Общество с ограниченной ответственностью
«УК «АРХСИТИ ГРУПП»

УТВЕРЖДАЮ
Директор
_____ М.С. Раздобурдин
«_16_» июля 2020г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных разработано в соответствии с Конституцией Российской Федерации, федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудового кодекса Российской Федерации, федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативно-правовых актов Российской Федерации в области обработки персональных данных.

1.2. Настоящее Положение определяет порядок и условия обработки персональных данных работников.

1.3. Настоящее Положение вступает в силу с момента его утверждения директором ООО «УК «АРХСИТИ ГРУПП» и является обязательным для исполнения всеми работниками, имеющим доступ к персональным сведениям работников.

1.4. Состав персональных данных, обрабатываемых ООО «УК «АРХСИТИ ГРУПП» определен Положением о персональных данных работников.

1.5. Информация о персональных данных может содержаться:
- на бумажных носителях;
- на электронных носителях.

2. Порядок сбора и уточнение персональных данных.

2.1. Сбор документов, содержащих персональные данные, осуществляется путем создания, копирования предоставленных оригиналов документов, внесения сведений в учетные формы (на бумажных и электронных носителях); внесение сведений в электронные информационные системы персональных данных.

2.2. Субъект персональных данных свои персональные данные предоставляет в ООО «УК «АРХСИТИ ГРУПП» самостоятельно либо через своего представителя. В случаях, предусмотренных законодательством, персональные данные также могут быть переданы оператору третьими лицами.

2.3. Субъект персональных данных при передаче своих персональных данных принимает решение о предоставлении ООО «УК «АРХСИТИ ГРУПП» давая согласие на обработку персональных данных в письменной форме.

2.4. Согласие на обработку персональных данных подписывается субъектом персональных данных собственноручно либо его представителем.

Равнозначным содержащему собственноручную подпись субъекта персональных данных, его представителя согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

2.5. Если согласие на обработку персональных данных дается представителем субъекта персональных данных от его лица, уполномоченным должностным лицом проверяются полномочия представителя (установленные в доверенности, либо основанные на иных документах).

2.6. Уточнение персональных данных производится путем обновления или изменения данных на бумажном носителе и (или) в электронной информационной системе персональных данных. Если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными

3. Обработка персональных данных

3.1. Обработка персональных данных – это любое действие (операция) или совокупность действий (опреаций), 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.

3.2. Общество использует следующие способы обработки персональных данных:
- без использования средств автоматизации;
- смешанная обработка (с применением объектов вычислительной техники).

3.2. Обработка персональных данных осуществляется:
- на основании согласия субъекта персональных данных;
- для выполнения возложенных на ООО «УК «АРХСИТИ ГРУПП» функций, полномочий и обязанностей;
- для заключения и исполнения договора, стороной которого является субъект персональных данных;
- для защиты жизни, здоровья и иных жизненно важных интересов субъекта персональных данных, если получение согласия работника невозможно;
- для осуществления прав и законных интересов ООО «УК «АРХСИТИ ГРУПП», третьих лиц либо для достижения общественно значимых целей, при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- для обработки информации в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- в иных, прямо предусмотренных федеральным законом случаях.

4. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

4.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в

отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

4.2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных, либо были извлечены из нее.

4.3. 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, в специальных разделах или на полях форм.

4.4. 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, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники ООО «УК «АРХСИТИ ГРУПП» или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами.

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

а) 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;

б) 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;

в) 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;

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

4.7. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

4.8. 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:

а) 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;

б) 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.

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

4.10. Правила, предусмотренные пунктами 4.8 и 4.9 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

5.1. Обработку персональных данных проводят только лица, назначенные приказом директора ООО «УК «АРХСИТИ ГРУПП».

5.2. Исключить несанкционированный просмотр обрабатываемой информации.

5.3 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

5.4. Раздельно хранить персональные данные (материальные носители), обработка которых осуществляется в различных целях.

5.5. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

5.6. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

6. Особенности обработки персональных данных, осуществляемой с использованием средств автоматизации

6.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

6.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

6.3. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

6.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа.

6.5. К паролям предъявляются следующие требования:

- пароль должен состоять из шести и более символов;
- пароль должен включать в себя буквы, цифры и специальные символы;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от значений трех предыдущих паролей.

