляется уполномоченными должностными лицами структурных подразделений Учреждения, осуществляющими оказание социальных услуг и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. При сборе персональных данных уполномоченное должностное лицо структурного подразделения Учреждения, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением социальной услуги, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

 2.5. Условия обработки персональных данных.

 2.5.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных, и дает согласие на их обработку Учреждением. В случае, если Учреждение получает персональные данные субъектов персональных данных от третьих лиц, получающих персональные данные у субъектов, в соответствие с ч.4 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Учреждение не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

2.5.2. Если персональные данные получены не от субъекта персональных данных и их обработка не поручена Учреждению, Учреждение до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию: наименование, либо фамилия, имя, отчество и адрес оператора или его представителя; цель обработки персональных данных и ее правовое основание; предполагаемые пользователи персональных данных; установленные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» права субъекта персональных данных; источник получения персональных данных. Форма уведомления о получении персональных данных от третьих лиц представлена в Приложении N 2 к настоящему Положению.

2.5.3. Учреждение освобождается от обязанности предоставить субъекту персональных данных указанные сведения в случаях, если:

 субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

 персональные данные получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

 персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

 Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

 предоставление субъекту персональных данных сведений, нарушает права и законные интересы третьих лиц.

2.5.4. Обработка персональных данных субъектов персональных данных осуществляется с их согласия на обработку их персональных данных, а также в иных случаях, предусмотренных ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных». Согласие на обработку персональных данных может быть дано субъектом персональных данных или его законным 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 проверяются Учреждением. Форма согласия может быть в письменной или иной форме, предусмотренной действующим законодательством. При недееспособности субъекта персональных данных письменное согласие на обработку его данных дает его законный представитель. Учреждение обязано иметь доказательство получения согласия субъекта персональных данных на обработку его персональных данных (в том случае, если такое согласие является необходимым).

2.5.5. В случаях, предусмотренных ч.4 ст.9 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

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

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);

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

цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта;

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

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

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

подпись субъекта персональных данных.

Форма согласия на обработку персональных данных (в соответствии с требованиями ФЗ №152 «О персональных данных» и Трудового кодекса РФ) для работников Учреждения приведена в Приложении N 3 к настоящему Положению.

Форма согласия на обработку персональных данных (сторонних субъектов персональных данных) для получателей социальных услуг приведена в Приложении N 4 к настоящему Положению.

2.5.6. В случае, если для предоставления социальной услуги необходима обработка персональных данных лица, не являющегося заявителем, и если в соответствии с федеральным законом обработка таких персональных данных может осуществляться с согласия указанного лица, при обращении за получением социальной услуги заявитель дополнительно представляет документы, подтверждающие получение согласия указанного лица или его законного представителя на обработку персональных данных указанного лица. При обращении за получением социальной услуги заявителю необходимо представить документы, подтверждающие получение согласия физического лица, не являющегося заявителем, или его законного представителя на обработку персональных данных. Документы, подтверждающие получение согласия, могут быть представлены, в том числе в форме электронного документа. Согласие не требуется с лиц, признанных безвестно отсутствующими, и разыскиваемых лиц, место нахождения которых не установлено уполномоченным федеральным органом исполнительной власти. Форма согласия лица, не являющегося заявителем на получение услуги, но чьи данные необходимы для получения такой услуги на обработку персональных данных представлена в Приложении N 5 к настоящему Положению.

2.5.7. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Согласие субъекта персональных данных (работника) на поручение обработки персональных данных третьим лицам представлено в Приложении N 6 к настоящему Положению.

2.5.8. Передача персональных данных субъектов персональных данных Учреждения третьим лицам (включая надзорные, правоохранительные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта персональных данных. В случае, если обязанность либо возможность предоставления имеющихся в распоряжении Учреждения персональных данных иным лицам (включая органы государственной и муниципальной власти) установлена законодательством, Учреждение обязано предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах. Если обязанность предоставления персональных данных фиксируется соответствующим запросом (ходатайством) уполномоченного лица, запрос подлежит обязательной проверке в целях контроля над обоснованностью предоставления запроса. При обоснованности подобного запроса Учреждение формирует ответ на запрос. При необоснованности запроса Учреждение направляет отправителю запроса письменное уведомление об отказе в предоставлении персональных данных. При передаче персональных данных третьим лицам, Учреждение обязано уведомлять лиц, получивших персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать их конфиденциальность и безопасность. Данное требование не распространяется на обмен персональными данными в порядке, установленном законодательством.

