Муниципальное дошкольное образовательное бюджетное учреждение
центр развития ребёнка – детский сад № 38 «Дюймовочка»
Октябрьского муниципального округа

УТВЕРЖДЕНО
Заведующий
МДОБУ ЦРР – д/с № 38
«Дюймовочка»
_____/О.А. Смирнова/
Приказ № 20 – О от 06.03.2023г.

ПОЛОЖЕНИЕ
о порядке обработки и защите персональных данных работников МДОБУ центр развития ребёнка – детский сад № 38 «Дюймовочка»

2023г.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об обработке и защите персональных данных работников (далее – Положение) регулирует отношения, связанные с обработкой и защитой персональных данных работников (далее – работник, субъект персональных данных) муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 37» (далее – ДОУ, работодатель, оператор) и гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю, а также устанавливает ответственности должностных лиц, имеющих доступ к персональным данным работников ДОУ.

1.2. Настоящее Положение разработано с целью обеспечения защиты прав и свобод работников ДОУ при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну работников от несанкционированного доступа, неправомерного их использования или утраты.

1.3 Настоящее Положение разработано в соответствии с: - Конституцией Российской Федерации; - Трудовым кодексом Российской Федерации; - Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; - Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»; - Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»; - Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; - иными нормативными актами, регулирующими вопросы обработки персональных данных и обеспечения безопасности конфиденциальной информации; - Коллективным договором ДОУ; - Уставом ДОУ.

1.4. В целях настоящего Положения используются следующие основные понятия:

1.4.1 Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

1.4.2. Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом№ 152-ФЗ «О персональных данных».

1.4.3. 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.

1.4.4. 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.

1.4.5. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.4.6. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.4.7. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.4.8. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.4.9. 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.

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

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

1.4.12. Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.
1.4.13. Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
1.5. В состав персональных данных, которые работник сообщает работодателю, входит:
- фамилия, имя, отчество;
- пол;
- дата рождения;
- возраст;
- гражданство;
- сведения об образовании, квалификации, профессиональной подготовке, повышении квалификации;
- адрес места проживания;
- паспортные данные;
- сведения о воинском учете;
- страховой номер индивидуального лицевого счета;
- сведения о трудовой деятельности;
- иные сведения, которые относятся к трудовой деятельности работника.
1.6. Документами, которые содержат персональные данные работников, являются: - комплекты документов, сопровождающих процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; - комплекты материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;
- подлинники и копии приказов (распоряжений) по кадрам;
- личные дела, трудовые книжки, сведения о трудовой деятельности работников;
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- копии отчетов, направляемых в государственные контролирующие органы;
- копия страхового свидетельства государственного пенсионного страхования;
- копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе – автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- документы о возрасте малолетних детей и месте их обучения;
- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);
- документы, которые с учётом 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, и психиатрического освидетельствования);
- трудовой договор;
- заключение по данным психологического исследования (если такое имеется);
- копии приказов о приёме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- личная карточка по форме Т-2;
- заявления, объяснительные и служебные записки работника;
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая

приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

II. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА И ГАРАНТИИ ИХ ЗАЩИТЫ

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

2.1.1. 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.

2.1.2. При определении объёма и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться ст. 24 Конституции Российской Федерации, ст. 65 Трудового Кодекса и иными федеральными законами.

2.1.3. 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.

2.1.4. Работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся (в соответствии со ст. 10 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных») 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;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О 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 25.01.2002 г. № 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.
2.1.5. 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.
2.1.6. Работодатель не вправе требовать от работника представления персональных данных, которые не характеризуют работника как сторону трудовых отношений.
2.1.7. 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.
2.1.8. Работодатель также не вправе принимать решения, затрагивающие интересы работника, основываясь на данных, допускающих двоякое толкование. В случае если на основании персональных данных работника невозможно достоверно установить какой - либо факт, работодатель предлагает работнику представить письменные разъяснения.
2.1.9. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счёт собственных средств, в порядке, установленном Трудовым Кодексом и иными федеральными законами.
2.1.10. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
2.1.11. Работники не должны отказываться от своих прав на сохранение и защиту тайны.
2.1.12. Работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.
2.2. ДОУ определяет объём, содержание обрабатываемых персональных данных работников, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.
2.3. 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.

