Муниципальное бюджетное учреждение дополнительного образования спортивная школа «Лидер» муниципального образования Щербиновский район

353620, Краснодарский край, Щербиновский район, станица Старощербиновская, ул. Советов 56
ИНН 2358005924 КПП- 235801001 ОГРН 1022305030978
Телефон 7-78-81 Факс (8 86151) 7-78-81
E-mail: St.sport_school@mail.ru

ПРИНЯТО:

Решением педагогического совета
МБУ ДО СШ «Лидер» МОЩР
Протокол № 2
от 17 февраля 2023 года

УТВЕРЖДАЮ:

Директор МБУ ДО
СШ «Лидер» МОЩР
_____ Н.Г. Федотова

«17» февраля 2023 года

СОГЛАСОВАНО:
Председатель первичной
профсоюзной организации
МБУ ДО СШ «Лидер» МОЩР
_____ Д.А. Ерохин
Протокол № 2
от 17 февраля 2023 года

ПОЛОЖЕНИЕ
о защите, обработке, хранении и использовании персональных данных работников муниципального бюджетного учреждения дополнительного образования спортивная школа «Лидер» муниципального образования Щербиновский район

станица Старощербиновская

I. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными сотрудников муниципального бюджетного учреждения дополнительного образования спортивная школа «Лидер» муниципального образования Щербиновский район (далее - Учреждение).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и свобод работников Учреждения при обработке их персональных данных в информационной системе персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Учреждения, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Сведения о персональных данных работников относятся к числу конфиденциальных (составляющих охраняемую законом тайну Учреждения), хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

1.4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Сбор, хранение, использование и распространение, в том числе передача третьим лицам, персональных данных работников без письменного согласия не допускается.

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

1.7. В целях защиты частной жизни, личной и семейной тайны, работники Учреждения не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

1.8. Настоящее Положение и изменения к нему вступают в силу с момента их утверждения директором Учреждения. Все работники учреждения должны быть ознакомлены с данным Положением и изменениями к нему под роспись.

II. Основные понятия

2.1. Для целей настоящего Положения используются следующие основные понятия:

- **персональные данные работника** - любая информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника;

- **обработка персональных данных работника** - действия (операции) с персональными данными, сбор персональных данных, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распро-

странение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

- **конфиденциальность персональных данных** - обязательное для соблюдения Учреждением или иным уполномоченным должностным лицом (назначенного ответственного лица), получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;

- **распространение персональных данных** – действия (операция) с персональными данными, направленные на передачу персональных данных работников определенному кругу лиц или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным работников каким-либо иным способом;

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

- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

- **уничтожение персональных данных** – действия (операции), в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;

- **обезличивание персональных данных** – действия (операции), в результате которых невозможно определить принадлежность персональных данных конкретному работнику;

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

- **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (в т.ч. Учреждение);

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

- **документированная информация** – информация зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

- **информационная система персональных данных** – информационная система, представляющая собой совокупность персональных данных, содержа-

щихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

- **пользователь** – сотрудник Учреждения, использующий ресурсы информационной системы предприятия для выполнения должностных обязанностей;

- **учетная запись** – информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе, также может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.);

- **пароль** – секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системы для получения доступа к данным и программам. Является средством защиты данных от несанкционированного доступа.

III. Принципы обработки персональных данных работника

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а так же полномочиям Учреждения;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации;
- наличие четкой разграничительной системы доступа работников Учреждения к документам и базам данных, содержащим персональные данные.

IV. Порядок обработки персональных данных в информационной системе персональных данных с использованием средств автоматизации

4.1. Обработка персональных данных в информационной системе персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 05.02.2010 №58 «О методах и способах защиты информации в информационных системах персональных данных».

4.3. Не допускается обработка персональных данных в информационной системе персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационной системы персональных данных, включающих акт классификации ИСПДН, инструкции пользователя, администратора по организации антивирусной защиты, и других нормативных и методических документов;

- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств, в соответствии с требованиями безопасности информации;

- охраны и организации режима допуска в помещение, предназначенное для обработки персональных данных.

4.4. Порядок обработки персональных данных без использования средств автоматизации.