6.6. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

6.7. Технические и программные средства должны удовлетворять требованиям, устанавливаемым законодательством Российской Федерации и обеспечивать защиту информации.

6.8. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

6.9. При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

6.10. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

7. Правила антивирусной защиты

7.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

7.2. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

7.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

7.4. В информационной системе персональных данных запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.5. 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 администратором, если он назначен на объекте) должен провести внеочередной антивирусный контроль своего персонального компьютера.

7.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:
- приостановить работу персонального компьютера;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности;
- провести «Лечение» или удаление зараженных файлов.

8. Восстановление после сбоев.

8.1. Работа любых технических средств связана с постоянным риском сбоя, вызванным как человеческим, так и природным факторами.

8.2. К природным факторам, вызывающим сбой работы технических средств, можно отнести любые природные явления – пожар, наводнение, землетрясение, ураганы, смерчи и т.д. Восстановление работоспособности технических средств в результате сбоя по причине природных факторов, крайне затруднено.

8.3. К человеческим факторам относятся перебои в подаче электроэнергии, разрушающие воздействия, направленные через сеть Интернет; вывод из рабочего состояния технических средств путем непосредственного воздействия на него в результате несанкционированного доступа (запуском вредоносных программ, затиранием системных файлов и т.д.).

8.4. Сотрудники, обрабатывающие персональные данные, должны следить за работой технических средств, и в случаях возникновения затруднений (медленная работа программ – «зависание», внеплановая перезагрузка операционной системы, оповещения антивирусным программным обеспечением о наличии вируса или вредоносной программы, произвольное открытие и закрытие операционных окон, передвижение курсора мыши и т.д.) сообщать администратору системы для принятия своевременных мер.

8.5. Во всех случаях прекращения работоспособности технического средства обработки персональных данных сотрудники обязаны оповестить администратора системы.

8.6. Администратор системы проводит выяснение причин прекращения работоспособности технических средств.

8.7. Для оперативного восстановления работоспособности системы необходимо вести резервное копирование файлов (база данных с персональными данными) не реже одного раза в полгода.

8.8. Резервные копии должны записываться на съемный носитель, учитываться в журнале учета съемных носителей и храниться в сейфе у ответственного лица.

8.9. Для исключения причин сбоев необходимо использовать источники бесперебойного питания, сертифицированные средства защиты информации от несанкционированного доступа, от воздействия из сети Интернет, а также соблюдение организационно-режимных мер по защите персональных данных.

9. Криптографическая защита

9.1. При передаче персональных данных третьим лицам (в Пенсионный фонд, Управление федеральной налоговой службы, банки и т.д.) через общедоступный

канал Интернет, необходимо использовать криптографические средства защиты канала связи и шифрование передаваемых данных.

9.2. Требования к криптографическим средствам и условиям их эксплуатации регламентируются Типовыми требованиями ФСБ от 21.02.2008г. № 149/6/6-622.

10. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

10.1. Все находящиеся на хранении и в обращении съемные носители (диски, дискеты, USB флеш - накопители, пр.), с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

10.2. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники, на которых возложены функции хранения носителей персональных данных. Работники ООО «УК «АРХСИТИ ГРУПП» получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. (Приложение 1). По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

10.3. Запрещается хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам, а также выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

10.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения директора ООО «УК «АРХСИТИ ГРУПП».

10.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения, содержащихся на них сведений немедленно ставится в известность директор ООО «УК «АРХСИТИ ГРУПП». На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

10.6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт (Приложение 2).

10.7. При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для систем высоких классов – также администратор системы безопасности. Техническое обслуживание оборудования должно осуществляться соответствующим обслуживающим персоналом.

11. Обязанности уполномоченных должностных лиц по защите персональных данных

11.1. Уполномоченные должностные лица обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных, настоящего Положения;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

11.2. При обработке персональных данных уполномоченным должностным лицам запрещается:

- использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;
- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации;
- снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные;
- выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, из места их хранения.

12. Порядок доступа работников ООО «УК «АРХСИТИ ГРУПП» в помещения, в которых ведется обработка персональных данных

12.1. Помещения, в которых ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

12.2. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

12.3. Вскрытие помещений, где ведется обработка персональных данных, производят работники, работающие в этих помещениях.