2.4. Обработка Оператором персональных данных осуществляется в следующих целях:
1. Цель обработки: подбор персонала (соискателей) на вакантные должности оператора

Категории данных	Персональные данные	Специальные данные
Перечень данных	фамилия, имя, отчество пол гражданство дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; страховой номер индивидуального лицевого счета (СНИЛС);	Сведения о состоянии здоровья

	сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации; семейное положение, наличие детей, родственные связи; сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий; данные о регистрации брака; сведения о воинском учете; сведения об инвалидности; сведения о судимости, привлечении к уголовной ответственности иные персональные данные, предоставляемые соискателями по их желанию	
Категории субъектов	Кандидаты на работу (соискатели)	
Способы обработки	Автоматизированная обработка и без средств автоматизации	
Сроки обработки	В течение срока, необходимого для рассмотрения кандидатуры соискателя и заключения трудового договора	
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе для анкеты (резюме) соискателя – 30 дней	
Порядок уничтожения	В соответствии с Порядком уничтожения персональных данных в ДОУ в зависимости от типа носителя персональных данных	

2. Цель обработки: обеспечение соблюдения трудового законодательства РФ

Категории данных	Персональные данные	Специальные персональные данные	Биометрические персональные данные
Перечень данных	фамилия, имя, отчество; пол; гражданство; дата и место рождения; изображение (фотография); паспортные данные; адрес регистрации по месту жительства; адрес фактического проживания; контактные данные; индивидуальный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации; семейное положение, наличие детей, родственные	Сведения о состоянии здоровья	Изображение на фото и видеозаписи, полученных с камер наблюдения

	связи; сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий; данные о регистрации брака; сведения о воинском учете; сведения об инвалидности; сведения об удержании алиментов; сведения о доходе с предыдущего места работы; сведения о судимости, привлечении к уголовной ответственности; иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства		
Категории субъектов	Работники, их родственники		
Способы обработки	Автоматизированная обработка и без средств автоматизации, в том числе: - получение персональных данных в устной и письменной форме непосредственно от субъектов персональных данных; - внесения персональных данных в журналы, реестры и информационные системы и документы ДОУ		
Сроки хранения	В течение срока, установленного номенклатурой дел в зависимости от типа документа, в котором содержатся персональные данные, в том числе в составе личных дел – 50 лет		
Порядок уничтожения	В соответствии с Порядком уничтожения персональных данных в ДОУ в зависимости от типа носителя персональных данных		

2.5. Работник представляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

2.6. При изменении персональных данных работник письменно уведомляет работодателя о таких изменениях в разумный срок, не превышающий 5 дней.

2.7. По мере необходимости работодатель истребует у работника дополнительные сведения. Работник представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

2.8. Чтобы обрабатывать персональные данные работников, работодатель получает от каждого работника согласие на обработку его персональных данных. Такое согласие работодатель получает, если закон не предоставляет работодателю права обрабатывать персональные данные без согласия работников.

2.9. Согласие на обработку персональных данных может быть отозвано работником. В случае отзыва работником согласия на обработку персональных данных работодатель вправе продолжить обработку персональных данных без согласия работника при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ.

2.10. Ответственным за организацию обработки персональных данных работников ДОУ является делопроизводитель, назначенный в соответствии с приказом руководителя ДОУ.

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

III. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. ДОУ обеспечивает защиту персональных данных работников от неправомерного использования или утраты.

3.2. 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.

3.3. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.4. Персональные данные работников ДОУ хранятся на бумажных и электронных носителях (к доступу имеется определенный код), в специально предназначенных для этого помещениях.