2.5.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных при условии, что подобная процедура не нарушает требований законодательства Российской Федерации. Форма отзыва согласия на обработку персональных данных представлена в Приложении N 7 к настоящему Положению, заявление о прекращении обработки персональных данных представлена в Приложении N 8. В случае отзыва субъектом персональных данных Учреждения согласия на обработку персональных данных, Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в п.п.2-11 ч.1 ст.6, ч.2 ст.10 и ч.2 ст.11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

2.5.10. В соответствии с п.п.2-11 ч.1 ст.6, ч.4 ст.6, ч.2 ст.10 и ч.2 ст.11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» обработка персональных данных может осуществляться без согласия субъекта персональных данных.

 2.5.11. Трансграничная передача персональных данных в Учреждении не осуществляется.

 2.6. Порядок обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации.

 2.6.1. Обработка персональных данных в Учреждении может проводиться с использованием средств автоматизации (информационных систем) и без таковых. Конкретный способ обработки персональных данных определяется на основании процедур использования данных, определенных внутренними документами Учреждения.

 Обработка персональных данных в Учреждении осуществляется на автоматизированных рабочих местах Учреждения в автоматизированной информационной системе «Электронный социальный регистр населения Санкт-Петербурга» (АИС ЭСРН), в автоматизированной информационной системе «1С: Предприятие (Зарплата + кадры)».

 2.6.2. Уровень защищенности персональных данных при их обработке в информационной системе персональных данных, требования по обеспечению безопасности обрабатываемых персональных данных субъектов персональных данных Учреждения, описаны в отдельных нормативных актах Учреждения.

2.6.3. Контроль за соответствием обработки персональных данных заявленным целям, возлагается на ответственного за организацию обработки персональных данных в Учреждении и на руководителей подразделений, в которых осуществляется обработка персональных данных, приказом.

2.6.4. Исключительно автоматизированная обработка персональных данных в Учреждении не осуществляется. Во всех процессах обработки персональных данных субъектов персональных данных с использованием средств автоматизации принимают участие уполномоченные работники Учреждения.

2.6.5. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

2.6.6. 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);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

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 и лиц, которым оператором поручена обработка персональных данных, 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;

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;

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;

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

2.6.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных, осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных, уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.6.9. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в сейфах или в надежно запираемых металлических шкафах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

2.6.10. 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).

 2.7. Доступ к персональным данным.

2.7.1. Перечень работников, осуществляющих обработку персональных данных, как в бумажном, так и в электронном виде и (или) имеющих доступ к персональным данным, утверждается приказом директора Учреждения. При этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения непосредственных должностных обязанностей.

2.7.2. В случае, если Учреждению оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований), и, в силу данных договоров, они должны иметь доступ к персональным данным субъектов персональных данных Учреждения, то соответствующие данные предоставляются Учреждением только после подписания с лицами, осуществляющими обработку персональных данных по поручению Учреждения, соответствующего соглашения, в котором должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

* + 1. Процедура оформления доступа к персональным данным включает в себя:

 ознакомление работников с Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 28.12.2013 №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Законом Санкт-Петербурга от 26.12.2014 №717-135 «О социальном обслуживании населения в Санкт-Петербурге», с настоящим Положением, инструкцией пользователя информационных систем персональных данных и другими нормативными актами, регулирующими обработку и защиту персональных данных в Учреждении, под роспись;

 подписание работником Учреждения обязательства о соблюдении конфиденциальности персональных данных. Форма обязательства о соблюдении конфиденциальности персональных данных представлена в Приложении N 9 к настоящему Положению.

 2.8. Обеспечение конфиденциальности персональных данных.

 2.8.1. Персональные данные относятся к категории конфиденциальной информации.

2.8.2. Учреждение вправе поручить обработку персональных данных другим юридическим или физическим лицам на основании договора (далее – поручение Учреждения) с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных». Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных». В поручении Учреждения должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

2.8.3. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

2.8.4. Необходимость доступа работников Учреждения к персональным данным субъектов персональных данных, обрабатываемым в Учреждении, должна быть документально определена в соответствующих должностных инструкциях.

