

Государственное бюджетное дошкольное образовательное учреждение детский сад № 18
комбинированного вида Кронштадтского района Санкт-Петербурга

ПРИНЯТО
Общим собранием работников
Образовательного учреждения
Протокол № 1
от « 30 » 08 2022 г.



УТВЕРЖДАЮ
Заведующий
М.И. Кошкина
Приказ № 148-12/1
от « 31 » 08 2022 г.

**Положение
об обработке и защите персональных данных
работников ГБДОУ детский сад №18
Кронштадтского района Санкт – Петербурга**

Санкт-Петербург
2022 г.

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных работников (далее - Положение) ГБДОУ детский сад №18 Кронштадтского района Санкт-Петербурга (далее – ДОУ) разработано в соответствии со статьей 24 Конституции Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом №266-ФЗ от 14.07.2022 г., Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», Федеральным законом № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации».

1.2. Данное Положение разработано с целью обеспечения защиты прав и свобод работника при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну работников ДОУ от несанкционированного или случайного доступа, неправомерного их использования или утраты, а также защита персональных данных от уничтожения, блокирования, копирования и распространения.

1.3. Данное Положение устанавливает основные понятия и состав персональных данных работников в ДОУ, регулирует отношения, связанные с обработкой персональных данных работников и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю, устанавливает ответственности должностных лиц, имеющих доступ к обработке персональных данных.

2. Основные понятия и состав персональных работников

2.1. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. **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.

2.3. **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, передачу¹ (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.4. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

2.5. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.6. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.7. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.8. 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.

2.9. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.10. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.11. Общедоступные данные — сведения общего характера и иная информация, доступ к которой не ограничен.

2.12. При определении, объема и содержания персональных данных работника администрация ДОУ руководствуется Конституцией Российской Федерации, Трудовым Кодексом, Федеральными законами и настоящим Положением.

2.13. ДОУ обрабатывает общедоступные и иные категории персональных данных. Специальные категории персональных данных ДОУ обрабатывает только на основании и согласно требованиям Федерального Законодательства.

2.14. Биометрические персональные данные ДОУ не обрабатывает.

2.15. Под персональными данными работника, понимается информация, необходимая работодателю в связи с трудовыми отношениями. Статьей 65 Трудового кодекса Российской Федерации установлен перечень документов, предъявляемых при заключении трудового договора:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- изображение (фотография);
- адрес регистрации по месту жительства, адрес фактического проживания;
- контактные данные;
- семейное положение, наличие детей, родственные связи;
- сведения о трудовой деятельности, в том числе о наличии поощрений, наградений и (или) дисциплинарных взысканий;
- данные о регистрации брака;
- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка (при наличии);
- СНИЛС;
- документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- документ об образовании и (или) квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергавшиеся или подвергавшиеся уголовному преследованию);
- справку о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, подвергнутые административному наказанию за потребление наркотических средств или психотропных веществ);
- ИНН;
- сведения об инвалидности;

- сведения об удержании алиментов;
- сведения о доходе с предыдущего места работы;
- заключение по данным психологического исследования (если такое имеется);
- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);

2.16. В личном деле работника могут храниться следующие документы, содержащие персональные данные сотрудника:

- внутренняя опись документов дела
- анкета
- заявление о приеме на работу
- согласие на обработку персональных данных
- согласие на фото и видеосъемку сотрудника
- должностная инструкция
- характеристики и рекомендательные письма
- личные заявления работника
- трудовой договор и дополнительные соглашения к нему
- договор о полной материальной ответственности
- копии приказов по личному составу в отношении работника
- аттестационные листы
- уведомления об изменении условий трудового договора по инициативе работодателя
- копии приказов о переводе на другую работу, о поощрении, применении и снятии дисциплинарных взысканий
- копии объяснительных и докладных записок, заявления работника по различным вопросам
- материалы аттестаций
- документы, послужившие основанием к изданию приказа о прекращении трудового договора
- копия приказа о прекращении трудового договора

2.16. ДОУ обрабатывает персональные данные следующих категорий субъектов персональных данных- работники ДОУ, а также персональные данные физических (третьих) лиц – родственников работников (детей, мужа, жены), а именно: фамилия, имя, отчество, степень родства, дата рождения.

2.17. Размещение на официальном сайте фотографий работников или видео с работниками, сотрудники разрешают путем предоставления согласия на фото и видеосъемку.

2.18. Персональные данные работника ДОУ являются конфиденциальной информацией и не могут быть использованы сотрудниками ДОУ в личных целях.

3. Общие требования при обработке персональных данных работника

3.1. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители, при обработке персональных данных работника, обязаны соблюдать следующие общие требования:

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

3.1.2. При определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться 24 статьей Конституцией Российской Федерации, 65 статьей Трудового Кодекса и иными федеральными законами.