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

4.4.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки, которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

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

4.4.3. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

4.4.4. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

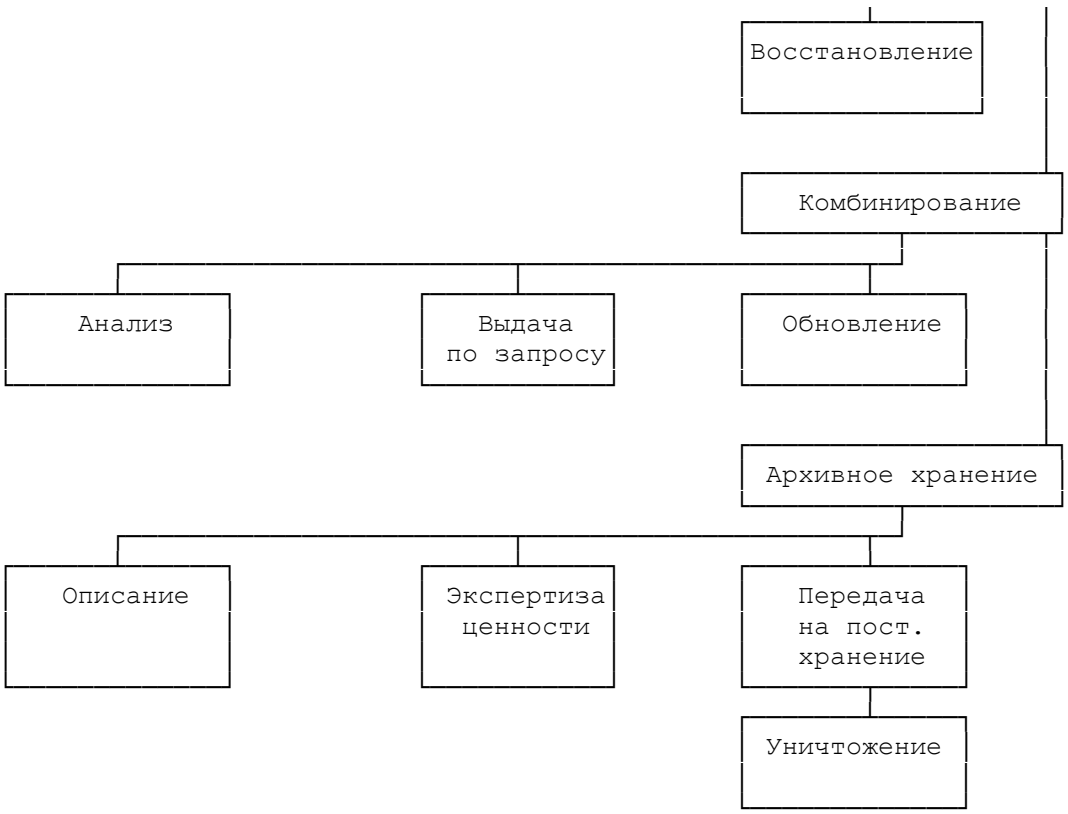
4.5. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

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

V. Организация обработки персональных данных сотрудников

5.1. Обработка персональных данных сотрудников организуется в соответствии со схемой 1.

Схема 1



5.2. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина работодатель и его законные, полномочные представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

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

5.2.2. При определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

5.2.3. Персональные данные следует получать у самого работника. Если персональные данные работника, возможно, получить только у третьей стороны, работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие (Приложение №4). Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

5.2.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья и частной жизни. В случаях, непосредственно связанных с вопросами трудовых от-

ношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) только с его письменного согласия.

5.2.5. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

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

5.2.7. Защита персональных данных сотрудника от неправомерного их использования, утраты, обеспечивается работодателем, за счет его средств в порядке, установленном федеральным законом.

5.2.8. Работники и их представители должны быть ознакомлены под роспись с документами Учреждения, определяющими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

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

5.2.10. Работодатель, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

5.3. Работодатель вправе обрабатывать персональные данные сотрудников только с их письменного согласия.

5.3.1. Письменное согласие сотрудника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

5.3.2. Согласие сотрудника не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия работодателя;

- обработка персональных данных в целях исполнения трудового договора;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов сотрудника, если получение его согласия невозможно.

5.3.3. Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия работодателя;

- обработка персональных данных в целях исполнения трудового договора;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- персональные данные относятся к состоянию здоровья работника, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

VI. Состав персональных данных работников

6.1. Персональные данные работника - любая информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

6.2. В состав персональных данных работника входят:

- фамилия, имя, отчество работника;

- дата и место рождения работника;

- адрес работника по прописке;

- адрес проживания (реальный);

- паспортные данные (серия, номер паспорта, кем и когда выдан);

- информация о трудовом стаже (место работы, должность, период работы, причины увольнения);

- семейное положение и состав семьи (муж/жена, дети);

- телефонный номер (домашний, рабочий, мобильный);

- образование, профессия работника;

- оклад;

- данные о трудовом договоре;

- сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

- ИНН;

- информация о приеме на работу, перемещении по должности, увольнении;

- информация об отпусках;

- информация о командировках;

- информация о болезнях;

- информация о негосударственном пенсионном обеспечении;

- другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

6.3. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса РФ лицо, поступающее на работу, предъявляет:

- паспорт или иной документ, удостоверяющий личность (серия, номер паспорта, кем и когда выдан);

- трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета - для лиц, подлежащих воинскому учету (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

- свидетельство о присвоении ИНН (при его наличии у работника).