2.8.5. В Учреждении документально определен перечень лиц, осуществляющих обработку персональных данных. Лица, осуществляющие такую обработку, проинформированы о факте обработки ими персональных данных, об особенностях и правилах осуществления такой обработки, а также об ответственности за нарушение действующего законодательства в области персональных данных. Лица, осуществляющие обработку персональных данных, ознакомлены под роспись с настоящим Положением и подписали обязательство о соблюдении конфиденциальности персональных данных и соблюдении правил обработки персональных данных.

2.8.6. В Учреждении документально определен перечень помещений, в которых ведется обработка персональных данных, порядок доступа работников в вышеуказанные помещения.

2.8.7. Передача персональных данных между структурными подразделениями Учреждения осуществляется только между работниками, включенными в перечень лиц, имеющих доступ к персональным данным.

2.8.8. Учреждения и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

* 1. Права и обязанности сторон при обработке персональных данных.
		1. Субъекты персональных данных обязаны предоставлять Учреждению только достоверные, документированные персональные данные и своевременно сообщать об изменении своих персональных данных.
		2. Каждый субъект персональных данных имеет право:

 на получение полной информации о своих персональных данных и на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных ч.8 ст.14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

 на получение информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки, правовые основания и цель обработки; способы обработки, наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»; сроки обработки персональных данных, в том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами. Сведения, указанные выше, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись субъекта персональных данных или его уполномоченного представителя;

 обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений, указанных выше, и ознакомления с такими персональными данными не ранее чем через 30 (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, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса;

 требовать от работников Учреждения уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

 заявить о своем несогласии при отказе работников Учреждения исключить или исправить персональные данные (в письменной форме с соответствующим обоснованием такого несогласия).

* + 1. Учреждение не вправе принуждать субъектов персональных данных к предоставлению персональных данных, однако вправе требовать этого, если подобные обязательства прямо вытекают из договорных отношений с субъектами персональных данных или требований нормативных и законодательных актов. Если сбор персональных данных осуществляется во исполнение требований законодательства, работники Учреждения, осуществляющие сбор персональных данных обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить персональные данные. Форма запроса о необходимости получения информации, составляющей персональные данные представлена в Приложении N 10 к настоящему Положению.
		2. Учреждение обязано безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к этому субъекту, а также внести в них необходимые изменения при предоставлении субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными. О внесенных изменениях и предпринятых мерах Учреждение обязано уведомить субъекта или его представителя и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы. Все обращения субъектов персональных данных по вопросам, касающимся обработки персональных данных, фиксируются в Журнале учета обращений субъектов персональных данных. Форма Журнала представлена в Приложении N 11 к настоящему Положению.
		3. Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) календарных дней с даты получения такого запроса.
	1. Передача персональных данных.
		1. Передача персональных данных субъектов персональных данных Учреждения третьим лицам (включая надзорные, правоохранительные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта персональных данных.
		2. При передаче персональных данных субъекта персональных данных работники Учреждения обязаны соблюдать следующие требования:

 не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Гражданским Кодексом Российской Федерации или иными федеральными законами;

 предупреждать лица, получающие персональные данные субъектов, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;

 не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

 передавать персональные данные субъекта представителям субъектов в порядке, установленном Гражданским Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;

 не отвечать на вопросы, связанные с передачей персональных данных субъекта по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими работниками своих непосредственных должностных обязанностей, адресатам, в чью компетенцию входит получение такой информации*.*

* + 1. В целях обеспечения контроля правомерности использования переданных по запросам персональных данных лицами, их получившими, сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также состав переданной информации фиксируются в Журнале учета передачи персональных данных. Форма Журнала учета передачи персональных данных представлена в Приложении N 12 к настоящему Положению.
	1. Хранение персональных данных.
		1. 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. Хранение персональных данных в Учреждении может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.
		2. Все хранимые или используемые средства защиты информации (далее - СЗИ), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним пользователям СЗИ, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала приведена в Приложении  N 13 к настоящему Положению.
		3. Все хранимые или используемые криптосредства (средства криптографической защиты информации), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету и выдаются под расписку в Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственным пользователем криптосредств пользователям криптосредств, несущим персональную ответственность за их сохранность. Форма соответствующего Журнала приведена в Приложении N 14 к настоящему Положению. Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств Лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы. Форма Лицевого счета пользователя криптосредств приведена в Приложении  N 15 к настоящему Положению.
		4. Хранение персональных данных субъектов осуществляется в порядке, исключающем их утрату или их неправомерное использование.
		5. Персональные данные субъектов, содержащиеся на бумажных носителях и отчуждаемых машинных носителях информации, должны храниться в недоступном для неуполномоченных лиц месте: в запираемых сейфах или запираемых несгораемых шкафах, установленных в помещениях, определенных приказом директора Учреждения. Все хранилища должны быть учтены, и соответствующая запись внесена в Журнал учета хранилищ (сейфов). Форма соответствующего Журнала приведена в Приложении  N 16  к настоящему Положению.