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

3.1.4. Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся к специальным категориям персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных;
- обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- 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;
- 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;
- обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется 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 без согласия в письменной форме субъектов персональных данных;
- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном

производстве, уголовно-исполнительным законодательством Российской Федерации;

- обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

3.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом или иными федеральными законами.

3.1.6. Работодатель вправе обрабатывать персональные данные уволенного работника, в случаях и в сроки, предусмотренные федеральным законодательством.

3.1.7. По истечении сроков, определенных законодательством Российской Федерации, личные дела работников и иные документы передаются на архивное хранение на срок 75 лет.

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

3.1.9. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым Кодексом и иными федеральными законами.

3.1.10. Работники и их представители должны быть ознакомлены под подпись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

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

3.1.12. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

3.2. Передача персональных данных работника в пределах ДООУ осуществляется в соответствии с локальными нормативными актами учреждения.

3.3. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.

3.4. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.5. Оператор при обработке персональных данных обязан 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.

3.6. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.7. Все меры конфиденциальности при сборе, обработке и передаче персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.8. Персональные данные работников обрабатываются путем смешанной и неавтоматизированной обработки персональных данных. Персональные данные работников вносятся в программу АИСУ «Параграф» и в систему «Контур.Экстерн».

3.9. Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу.

3.10. Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключило договор, а также при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц.

3.11. В случае получения резюме соискателя по каналам электронной почты, факсимильной связи работодателю необходимо дополнительно провести мероприятия, направленные на подтверждение факта направления, указанного резюме самим соискателем. Например, пригласить соискателя на личную встречу или посредством обратной связи через электронную почту.

3.12. При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо, его направившее, не представляется возможным, данное резюме подлежит уничтожению в день поступления.

3.13. В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней, за исключением случаев, предусмотренных законодательством Российской Федерации.

3.14. Получение согласия также является обязательным условием при направлении работодателем запросов в иные организации, в том числе, по прежним местам работы, для уточнения или получения дополнительной информации о соискателе.

4. Меры обеспечения безопасности и защиты персональных данных работников

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

4.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия,

экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

4.3. К основным мерам обеспечения безопасности персональных данных в ДОУ относятся:

4.3.1. Назначение ответственного за организацию обработки персональных данных. В обязанности ответственного входит организация обработки персональных данных, инструктаж работников, внутренний контроль за соблюдением в ДОУ требований законодательства к защите персональных данных.

4.3.2. Издание Политики в отношении обработки персональных данных в ДОУ и локальных актов по вопросам обработки персональных данных.

4.3.3. Ознакомление работников, осуществляющих обработку персональных данных, с положениями Законодательства о персональных данных, в том числе с требованиями к защите персональных данных, Политикой обработки персональных данных и локальными актами ДОУ по вопросам обработки персональных данных.

4.3.4. Регистрация и учет всех действий, совершаемых с персональными данными в системах, контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем.

4.3.5. Учета машинных носителей персональных данных.

4.3.6. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, оценка соотношения указанного вреда и принимаемых мер.

4.3.7. Внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям законодательства.

4.3.8. Публикация Политики ГБДОУ детский сад №18 в отношении обработки персональных данных и локальных актов по вопросам обработки персональных данных на официальном сайте ДОУ.

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

4.5. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

4.6. "Внутренняя защита":

4.6.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

4.6.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности

- которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
 - рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
 - знание работником требований нормативно - методических документов по защите информации и сохранении тайны;
 - наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
 - определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
 - организация порядка уничтожения информации;
 - своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
 - воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с персональными данными;
 - не допускается выдача личных дел сотрудников на рабочие места руководителей.

4.6.3. Защита персональных данных сотрудников на электронных носителях.

Все программы и папки, содержащие персональные данные сотрудника, должны быть защищены паролем.

4.7. "Внешняя защита":

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

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

4.7.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

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

4.7.4. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных.

4.7.5. По возможности персональные данные обезличиваются.

4.7.6. Кроме мер защиты персональных данных, установленных законодательством, работодателя, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

5. Сроки обработки, хранения и передачи персональных данных

5.1. ДОУ обрабатывает персональные данные в сроки:

- необходимые для достижения целей обработки персональных данных;
- определенные законодательством для обработки отдельных видов персональных данных;
- указанные в согласии субъекта персональных данных.

5.2. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения или продлевается на основании заключения экспертной комиссии ДОУ, если иное не определено законом.

5.3. 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.