3.5. Персональные данные работников могут также храниться в электронном виде в локальной компьютерной сети ДОУ. Доступ к электронным базам данных, содержащим персональные данные работников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются руководителем ДОУ и сообщаются индивидуально работникам, имеющим доступ к персональным данным работников.

3.6. Изменение паролей производится руководителем ДОУ не реже одного раза в два месяца.

3.7. 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.

3.8. Доступ к персональным данным работников имеют:

- заведующий ДОУ;
- заместитель заведующего по ХЧ;
- главный бухгалтер;
- иные работники, определяемые приказом руководителя ДОУ в пределах своей компетенции.

3.9. Помимо лиц, указанных в п. 3.4. настоящего Положения, право доступа к персональным данным работников имеют лица, уполномоченные действующим законодательством.

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

3.11. Копировать и делать выписки из персональных данных работника разрешается исключительно в служебных целях с разрешения руководителя ДОУ или его заместителя.

IV. ПЕРЕДАЧА И РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

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

4.1.1. Не сообщать 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.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

4.1.3. 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.

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

4.1.5. 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
4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.
4.1.7. 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.
4.2. При передаче работодателем персональных данных работника сотрудник должен дать на это согласие в письменной или электронной форме. Если сотрудник оформил согласие на передачу персональных данных в электронной форме, то он подписывает согласие усиленной электронной цифровой подписью.
4.3. Работодатель вправе передать информацию, которая относится к персональным данным работника, без его согласия, если такие сведения нужно передать по запросу государственных органов, в порядке, установленном законодательством.
4.4. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение информации, относящейся к персональным данным работника, работодатель обязан отказать лицу в выдаче информации. Лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации, копия уведомления подшивается в личное дело работника.
4.5. Работодатель не вправе распространять персональные данные работников третьим лицам без согласия работника на передачу таких данных.
4.6. Согласие на обработку персональных данных, разрешенных работником для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.
4.7. Работодатель обязан обеспечить работнику возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на распространение персональных данных.
4.8. В случае если из предоставленного работником согласия на распространение персональных данных не следует, что работник согласился с распространением персональных данных, такие персональные данные обрабатываются работодателем без права распространения.
4.9. В случае, если из предоставленного работником согласия на передачу персональных данных не следует, что работник не установил запреты и условия на обработку персональных данных или не указал категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, работодатель обрабатывает такие персональные данные без возможности передачи (распространения, предоставления, доступа) неограниченному кругу лиц.
4.10. Согласие работника на распространение персональных данных может быть предоставлено работодателю: - непосредственно; - с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.
4.11. В согласии на распространение персональных данных работник вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных работодателем неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ работодателя в установлении работником данных запретов и условий не допускается.
4.12. Работодатель обязан в срок не позднее трех рабочих дней с момента получения согласия работника на распространение персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных работника для распространения.
4.13. Передача (распространение, предоставление, доступ) персональных данных, разрешенных работником для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению.
4.14. Действие согласия работника на распространение персональных данных прекращается с момента поступления работодателю требования, указанного в пункте 4.13 настоящего Положения.
4.15. Работник вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных для распространения, к

любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ или обратиться с таким требованием в суд. Работодатель или третье лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования работника или в срок, указанный во вступившем в законную силу решении суда. Если такой срок в решении суда не указан, то работодатель или третье лицо обязаны прекратить передачу персональных данных работника в течение трех рабочих дней с момента вступления решения суда в законную силу.

V. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Федерального закона «О персональных данных», предоставляются Оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя. В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;
- подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Федерального закона «О персональных данных» все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона «О персональных данных», в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.3. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

5.4. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если: - иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных; - оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

5.5. Подтверждение уничтожения персональных данных осуществляется в соответствии с требованиями, установленными приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

5.6. В связи с утратой необходимости и (или) достижением целей обработки персональные данные подлежат комиссионному уничтожению.