 2.11.6. Выдача ключей от сейфа производится руководителем структурного подразделения, в функции которого входит обработка определенных персональных данных (а на период его временного отсутствия - болезнь, отпуск и т.п. - лицом, исполняющим его обязанности), только работникам данного структурного подразделения. Сдача ключа осуществляется лично руководителю после закрытия сейфа или несгораемого металлического запираемого шкафа.

2.11.7. Персональные данные субъектов, содержащиеся на машинных носителях информации, хранятся на автоматизированных рабочих местах и серверах информационных систем персональных данных Учреждения.

2.11.8. Вынос носителей с резервными копиями баз данных, содержащих персональные данные, а также материальных носителей персональных данных из здания Учреждения запрещен, если иное не предусмотрено законодательством.

* 1. **Архивирование и обезличивание персональных данных.**
		1. Персональные данные, не используемые в операционной деятельности Учреждения и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов независимо от их форм собственности.
		2. Архивирование персональных данных производится в рамках, действующих в Учреждении систем документооборота и работы с архивными документами с соблюдением принципов, изложенных в настоящем Положении. Обязательным условием архивирования персональных данных является обеспечение их конфиденциальности и безопасности.
		3. Подразделения Учреждения, хранящие архивные персональные данные на бумажных носителях, обязаны обеспечить ограничение доступа к указанным данным только тех работников, деятельность которых непосредственно связана с обработкой хранимого типа архивных персональных данных. Доступ к архивным персональным данным, хранение которых осуществляется на электронных носителях, должен быть ограничен исходя из требований информационной безопасности, указанных в данном Положении и отдельных локальных нормативных актах Учреждения.
		4. С целью уменьшения объема персональных данных, подлежащих защите в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», подзаконных актов и методических указаний, а также в целях снижения нагрузки и обременений на Учреждение, приводящих к дополнительным затратам без повышения уровня защищенности персональных данных и прав субъектов персональных данных Учреждения, может быть произведено обезличивание персональных данных субъектов персональных данных Учреждения. Также обезличивание производится в целях предоставления статистической отчетности, агрегированной информации о деятельности Учреждения, а также в иных целях, предусмотренных действующим законодательством, например, по достижении целей их обработки или в случае утраты необходимости в достижении этих целей в соответствии со ст.5 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».
		5. Обезличенные персональные данные должны представлять собой информацию на бумажном или магнитном носителе, принадлежность которой к конкретному физическому лицу невозможно определить без использования дополнительной информации в силу произведенных при обработке персональных данных действий.
		6. Решение о необходимости и способе обезличивания персональных данных принимает ответственный за организацию обработки персональных данных в Учреждении.
	2. Прекращение обработки и уничтожение персональных данных.
		1. Уничтожение персональных данных субъектов персональных данных производится Учреждением:

 при выявлении неустранимых неправомерных действий с персональными данными;

 по достижении целей обработки персональных данных (при условии невозможности обезличивания персональных данных);

 при получении от субъекта персональных данных отзыва согласия на обработку персональных данных (при условии, что такой отзыв не противоречит обязанностям Учреждения продолжать обработку персональных данных в соответствии с действующим законодательством);

 по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных – если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

2.13.2. Уничтожению подлежат все требуемые к уничтожению персональные данные, зафиксированные на материальных носителях или хранящиеся в информационной системе. Уничтожение персональных данных в информационной системе производится должностным лицом, использовавшим указанные данные. Ответственный за организацию обработки персональных данных контролирует полноту уничтожения указанных данных в информационной системе Учреждения.

2.13.3. Если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения, то Учреждение обязано обеспечить их уничтожение в соответствии с данным Положением.