6.4. При оформлении работника отделом кадров заполняется унифицированная форма Т-2 "Личная карточка работника", в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);

- сведения о воинском учете;

- данные о приеме на работу;

- сведения об аттестации;

- сведения о повышенной квалификации;

- сведения о профессиональной переподготовке;

- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;

- сведения о социальных гарантиях;

- сведения о месте жительства и о контактных телефонах.

6.5. В отделе кадров Учреждения создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

6.5.1. Документы, содержащие персональные данные сотрудников:

- комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
- комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;
- подлинники и копии приказов (распоряжений) по кадрам;
- личные дела и трудовые книжки;
- дела, содержащие основания к приказу по личному составу;
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

6.5.2. Документация по организации работы структурных подразделений:

- положения о структурных подразделениях;
- должностные инструкции работников;
- приказы, распоряжения, указания руководства Учреждения;
- документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

VII. Доступ к персональным данным работников

7.1. **Внутренний доступ (доступ внутри организации).**

7.1.1. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора Учреждения.

7.1.2. Право доступа к персональным данным сотрудников имеют:

- руководитель Учреждения;
- работники отдела кадров;
- работники бухгалтерии;
- начальник отдела экономической безопасности (информация о фактическом месте проживания и контактные телефоны работников);

7.2. **Внешний доступ.**

7.2.1. К числу массовых потребителей персональных данных вне учреждения можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды.

7.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7.2.3. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.2.4. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

VIII. Передача персональных данных работника

8.1. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

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

8.2.1. 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 случаях, установленных федеральным законом.

8.2.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, допускается только с его предварительного согласия.

8.2.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

8.2.4. Осуществлять передачу персональных данных работников в пределах Учреждения в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под роспись.

8.2.5. Персональные данные работников должны быть доступны в Учреждении только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения их конкретных функций.

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

8.2.7. Передавать персональные данные работника его законным, полномочным представителям работников в порядке, предусмотренном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

8.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника (Приложение №5), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

8.4. Персональные данные работников обрабатываются и хранятся в отделе кадров.

8.5. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранения, как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

8.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных работника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

8.7. При получении персональных данных не от работника (за исключением случаев, если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральными законами права субъекта персональных данных.

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

8.9. Копировать и делать выписки персональных данных сотрудника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров или Директора Учреждения.

IX. Защита персональных данных

9.1. 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.

9.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии техни-

ческих средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

9.3. 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.

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

9.5. **«Внутренняя защита»**

9.5.1. 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.

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

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- 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;
- регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и хранение съемных носителей информации, и их обращение, исключающее хищение, подмену и уничтожение;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

9.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается ИТ – специалисту.

9.5.4. В состав системы защиты персональных данных в информационной системе персональных данных должны быть включены следующие средства:

средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационной системе персональных данных;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности.

9.5.5. При взаимодействии информационной системы с сетями общего пользования основными методами и способами защиты информации от несанкционированного доступа являются:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

- защита информации при ее передаче по каналам связи;

- использование средств антивирусной защиты;

- использование защищенных каналов связи.

9.5.6. Сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (спец. помещениях, шкафах, и т.п.).

9.5.7. Специалистами учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

9.6. «Внешняя защита».

9.6.1. 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.

9.6.2. 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.

9.6.3. Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных.

9.7. По возможности персональные данные обезличиваются.

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

X. Права и обязанности работника в целях обеспечения защиты персональных данных, хранящихся у работодателя

10.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

10.2. В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники **имеют право** на:

- полную информацию об их персональных данных и об обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право получения копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определять своих представителей для защиты своих персональных данных;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового Кодекса. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суде любых неправомерных действий (бездействий) или бездействия работодателя при обработке и защите его персональных данных.

10.3. **Работник обязан:**

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
- своевременно сообщать работодателю об изменении своих персональных данных, ставить работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

XI. Ответственность за нарушение норм, регулирующих обработку персональных данных

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

11.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут дисциплинарную, административную, гражданско-правовую или уголов-

ную ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации. Каждый работник Учреждения, работающий с конфиденциальной информацией, подписывает Обязательство о неразглашении персональных данных (Приложение №1).

11.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

11.4. Руководитель Учреждения за нарушение порядка обращения с персональными данными несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях РФ, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом работнике.

11.5. Каждый работник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

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

11.8. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

11.9. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

11.10. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.