5.7. Уничтожение носителей, содержащих персональные данные должно соответствовать следующим правилам:
- быть максимально надежным и конфиденциальным, исключая возможность последующего восстановления персональных данных;
- для проведения процедуры уничтожения персональных данных, обрабатываемых в ДОУ, создаются Комиссии по уничтожению персональных данных, назначаемая приказом заведующего, состоящая из работников ДОУ, допущенных к обработке персональных данных;
- уничтожение оформляется соответствующим Актом об уничтожении, по установленной настоящим Положением типовой форме, с учетом отбора носителей, содержащих персональные данные, обрабатываемые в ДОУ, к уничтожению;
- уничтожение должно касаться только тех носителей, содержащих персональные данные, обрабатываемые в ДОУ, которые подлежат уничтожению в связи с достижением цели обработки указанных персональных данных либо утраты необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей персональных данных.
5.8. По общему принципу уничтожение материальных носителей, содержащих персональные данные, осуществляется механическим способом (до степени, исключающей возможность воспроизведения персональных данных) либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.).
5.9. Персональные данные, обрабатываемые в ДОУ, хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.
5.10. Носители, содержащие персональные данные, обрабатываемые в ДОУ, уничтожаются по итогам работы Комиссий по уничтожению персональных данных, назначаемых приказом заведующей ДОУ (далее - Комиссии).
5.11. Носители, содержащие персональные данные, обрабатываемые в ДОУ, уничтожаются Комиссиями в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных либо утраты необходимости в их достижении.
5.12. Уничтожение персональных данных производится по мере необходимости, в зависимости от объемов, накопленных для уничтожения бумажных и электронных носителей персональных данных, но не реже одного раза в год. Комиссии производят отбор бумажных и электронных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.
5.13. На все отобранные к уничтожению носители (как бумажные, так и электронные) составляется Акт об уничтожении.
5.14. В Акте об уничтожении исправления не допускаются.
5.15. По результатам работы Комиссии составляется Акт об уничтожении, который подписывается членами Комиссии и утверждается председателем комиссии. Уничтожение носителей, содержащих персональные данные, обрабатываемые в ДОУ, производится на основании соответствующего Акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения данных, перечисленных в Акте об уничтожении.
5.16. Уничтожение 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, обезличивание).
5.17. Уничтожение бумажных носителей, содержащих персональные данные, обрабатываемые в ДОУ, осуществляется в следующем порядке:
1. Лица, ответственные за архивную обработку документов в ДОУ, осуществляют систематический контроль за выделением (отбором) документов на бумажных носителях, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.
2. Бумажные носители персональных данных (документы, их копии, выписки и прочее), уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации или, сжигаются.
3. По окончании уничтожения бумажных носителей комиссией составляется Акт об уничтожении бумажных носителей персональных данных по типовой форме (приложение № 1 к настоящему Положению).
4. Уничтожение персональных данных на бумажных носителях осуществляется под контролем лица, ответственного за обработку персональных данных, совместно с работником, осуществляющего мероприятия по защите информации.