5.4. Сроки хранения персональных данных в организации установлены в Приказе Росархива от 20.12.2019 N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения"

5.5. Персональные данные работников ДОУ хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях. В процессе хранения персональных данных работников должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

5.6. Доступ к персональным данным работников имеют:

- заведующий ДОУ;
- заместитель заведующего;
- документовед;
- делопроизводитель;
- старший воспитатель;
- сам работник, носитель данных;
- иные работники, определяемые приказом заведующего ДОУ, в пределах своей компетенции.

5.7. Помимо лиц, указанных в п.5.6. настоящего Положения, право доступа к персональным данным работников имеют лица, уполномоченные действующим законодательством.

5.8. Сотрудники, имеющие доступ к сведениям конфиденциального характера, подписывают приказ о неразглашении конфиденциальной информации работниками ГБДОУ детский сад №18.

5.9. Сотрудники, ответственные за обеспечение безопасности, сохранение, неразглашение и обработку персональных данных в ДОУ подписывают обязательство о неразглашении персональных данных. По мере смены должностных лиц обязательства обновляются.

5.10. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные работников лишь в целях, для которых они были предоставлены.

5.11. Ответственным за организацию и осуществление хранения персональных данных

работников организации является заместитель заведующего в соответствии с приказом заведующего ДОУ.

5.12. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных шкафах, под замком, в алфавитном порядке.

5.13. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

5.13.1. Не сообщать и не передавать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым Кодексом или иными федеральными законами.

5.13.2. Не сообщать и не передавать персональные данные работника в коммерческих целях без его письменного согласия.

5.13.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым Кодексом и иными федеральными законами.

5.13.4. Осуществлять передачу персональных данных работника в пределах ДОУ в соответствии с данным Положением, с которым работник должен быть ознакомлен под подпись.

5.13.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

5.13.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.13.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

6. Права работника в целях обеспечения защиты персональных данных, хранящихся у работодателя

6.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя. Работники имеют право:

6.1.1. Получать полную информацию о своих персональных данных и их обработке.

6.1.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, - к заместителю заведующего, ответственному за организацию и осуществление хранения

персональных данных работников.

6.1.3. На определение своих представителей для защиты своих персональных данных.

6.1.4. На доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору.

6.1.5. Требовать об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя заведующего ДОУ. При отказе руководителя организации исключить или исправить персональные данные работника, работник имеет право заявить в письменном виде руководителю организации, осуществляющей образовательную деятельность, о своем несогласии, с соответствующим обоснованием такого несогласия.

Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

6.1.6. Требовать об извещении организацией всех лиц, которым ранее были сообщены неверные или неполные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.7. Обжаловать в суде любые неправомерные действия или бездействия организации при обработке и защите его персональных данных.

7. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

7.1. В целях обеспечения достоверности персональных данных работники обязаны:

7.1.1. При приеме на работу в ДОУ представлять уполномоченным работникам достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

7.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 14 календарных дней с даты их изменений.

8. Порядок уничтожения персональных данных

8.1. Порядок уничтожения персональных данных при достижении целей их обработки или при иных законных основаниях осуществляется на основании «Порядка уничтожения и обезличивания персональных данных в ГБДОУ детский сад №18 Кронштадтского района Санкт-Петербурга» и предполагает следующий порядок действий:

8.2. В ДОУ приказом заведующего создается специальная комиссия для выявления неактуальных персональных данных и последующего их уничтожения и составления сопроводительного акта.

8.3. Комиссия выявляет список необходимых для ликвидации документов и проводит процедуру уничтожения.

8.4. Комиссия составляет акт с перечнем уничтоженных документов. Функция этого документа — удостоверить, что процедура была совершена по всем правилам. Члены комиссии в подтверждение этого ставят на акте свои подписи.

8.5. Информация на уничтожаемых носителях не должна быть подвержена восстановлению. В случае с бумажными носителями используют такие способы уничтожения, как измельчение (ножницами или с помощью shreddera), сжигание и др.

При данной обработке носители будут невосстановимы.

8.6. За результативность процесса несут ответственность члены комиссии.

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

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

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

9.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

9.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

9.5. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

9.6. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и в соответствии с Федеральным законом № 152-ФЗ «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

9.7. Организация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- 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;
- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию организации или в иных аналогичных целях;

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

9.8. Во всех остальных случаях оператор (руководитель организации, осуществляющей образовательную деятельность, и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

10. Заключительные положения

10.1. Настоящее Положение является локальным нормативным актом ДОУ, принимается Общим собранием работников Образовательного учреждения и утверждается (либо вводится в действие) приказом заведующего ДОУ.

10.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии с действующим законодательством РФ.

10.3. Срок действия данного Положения не ограничен. Положение действует до принятия нового.