12.4. При отсутствии сотрудников, работающих в этих помещениях, помещения могут быть вскрыты комиссией, созданной по указанию директора.

12.5. В случае утраты ключей от помещений немедленно заменяется замок.

12.6. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии служащих, работающих в этих помещениях.

12.7. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка персональных данных, посторонних лиц, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность директор.

12.8. Одновременно принимаются меры по охране места происшествия и до выяснения обстоятельств в эти помещения никто не допускается.

13. Обезличивание персональных данных

13.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

13.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- .уменьшение перечня обрабатываемых сведений;
- .замена части сведений идентификаторами;
- .обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, населенного пункта, улицы, дома и квартиры, а может быть указан только город, населенный пункт)
- .деление сведений на части и обработка в разных информационных системах;
- другие способы.

13.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

13.4. Для обезличивания персональных данных годятся любые способы, не запрещенные законодательством Российской Федерации.

13.5. Сотрудники ООО «УК «АРХСИТИ ГРУПП», непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания и совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом

13.6. Директор принимает решение о необходимости обезличивания персональных данных.

14. Блокирование и уничтожение персональных данных

14.1. В случае достижения целей обработки персональных данных или в случае утраты необходимости в их достижении уполномоченное должностное лицо обязано:

- незамедлительно прекратить обработку персональных данных;
- уничтожить либо обезличить соответствующие персональные данные в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных.

Персональные данные не уничтожаются (не обезличиваются) в случаях, если:

- договором, соглашением стороной которого, выгодоприобретателем или поручителем является субъект персональных данных, предусмотрен иной порядок обработки персональных данных;
- законодательством установлены сроки обязательного архивного хранения материальных носителей персональных данных;
- в иных случаях, прямо предусмотренных законодательством.

14.2. Обезличивание или уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим

дальнейшую обработку этих персональных данных с сохранением возможности обработки иных персональных данных, зафиксированных на материальном носителе (закрашиванием, вырезанием и т.д.).

14.3. В случае выявления недостоверности персональных данных, неправомерности действий с персональными данными уполномоченное должностное лицо осуществляет немедленное блокирование указанных персональных данных и в срок, не превышающий трех рабочих дней с даты такого выявления, обязано устранить допущенные нарушения.

В случае подтверждения факта недостоверности персональных данных уполномоченное должностное лицо уточняет персональные данные и снимает с них блокирование на основании документов, представленных:
- субъектом персональных данных (его законным представителем);
- уполномоченным органом по защите прав субъектов персональных данных;
- иными лицами.

14.4. В случае невозможности устранения допущенных нарушений уполномоченное должностное лицо в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное должностное лицо уведомляет субъекта персональных данных (его законного представителя) и (или) уполномоченный орган по защите прав субъектов персональных данных.

14.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных уполномоченное должностное лицо обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва.

Об уничтожении персональных данных уполномоченное должностное лицо уведомляет субъекта персональных данных (его законного представителя).

14.6. Уничтожение документов, содержащих персональные данные, утративших свое практическое значение и не подлежащих архивному хранению производится на основании акта об уничтожении персональных данных.

Составила
Специалист по кадрам Н.И. Ляушкина

Приложение 1

ЖУРНАЛ
учета съемных носителей персональных данных

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.
на _____листах

_____ _____
(должность и ФИО ответственного за хранение) (подпись)

№ п/п	Метка съемного носителя (учетный номер)	Фамилия пользователя	(Получил, вернул)	Подпись ответственного за хранение съемного носителя	Примечание*
1					
2					
3					
4					
5					

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 2

Общество с ограниченной ответственностью «УК «АРХСИТИ ГРУПП»

УТВЕРЖДАЮ
Директор
_____ М.С. Раздобкрдин
«____» _____ 20___г.

АКТ
уничтожения съемных носителей персональных данных

Основание – приказ директора ООО «УК «АРХСИТИ ГРУПП» от «___»_____ 202__г. № ___
Комиссия, в составе:

_____

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1	2	3	4

Всего съемных носителей_____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем (разрезания, демонтажа и т.п.), измельчены и сданы для уничтожения по утилизации вторичного сырья.

Председатель комиссии Подпись Дата

Члены комиссии

Подпись Дата

Приложение 3

ЖУРНАЛ

учета обращений субъектов персональных данных

№	ФИО	Дата	Цель