5.18. Уничтожение носителей, содержащих персональные данные, обрабатываемые в ДОУ, в электронном виде осуществляется в следующем порядке:
1. К персональным данным, обрабатываемым в ДОУ в электронном виде, относятся файлы, папки, электронные архивы на жестких дисках компьютеров и машиночитаемых носителях (компакт-дисках CB-R/RW или DVD-R/RW, флеш-носителях и т.д.), а также сведения, обрабатываемые в автоматизированных информационных системах персональных данных (далее - ИСПДн), используемых в ДОУ. Уничтожение носителей, содержащих персональные данные, обрабатываемые в ДОУ, в электронном виде осуществляется путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя или его сжигания.
2. Машиночитаемые носители (компакт-диски и дискеты) по истечению сроков обработки и хранения на них персональных данных, подлежат уничтожению. Компакт диски и дискеты физически уничтожаются с целью невозможности восстановления и дальнейшего использования путем деформирования, нарушения единой целостности носителя или его сжигания.
3. Подлежащие уничтожению файлы с персональными данными, обрабатываемыми в ДОУ, расположенные на жестких дисках компьютеров, в ИСПДн, удаляются средствами операционной системы компьютера с последующим «очищением корзины».
4. В случае допустимости повторного использования носителей формата CDRW, DVD-RW, флэш-носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.
5. С целью ведения статистического учета и отчетности, снижения ущерба от разглашения обрабатываемых в ДОУ персональных данных и обеспечения защищенности ИСПДн, если иное не предусмотрено действующим законодательством Российской Федерации, Комиссией на основании соответствующего Акта производится обезличивание персональных данных, обрабатываемых в ДОУ, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных. Обезличивание персональных данных осуществляется в ДОУ в соответствии с приказом Роскомнадзора от 5 сентября 2013г. №996 «Об утверждении требований и методов по обезличиванию персональных данных». Комиссия несет ответственность за организацию и проведение мероприятий по уничтожению (обезличиванию) персональных данных. Обезличенные персональные данные не подлежат разглашению. В последующем при обработке обезличенных персональных данных в ИСПДн, используемых в ДОУ, необходимо соблюдение: - парольной политики; - антивирусной политики; - правил работы со съемными носителями; - правил резервного копирования; - правил доступа в помещения, где расположены автоматизированные рабочие места пользователей, соответствующих ИСПДн.
5.19. Уничтожение по окончании срока обработки персональных данных (обезличенных персональных данных) в ИСПДн, используемых в ДОУ, производится удалением персональных данных методами и средствами гарантированного удаления остаточной информации.
5.20. В ходе осуществления вышеуказанных процедур уничтожения электронных носителей (форматирования носителей, обезличивания персональных данных и т.д.) требуется присутствие всех членов Комиссии.
5.21. Во всех вышеуказанных случаях уничтожение носителей, содержащих персональные данные, обрабатываемые в ДОУ, Комиссия составляет и подписывает Акт об уничтожении персональных данных на электронных носителях (информации, содержащейся на электронных носителях, информации из информационных систем, используемых в ДОУ) по типовой форме (приложение № 2 к настоящему Положению).

VI. ПОРЯДОК ОФОРМЛЕНИЯ ДОКУМЕНТОВ ОБ УНИЧТОЖЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Комиссия составляет и подписывает Акт об уничтожении бумажных носителей персональных данных по установленной настоящим Положением типовой форме. После утверждения соответствующего Акта председателем Комиссии Акты направляются для хранения в архив ДОУ.
6.2. Комиссия составляет и подписывает Акт об уничтожении персональных данных на электронных носителях (информации, содержащейся на электронных носителях, информации из информационных систем, используемых в ДОУ), по установленной настоящим Положением типовой форме. После утверждения соответствующего Акта председателем Комиссии Акты направляются для хранения в архив ДОУ.
6.3. Каждый факт уничтожения носителя персональных данных фиксируется в «Журнале регистрации носителей персональных данных», оформляемом по форме, предусмотренной в приложении № 3 к

настоящему Положению, который хранится у заведующей. В графе журнала «Дата и номер акта уничтожения» заносятся соответствующие данные.

VII. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Оператор и иные лица, получившие доступ к персональным данным работника, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
7.2. 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.
7.3. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.
7.4. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.
7.5. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами.
7.6. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.
7.7. Основными мерами защиты ПД, используемыми Оператором, являются:
7.7.1. Назначение лица, ответственного за организацию обработки ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД.
7.7.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД и разработка мер и мероприятий по защите ПД.
7.7.3. Разработка политики в отношении обработки персональных данных.
7.7.4. Установление правил доступа к ПД, обрабатываемых в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПД в ИСПД.
7.7.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.
7.7.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.
7.7.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
7.7.8. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.
7.7.9. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.
7.7.10. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
7.7.11. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Оператора в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.
7.7.12. Осуществление внутреннего контроля и аудита.
7.7.13. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.
7.8. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.
7.9. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор: - в течение 24 часов – уведомляет Роскомнадзор о произошедшем инциденте,

предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом; - в течение 72 часов – уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

7.10. Взаимодействия оператора с Роскомнадзором в рамках ведения реестр учета инцидентов в области персональных данных осуществляется в соответствии с приказом Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

7.11. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Закона о персональных данных производится в соответствии с приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"».

