ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ ГРАЖДАН
ПОЖИЛОГО ВОЗРАСТА И ИНВАЛИДОВ
БОЛЬШЕМУРАШКИНСКОГО РАЙОНА»

П Р И К А З

«29» декабря 2017 года № 157

Об утверждении инструкции пользователя при обработке
работниками персональных данных

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 г. N1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, в целях организации работы по защите конфиденциальной информации в ГБУ "ЦСОГПВИИ Большемурашкинского района"

п р и к а з ы в а ю:

1. Утвердить инструкцию пользователя при обработке работниками персональных данных ГБУ "ЦСОГПВИИ Большемурашкинского района" (Приложение1).

2. Специалисту по кадрам Федяевой Ю.В. ознакомить под роспись работников ГБУ "ЦСОГПВИИ Большемурашкинского района" осуществляющих обработку персональных данных.

4. Контроль за исполнением данного приказа оставляю за собой.

Директор ГБУ «ЦСОГПВИИ
Большемурашкинского района» Л. Г. Макарова

Лист

ознакомления с приказом ГБУ "ЦСОГПВИИ Большемурашкинского района" от 29.12.2017г. № ___ "Об утверждении инструкции пользователя при обработке работниками персональных данных"

Заместитель директора	Т.Н.Калина
Главный бухгалтер	Е.А.Леднева
Специалист по кадрам	Ю.В.Федяева
Заведующий отделением социально-бытового обслуживания на дому	Н.П. Мотовичева
Заведующий отделением социально-бытового обслуживания на дому	Н.А. Кочеткова
Заведующий отделением срочного социального обслуживания	Н.В.Дьякова
Заведующий отделением социально-консультативной помощи	И.А.Ильина
Специалист по социальной работе	О.А.Плетнева
Специалист по социальной работе	А.А. Зиновьева
Специалист по социальной работе	Г.М.Додулева
Специалист по социальной работе	Н.И.Ситкова
Специалист по социальной работе	Т.И.Школина
Специалист по социальной работе	С.Н.Максимова
Специалист по социальной работе	С.С.Назарова
Специалист по социальной работе	Г.Н.Мерзлякова
Социальный работник отделения срочного социального обслуживания	Е.В.Серова

Приложение 1
к приказу ГБУ "ЦСОГПВИИ
Большемурашкинского
района"
от 29.12.2017г. № _157

Инструкция
пользователя при обработке сотрудниками персональных данных в Государственном бюджетном учреждении «Центр социального обслуживания граждан пожилого возраста и инвалидов Большемурашкинского района"

1. Общие положения

1.1.Инструкция определяет права, обязанности и ответственность пользователей при работе в автоматизированной системе персональных данных (далее - АС) с целью защиты от несанкционированного доступа (далее - НСД) к персональным данным. Также устанавливаются особый порядок обработки и хранения персональных данных, без использования средств автоматизации в Учреждении. Также инструкция определяет функции, задачи и порядок эксплуатации пользователями средств вычислительной техники (далее - СВТ), входящих в состав АС.

1.2.Пользователями АС являются сотрудники (работники) государственного бюджетного учреждения "Центр социального обслуживания граждан пожилого возраста и инвалидов Большемурашкинского района" (далее - Учреждение), допущенные к обработке персональных данных согласно утвержденному директором Учреждения перечню должностей.

1.3. Перед началом работ пользователь должен ознакомиться содержанием следующих документов: Федеральным законом от 27 № 152-ФЗ «О персональных данных»; эксплуатационной документацией на

установленные в АС средства защиты; нормативными актами Учреждения в области защиты персональных данных.

1.4. Оперативный контроль за действиями пользователей при работе с персональными данными осуществляет ответственный за обработку персональных данных (Администратор автоматизированной системы, локальной сети и т.п.) Учреждения, который имеет право приостановить обработку информации в случае выявления нарушений.

2. Термины и определения

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

2.2. **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.