 2.13.4. Решение об уничтожении персональных данных принимается руководителем подразделения, ответственного за обработку соответствующих персональных данных, признанных необходимыми к уничтожению. Решение об уничтожении должно быть принято в срок, не превышающий 3 (трех) рабочих дней с даты появления оснований к уничтожению персональных данных. После принятия решения об уничтожении, руководитель подразделения, ответственного за обработку персональных данных, обязан уведомить об этом ответственного за организацию обработки персональных данных в Учреждении, который назначает комиссию по уничтожению персональных данных.

 2.13.5. Уничтожение персональных данных производится руководителем подразделения (для данных, хранящихся в электронной форме) либо комиссией по уничтожению персональных данных (для документов на материальных носителях) в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неустранимых неправомерных действий с персональными данными, не превышающий 30 (тридцати) календарных дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо, если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами, в срок, не превышающий 30 (тридцати) календарных дней с даты поступления от субъекта персональных данных отзыва согласия на обработку его персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо, если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного выше, Учреждение осуществляет уничтожение или обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами. Форма Акта на списание и уничтожение машинных (бумажных) носителей информации представлена в Приложении  N 17 к настоящему Положению.

2.13.6. В случае, если согласно имеющейся у Учреждения информации, персональные данные субъектов персональных данных были направлены третьим лицам, руководитель подразделения, ответственного за обработку соответствующих персональных данных, обязан потребовать у указанных третьих лиц в письменной форме уничтожения персональных данных с изложением оснований для подобного уничтожения.

2.13.7. При необходимости уничтожения персональных данных, являющихся частью материального носителя, содержащего персональные данные, не подлежащие уничтожению, комиссией по уничтожению персональных данных осуществляется вымарывание либо иное физическое удаление данных с условием сохранения данных, не подлежащих уничтожению. Скорректированные подобным образом документы подлежат возврату в соответствующее подразделение.

 2.13.8. После уничтожения данных, председатель комиссии по уничтожению персональных данных обязан уведомить о данной операции подразделение, передавшее информацию на уничтожение.

2.13.9. При получении информации об уничтожении либо после самостоятельного уничтожения, подразделение, осуществлявшее обработку персональных данных, обязано уведомить о факте уничтожения субъекта персональных данных, в случае, если уничтожение произведено по запросу уполномоченного органа по защите персональной информации, указанный орган. Уведомление должно содержать перечень мер, предпринятых Учреждением по результатам обнаружения случаев неправомерной обработки персональных данных. Форма уведомления об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке персональных данных, представлена Приложении  N 18 к настоящему Положению.

 2.13.10. Ответственный за организацию обработки персональных данных в Учреждении в рамках проверок по направлениям деятельности контролирует своевременность и полноту уничтожения персональных данных руководителями подразделений.

**3. Защита персональных данных**

 3.1. Учреждение при обработке персональных данных 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.

 3.2. Защита персональных данных представляет собой технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Учреждения.

3.3. Для осуществления мер по защите персональных данных субъектов персональных данных в Учреждении назначаются ответственные.

3.3.1. Ответственность за обеспечение безопасности персональных данных (сохранности персональных данных и исключение несанкционированного к ним доступа) возлагается на ответственного за организацию обработки персональных данных в Учреждении.

3.3.2. Ответственность за обеспечение безопасности персональных данных в информационной системе персональных данных возлагается на администратора информационной безопасности информационной системы персональных данных.

3.3.3. Обеспечение безопасности персональных данных субъектов персональных данных, обрабатываемых в Учреждении без использования средств автоматизации, осуществляет ответственный за организацию обработки персональных данных без использования средств автоматизации.

3.4. Обеспечение безопасности персональных данных достигается, в частности:

 определением угроз безопасности персональных данных при их обработке в информационной системе персональных данных;

 применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных, необходимых для выполнения требований к защите персональных данных;

 применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

 учетом машинных носителей персональных данных;

 обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

 восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

 установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

 контролем за принимаемыми мерами по обеспечению безопасности персональных данных.