7.12. Угрозы защищенности персональных данных.

7.12.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

7.12.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением – внешними программами, которые установлены на компьютерах работников.

7.12.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

7.13. Уровни защищенности персональных данных.

7.13.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

7.13.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории ПД работников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

7.13.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические ПД, или при третьем типе угрозы работодатель обрабатывает общие ПД более чем 100 тыс. физических лиц.

7.13.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.

7.14. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

7.15. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 5.10 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности ПД в информационной системе.

7.16. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 5.10, 5.11 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

7.17. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 5.10-5.12 настоящего Положения, работодатель: - обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;

- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

7.18. В целях защиты ПД на бумажных носителях работодатель: - приказом назначает ответственного за обработку ПД; - ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников; - хранит документы, содержащие ПД работников в шкафах, запирающихся на ключ; - хранит трудовые книжки работников в сейфе в отделе кадров.
7.19. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии, учебной части и службы охраны труда работодателя.
7.20. Работники отдела кадров, бухгалтерии, учебной части и службы охраны труда работодателя, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.
7.21. Допуск к документам, содержащим ПД работников, внутри ДОУ осуществляется на основании Регламента допуска работников к обработке персональных данных.
7.22. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.
7.23. Передача информации, содержащей сведения о ПД работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

VIII. ПРАВА РАБОТНИКА В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ХРАНЯЩИХСЯ У РАБОТОДАТЕЛЯ

8.1. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право:
8.1.1. Получать полную информацию о своих персональных данных и их обработке.
8.1.2. 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 ответственному за организацию обработки персональных данных работников.
8.1.3. На определение своих представителей для защиты своих персональных данных.
8.1.4. На доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору.
8.1.5. Требовать об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. При отказе руководителя ДОУ исключить или исправить персональные данные работника, работник имеет право заявить в письменном виде руководителю ДОУ о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.
8.1.6. Требовать об извещение ДОУ всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях.
8.1.7. Обжаловать в суде любые неправомерные действия или бездействия ДОУ при обработке и защите его персональных данных.

IX. ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ ДОСТОВЕРНОСТИ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. В целях обеспечения достоверности персональных данных работники обязаны:
9.1.1. При приёме на работу в ДОУ представлять уполномоченным работникам достоверные сведения о себе в порядке и объёме, предусмотренном законодательством Российской Федерации.
9.1.2. 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 5 рабочих дней с даты их изменений.

X. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

10.1. 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.
10.2. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
10.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие её, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
10.4. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несёт материальную ответственность в соответствии с действующим трудовым законодательством.
10.5. Материальный ущерб, нанесённый субъекту персональных данных за счёт ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.
10.6. 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 понесенных субъектом персональных данных убытков.
10.7. ДОУ вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:
• включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
• в случае если Оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;
Во всех остальных случаях оператор (руководитель ДОУ и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящее Положение является локальным нормативным актом, принимается на Общем собрании работников ДОУ и утверждается (либо вводится в действие) приказом руководителя ДОУ.
11.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации.
11.3. Положение о защите персональных данных работников ДОУ принимается на неопределенный срок. Изменения и дополнения к Положению принимаются в порядке, предусмотренном п.11.1. настоящего Положения.
11.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение № 1

**Типовые формы документов,
в которых используется персональные данные субъектов ПДн,
необходимые для функционирования различных подразделений
образовательного учреждения.**