2.3. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

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

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

2.6. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Автоматизированное рабочее место (АРМ)** – программнотехнический комплекс, посредством которого Пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.8. **Несанкционированный доступ (НСД)** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.9. **Посторонние лица** – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИСПДн и (или) не имеют допуска к персональным данным.

2.10. **Средство защиты информации от несанкционированного доступа (СЗИ от НСД)** – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

3. Обязанности пользователя

3.1. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения директора Учреждения.

3.3. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4. Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5. Знать и соблюдать установленные требования обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7. Незамедлительно, в кратчайшие сроки, сообщать директору Учреждения об утрате или недостаче носителей информации, ключей от помещений, хранилищ, сейфов и о других фактах, которые могут привести к разглашению персональных данных.

3.8. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, оптические диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы), передать директору Учреждения.

3.9. Соблюдать требования парольной политики (раздел 4).

3.10. Соблюдать требования антивирусной защиты (раздел 5).

3.11. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена (раздел 6).

3.12. Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию по обращению со средствами криптографической защиты информации.

3.13. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.14. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к ответственному за организацию обработки персональных данных.

Пользователям запрещается:

3.14.1. Нарушать установленные в Учреждении инструкции по работе с персональными данными.

3.14.2. Использовать компоненты программного и аппаратного обеспечения Учреждения в неслужебных целях.

3.14.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

3.14.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

3.14.5. Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флешнакопителях и т.п.).

3.14.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

3.14.7. Самовольно подключать АРМ, изменять IP-адрес и иные настройки сети АРМ.

3.14.8. Производить действия, направленные на получение несанкционированного доступа к АРМ, сети Интернет, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
- установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

˜ действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

˜ уничтожение, модификация программного обеспечения или данных без согласования с директором Учреждения или владельцами этого ресурса;

˜ попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

˜ умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Учреждения так и вне), либо на нарушение целостности и работоспособности этих систем;

˜ действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

3.14.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

3.14.10. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения директора Учреждения, не относящиеся к производственному процессу) программы (например: игры; IM-клиенты, такие как Google Messenger, ICQ и т.п..).

3.14.11. Разрешать посторонним лицам работать под своей учетной записью в ИСПДн.

3.14.12. Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

3.14.13. Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

3.14.14. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

3.14.15. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

3.14.16. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

3.14.17. Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования ИСПДн).

3.14.18. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя Учреждения.

4. Парольная политика

4.1. Общие требования к паролям:

˜ Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; ’] [{ } < > . и т.п.).

˜ Минимальная длина пароля: не менее 6 (шести) символов.

˜ Максимальный срок действия пароля: 90 суток.

˜ Запрет использования трех ранее использовавшихся паролей.

˜ Пароль Пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

˜ Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

˜ Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.).

4.2. Правила использования паролей:

˜ Хранить в тайне свой пароль, не сообщать его другим лицам.

˜ Не предоставлять доступ в ИСПДн другим лицам под своей учетной записью и паролем.

˜ Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

˜ Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д.

˜ Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

4.3. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:

˜ в случае подозрения на компрометацию пароля;

˜ по окончании срока действия;

˜ в случае прекращения полномочий (увольнение, переход на другую работу внутри Учреждения) Пользователя после окончания последнего сеанса работы в информационных системах персональных данных;

˜ по указанию ответственного за организацию обработки персональных данных.

4.4. При увольнении, переходе на новую должность работника, имеющего доступ помимо своей учетной записи к другим ресурсам

(межсетевые экраны, маршрутизаторы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

5. Антивирусная защита

5.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флеш–накопителе;
- ином съемном носителе информации;
- полученные иным способом.

5.2. Перед открытием вложения (ссылок) убедиться в том, что отправитель действительно послал вам этот файл, даже если он и должен был это сделать. Позвоните ему сами. Не доверяйте имени отправителя и указанным в тексте письма номерам телефонов, а также лицам, позвонившим вам самостоятельно с просьбой открыть файлы и пройти по ссылкам.

5.3. Пользователю запрещается:

5.3.1. Осуществлять действия, направленные на выключение антивирусной программы.