3.5. Основными организационными мерами по защите персональных данных в Учреждении являются:

 разработка комплекта организационно-распорядительных документов Учреждения, регламентирующих процессы обработки персональных данных;

 определение и закрепление перечня сведений конфиденциального характера;

 назначение ответственных за организацию обработки персональных данных;

 ограничение доступа к конфиденциальной информации;

 определение состава работников, функциональные обязанности которых требуют обработки персональных данных;

 обеспечение ознакомления работников с требованиями федеральных законов, локальных нормативных актов Учреждения по обработке и защите информации;

 обеспечение наличия необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

 организация процесса уничтожения информации;

 организация разъяснительной работы с работниками Учреждения по предупреждению утраты и утечки сведений при работе с конфиденциальными документами, содержащими персональные данные;

 заключение с работниками, получившими доступ к персональным данным, обязательства о неразглашении конфиденциальной информации;

 осуществление внутреннего контроля соответствия обработки персональных данных требованиям действующего законодательства в области обработки и защиты персональных данных.

3.6. В качестве технических мер защиты персональных данных в Учреждении должны применяться:

 антивирусная защита;

 межсетевые экраны;

 специализированные средства защиты информации от несанкционированного доступа.

3.7. После установки (обновления) программного обеспечения ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных должен произвести требуемые настройки средств управления доступом к компонентам персональных электронных вычислительных машин (далее – ПЭВМ) и проверить работоспособность программного обеспечения и правильность его настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ. Формат записей Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ приведен в Приложении  N 19 к настоящему Положению.

3.8. Ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных должен проводить периодическое тестирование технических и программных средств защиты и вносить результаты в Журнал периодического тестирования средств защиты информации, форма которого представлена в Приложении  N 20  к настоящему Положению.

# **4. Взаимодействие с контрольно-надзорными органами**

4.1. При поступлении запроса от уполномоченного органа по защите прав субъектов персональных данных (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций), Учреждение обязано сообщить информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати рабочих дней с даты получения такого запроса.

4.2. В случае выявления неправомерной обработки персональных данных по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента получения указанного запроса на период проверки. В случае выявления неточных персональных данных по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

4.3. В случае подтверждения факта неточности персональных данных, Учреждение на основании сведений, представленных уполномоченным органом по защите прав субъектов персональных данных, обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

4.4. При проведении контрольно-надзорных мероприятий за выполнением требований к обеспечению безопасности персональных данных при их обработке в государственных информационных системах персональных данных, а также в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных (по решению Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных), осуществляемых федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), представители вышеуказанных контрольно-надзорных органов не имеют права на ознакомление с персональными данными, обрабатываемыми в информационных системах персональных данных.

4.5. При проведении контрольно-надзорных мероприятий за выполнением требований к обеспечению безопасности персональных данных, Учреждение обязано предоставить Журнал учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля.

4.6. При проведении контрольно-надзорных мероприятий в отношении Учреждения контрольно-надзорными органами, не осуществляющими контроль и надзор в сфере обработки персональных данных, представители вышеуказанных контрольно-надзорных органов имеют право на доступ к персональным данным только в сфере своей компетенции и в пределах своих полномочий в соответствии с законодательством Российской Федерации.

**5. Ответственность за разглашение конфиденциальной информации,**

**содержащей персональные данные**

5.1. Директор Учреждения, разрешающий доступ работника к персональным данным, несет персональную ответственность за данное разрешение.

5.2. Каждый работник Учреждения, получающий доступ к информации, содержащей персональные данные, несет персональную ответственность за сохранность конфиденциальности информации.

5.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, обрабатываемых Учреждением, несут ответственность в порядке, установленном федеральными законами и полную материальную ответственность в случае причинения их действиями ущерба в соответствии с п.7 ст.243 Трудового кодекса Российской Федерации.

5.4. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера, работодатель вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

5.5. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому субъекту персональных данных возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом Российской Федерации об административных правонарушениях.

5.6. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, являющуюся конфиденциальной, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

5.7. Нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, наказываются штрафом, либо исправительными работами, либо ограничением свободы, либо лишением свободы, либо лишением права занимать определенные должности или заниматься определенной деятельностью в соответствии с Уголовным кодексом Российской Федерации.

5.8. Неправомерность деятельности Учреждения по обработке персональных данных может быть установлена в судебном порядке.

**6. Заключительные положения**

6.1. Настоящее Положение вступает в силу с момента его утверждения и введения в действие приказом директора Учреждения и действует бессрочно, до замены его новым Положением.

6.2. Изменения к настоящему Положению утверждаются и вводятся приказом директора Учреждения.

Главный специалист по защите информации Ю.В. Базаитов

СОГЛАСОВАНО

Первичной профсоюзной организацией

СПб ГБУСОН «КЦСОН Невского района»

(протокол от 19.10.2018 №21)