Наименование типового документа	Состав персональных данных	Цель составления документа	Основание
1	2	3	4
Бухгалтерия			
Доверенность	Ф.И.О, паспортные данные	Получение товарно-материальных ценностей	Приказы Минфина России: от 28.12.2001г. № 119н «Об утверждении Методических указаний по бухгалтерскому учету материально производительных запасов» и от 01.12.2010 г. № 157н «Об утверждении единого плана счетов бухгалтерского учета для органов государственной власти (государственных органов), органов местного самоуправления, органов управления государственными внебюджетными фондами, государственных академий наук, государственных (муниципальных) учреждений и Инструкции по его применению» (далее – Приказ Минфина России № 157н)
Договор	Ф.И.О., паспортные данные, адрес регистрации, должность, ИНН, № страхового свидетельства	Начисление заработной платы	Трудовой кодекс Российской Федерации (далее ТК РФ), Приказ Минфина России № 157н
Формы налогового учета	То же	Ведение в качестве налогового агента учета доходов, полученных физическими лицами в виде заработной платы	Налоговый кодекс Российской Федерации от 05.08.2000 г. № 117-ФЗ, Приказ Минфина России № 157н
Индивидуальные сведения	То же	Предоставление персонифицированных данных в Пенсионный фонд РФ	Федеральный закон от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Приказ Минфина России № 157н
Отдел кадров			
Трудовой договор	Ф.И.О., паспортные данные, должность, ИНН, № страхового свидетельства	Прием на работу	Ст. 65 ТК РФ

Анкета работника	Ф.И.О., паспортные данные	Прием на работу	Ст. 65 ТК РФ
Личная карточка (форма Т-2)	Ф.И.О., паспортные данные, адрес регистрации, должность, ИНН, № страхового свидетельства	Прием на работу	Ст. 65 ТК РФ
Табель учета рабочего времени	То же	Прием на работу. Начисление заработной платы	Ст. 65 ТК РФ
Заявление о приеме на работу	То же	Прием на работу	Ст. 65 ТК РФ

Приложение № 2

Согласие
на обработку персональных данных
для сотрудника.

Я, _____(**далее Субъект**),
зарегистрированный)
(ФИО субъекта персональных данных)
по адресу:_____
_____
(адрес субъекта персональных данных)
паспорт серия_____ № _____ выдан _____
_____
_____ дата выдачи _
_____

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152 – ФЗ «О персональных данных» даю свое согласие МДОБУ ЦРР – детскому саду № 38 «Дюймовочка» (далее Оператор), расположенному по адресу : Приморский край, Октябрьский район, с.Покровка, ул.Завитая 3а, на обработку своих персональных данных на следующих условиях:

1. Субъект дает согласие на обработку своих персональных данных, как с использованием средств автоматизации, так и без использования таких средств (в том числе по телефону), т.е. совершение, в том числе следующих действий: сбор, систематизацию, накопления, хранения, уточнение, использование, блокирование, уничтожение, а также право на передачу такой информации третьим лицам для осуществления проверки информации о Субъекте в случаях, установленных законодательством, и по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их обработка будет осуществляться лицом, обязанным сохранять конфиденциальность персональных данных.
2. Перечень персональных данных субъекта, передаваемых оператору на обработку:

- Фамилия, имя, отчество, пол, дата и место рождения, адрес регистрации и проживания, контактные телефоны
- Иные паспортные данные (дата выдачи, серия, номер, кем выдан), фотография.
- Данные документа воинского учета.
- ИНН, номер свидетельства государственного пенсионного страхования.
- Данные о дипломе (свидетельстве, документа об образовании)– серия, номер, дата выдачи, вид образования, название учебного заведения, год окончания, вид обучения, специальность, квалификация по диплому (свидетельству).
- Основная профессия, специальность (должность в МДОБУ.)
- Стаж работы (общий, страховой, педагогический), последнее место работы.
- Семейное положение, сведения о составе семьи, сведения о состоянии здоровья и об индивидуальности.
- Данные документов о прохождении аттестации, обследовании, повышения квалификации, результатов оценки и обучения.
- Иные сведения, которые необходимы для корректного документального оформления правоотношений между субъектом и оператором.
- Данные иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены субъектом при заключении трудового договора или в период его действия
- Сумма подлежащая начислению, сведения о доходах, имуществе и имущественных обязательств.