5.3.2. Самостоятельно устанавливать на АРМ программное обеспечение.

5.3.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

5.3.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - администратор

безопасности) должен провести внеочередной антивирусный контроль своего рабочего места.

5.3.5. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за обработку персональных данных в Учреждении;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

6. Порядок работы в ИСПДн и сети Интернет

6.1. Подключение к ИСПДн и сети Интернет.

6.2. Целью работы Пользователя в ИСПДн и сети Интернет является сбор, обработка, хранение персональных данных, обмен электронными сообщениями в служебных целях.

6.2.1. Доступ к ИСПДн и сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям настоящей Инструкции и иными нормативными документами в области защиты информации.

6.2.2. Доступ пользователя к ИСПДн для обработки персональных данных производится только с рабочих мест, на которых установлены средства защиты информации.

6.2.3. Ответственный за организацию обработки персональных данных, либо сотрудник, выполняющий его функции, осуществляет контроль над использованием данных ресурсов и сервисов.

6.2.4. Основанием для отключения пользователя от ИСПДн и сети Интернет являются следующие события:

- нарушение инструкций и иных локальных нормативных актов в области защиты информации Учреждения;
- увольнение Пользователя, либо перевод его в другое подразделение.

6.3. Порядок работы в сети Интернет.

6.3.1. Использование сотрудниками Учреждения сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

6.3.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника Учреждения является собственностью Учреждения и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

6.3.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

6.3.4. При работе в сети Интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;
- передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;
- фальсифицировать IP-адрес, иные адреса, используемые в сетевых протоколах, а также прочую информацию при передаче данных через сеть Интернет.
- предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную

вычислительную сеть Учреждения (например: путем несанкционированной установки локального Интернет-шлюза на рабочее место);

˜ получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, Правилами Учреждения т.п.);

˜ осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

˜ выполнять действия (взлом, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, программного обеспечения).

6.4. Правила работы Пользователей с электронной почтой:

6.4.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

6.4.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

6.4.3. Запрещается массовая рассылка почтовых сообщений (более 100) внешним адресатам без согласования с руководством (спама).

6.4.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

6.4.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat, js, vbs и т.п.). В случае необходимости отправки таких файлов, помещать их в архив и установить пароль.

6.4.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

6.4.7. Корпоративные рекомендации использования электронной почты:

˜ Вы должны оказывать то же уважение, что и при устном общении.

˜ Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением.

˜ Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания).

˜ Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию.

˜ Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям.

˜ Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания.

˜ Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки персональных данных без использования средств защиты (шифрование).

˜ Вы не должны использовать корпоративную электронную почту для посланий личного характера.

˜ Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

7. Порядок работы со съемными носителями информации

7.1. Под использованием носителей информации в ИСПДн Учреждения понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между информационными системами и носителями информации.

7.2. Допускается использование только учтенных носителей информации, которые являются собственностью Учреждения и подвергаются регулярной ревизии и контролю.

7.3.Если доступ к ИСПДн производится при помощи персональных идентификаторов (eToken, Rutoken, др.), то факт получения и сдачи данных идентификаторов обязательно фиксируется ответственным за организацию обработки персональных данных, в соответствующих журналах.

7.4.Возможность подключения носителей информации, а также

получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у Пользователя служебной необходимости.

7.5. При использовании носителей информации необходимо:

- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- бережно относится к носителям персональных данных.
- обеспечивать физическую безопасность носителей информации всеми разумными способами;
- извещать ответственному за организацию обработки персональных данных о фактах утраты (кражи) носителей информации.

7.6.При использовании носителей персональных данных запрещено:

- использовать носители персональных данных в личных целях;
- передавать носители персональных данных другим лицам (за исключением администраторов);
- хранить съемные носители с персональными данными на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

7.7.Любое взаимодействие (обработка, прием/передача информации) инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее).

7.8. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная

проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю Учреждения для принятия мер согласно локальным нормативным актам Учреждения и действующему законодательству РФ.