3. Согласие дается Субъектом в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействие в трудоустройстве, предоставления информации

в медицинские учреждения, страховые компании; обеспечения предоставления социального пакета; обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, с целью исполнения оператором обязательств по трудовому договору. Оператор в праве обрабатывать персональные данные Субъекта посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами.

4. Обработка персональных данных (за исключением хранения) прекращается по достижению цели обработки или прекращения обязательств по заключенным договорам и соглашениям или исходя из документов Оператора, регламентирующих вопросы обработки персональных данных.

5. Субъект может отозвать настоящее согласие путем направления письменного заявления Оператору. В этом случае Оператор прекращает обработку персональных данных Субъекта, а персональные данные подлежат уничтожению.

6. Данное согласие действует в течении всего срока обработки персональных данных до момента, указанного в п. 4 или п. 5 данного согласия.

7. Согласие является приложением к «Приложению об обработке персональных данных», данным согласием подтверждается факт ознакомления с Положением и его содержанием.

«_____» _____20____г. _____ _____

Дата **Подпись** **ФИО субъекта**

Приложение № 3

ОБЯЗАТЕЛЬСТВО

о соблюдении конфиденциальности персональных данных и правил их обработки

Я, _____

_____,

в качестве сотрудника МДОБУ ЦРР детского сада № 38 «Дюймовочка» в период трудовых отношений с организацией в течении трех лет после их окончания **обязуюсь:**

- не разглашать сведения, содержащие персональные данные, которые стали известны мне в связи выполнением служебных обязанностей;
- не сообщать персональные данные субъектов третьей стороне без их письменного согласия, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью субъектов, а также в случаях установленных Федеральным законом;
- выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению безопасности персональных данных;
- в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, обрабатываемые в МДОБУ ЦРР детском саду № 38 «Дюймовочка» немедленно сообщить об этом ответственному за защиту персональных данных;
- в случае моего увольнения все носители персональных данных (рукописи, черновики, диски, дискеты, распечатки), которые находились в моем распоряжении в связи с выполнением служебных обязанностей – передать ответственному за защиту персональных данных;
- об утрате или недостачи носителей персональных данных, удостоверений, пропусков, ключей от защищенных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки сведений, немедленно сообщить ответственному за защиту персональных данных.

Я, предупрежден(а), что, в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, могу быть уволен(а) из МДОБУ ЦРР детского сада № 38 «Дюймовочка».

Мне известно, что нарушение настоящего Обязательства может повлечь уголовную, административную, гражданско – правовую или иную ответственность в соответствии с законодательством РФ.

_____

(должность) **(подпись)** **(Ф.И.О)**

Один экземпляр обязательства получил(а) «____»_____20____г.

_____

(подпись)

Приложение № 4

Заведующему муниципальным
дошкольным образовательным бюджетным
учреждением центром развития ребёнка –
детским садом №38 «Дюймовочка»
Смирновой О.А.

от _____
(Ф.И.О.)

_____

адрес: _____

_____

паспортные данные: _____

_____

_____

телефон: _____

Согласие на обработку персональных данных

Я,_____

(Ф.И.О. работника полностью)

предоставляя муниципальному дошкольному образовательному бюджетному учреждению центру развития ребёнка – детскому саду №38 «Дюймовочка» (далее – Учреждение), зарегистрированного по адресу: 692561 Приморский край, Октябрьский муниципальный округ, с.Покровка, ул. Завитая 3а, ИНН 2522020059, ОГРН 1022500858181, мои персональные данные (фотографию с подписью фамилии, имени, отчества) с целью размещения на официальном сайте Учреждения, своей волей и в своих интересах выражаю согласие на сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение) использование, распространение, обезличивание, блокирование, уничтожение этих данных при обработке без использования и с использованием средств автоматизации.

Настоящее согласие действует со дня его подписания и до дня отзыва в письменной форме.

_____ «____»_____202 г.

_____ _____

(подпись) (расшифровка) (дата подписания)