7.9. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

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

7.11. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

7.12.. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются и делаются соответствующие пометки в журнале учета машинных носителей.

8. Порядок обработки персональных данных без использования средств автоматизации в Учреждении

8.1. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации, в Учреждении:

8.1.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных

носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

8.1.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели, обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, должен использоваться отдельный материальный носитель.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; имя (наименование) и адрес оператора; фамилию, имя, отчество и адрес субъекта персональных данных;
- источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации (при необходимости получения письменного согласия на обработку персональных данных);
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными,

содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

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

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

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

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

8.1.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

8.1.6. Требования, предусмотренные пунктами 8.1.4. и 8.1.5. настоящих Правил, применяются также в случае, если необходимо обеспечить

раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

8.1.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

8.2. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации в Учреждении.

8.2.1. К обработке персональных данных, осуществляемая без использования средств автоматизации, допускаются только лица, согласно утвержденному директором Учреждения перечню должностей.

8.2.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8.2.3. Учет документов по обработке персональных данных без использования автоматизированных систем должен производиться отдельным делопроизводством. На документах должна указываться пометка «Персональные данные». Документы должны храниться в надежно запираемых шкафах и сейфах. Ключи от них, а также от помещений должны находиться у ответственных за данную работу лиц.

8.2.4. При обработке персональных данных необходимо соблюдать следующие требования:

- к работе допускаются только лица, назначенные соответствующим приказом;

- на период обработки защищаемой информации в помещении могут находиться лица, допущенные в установленном порядке к обрабатываемой информации;
- допуск других лиц может осуществляться с разрешения представителя нанимателя (работодателя);
- должен быть исключен несанкционированный просмотр обрабатываемой информации.

9. Сроки обработки и хранения персональных данных без использования средств автоматизации в Учреждении

9.1. Сроки обработки и хранения персональных данных работников Учреждения определяются в соответствии с законодательством Российской Федерации:

9.1.1. Персональные данные, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, о совмещении, об установлении выплат, поощрений, отпусках без сохранения заработной платы, отпусках по беременности и родам, по уходу за ребенком, и т.д.) хранятся в Учреждении в течение 75 лет.

9.1.1.1. В журналах регистрации - 75 лет, от момента последней регистрационной записи.

9.1.2. Персональные данные, содержащиеся в личных делах, а также личных карточках, завершенных в делопроизводстве, хранятся в Учреждении в течение 75 лет. Персональные данные, содержащиеся в личных делах, а также личных карточках, не завершенные в делопроизводстве в сейфе специалиста по кадрам.

9.1.3. Персональные данные, содержащиеся в приказах о предоставлении очередных отпусков, подлежат хранению у специалиста по кажпам в течение пяти лет с последующим уничтожением в установленном нормативно - правовыми актами порядке.

9.1.4. Персональные данные, содержащиеся в ведомостях, лицевых счетах, сведениях персонифицированного учета хранятся в Учреждении в течение 75 лет (в течение 5 лет от момента издания в кабинете бухгалтера).

9.2. Персональные данные граждан, обратившихся в Учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение пяти лет, от момента исполнения последнего обращения по одному и тому же вопросу.

9.3. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

9.4. Контроль за хранением и использованием материальных носителей персональных данных работников, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляет специалист по кадрам, главный бухгалтер, бухгалтер Учреждения.

9.5. Срок хранения персональных данных, внесенных в информационные системы персональных данных: «1:С Бухгалтерия», «СбиС++: Электронная отчетность», система «Сбербанк - бизнес онлайн», должен соответствовать сроку хранения бумажных оригиналов.

10. Права пользователя

10.1.Использовать ИСПДн Учреждения для выполнения должностных обязанностей.

10.2.Обращаться к ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

10.3.Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

10.4.Направлять предложения по модернизации АРМ (замены на новые аналоги), с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами.

10.5.Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Учреждении.

11. Ответственность

11.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые могут повлечь за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или их отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Учреждения.