

**ПОЛОЖЕНИЕ
О ПЕРСОНАЛЬНЫХ ДАННЫХ
ГК «Аталиан»**

1. Общие положения.

1.1. Настоящее Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных» от 27.07.06 № 152-ФЗ и другими нормативными правовыми актами и определяет порядок обработки и защиты персональных данных работников ГК «Аталиан» (далее – Общество).

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Обществе.

1.3. Требования настоящего Положения распространяются на всех лиц, осуществляющих обработку и защиту персональных данных работников в Обществе.

1.4. Настоящее положение определяет порядок обработки, распространения, передачи персональных данных работников Общества, других категорий лиц, а также их защиту.

2. Основные термины, сокращения и определения.

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. Под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

2.3. Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ.

Персональными данными, разрешенными субъектом персональных данных для распространения, могут являться его фамилия, имя, отчество, месяц и дата рождения, место работы, занимаемая должность, рабочие телефон и адрес электронной почты, а также иные сведения, указанные работником в Согласии на обработку персональных данных, разрешенных для распространения в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ.

Персональные данные, разрешенные субъектом персональных данных для распространения, используются в целях размещения на внутренних информационно-справочных ресурсах Общества, а также для иных целей, указанных работником в Согласии на обработку персональных данных, разрешенных для распространения.

2.4. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

2.5. Под обработкой персональных данных работника понимается 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.

2.6. Распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц.

2.7. Предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц.

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

2.9. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников.

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

2.11. Документами, содержащими персональные данные работников, являются:

- комплексы документов, сопровождающих 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, трудовые книжки, сведения о трудовой деятельности работников (СТД-Р);
- дела, содержащие материалы аттестаций работников;
- дела, содержащие материалы внутренних расследований;
- справочно-информационный банк данных по персоналу (картотеки, журналы);
- копии отчетов, направляемых в государственные контролирующие органы.

3. Сбор и обработка персональных данных.

3.1. Целью обработки персональных данных субъектов является соблюдение трудового законодательства РФ, законодательства РФ об охране труда и техники безопасности, законодательства РФ об охране здоровья, заключение договоров дополнительного страхования в интересах работников, заключение и исполнение трудовых договоров, стороной которых является субъект персональных данных, организация пропуска субъекта персональных данных на территорию, на которой находится оператор, зачисление заработной платы работников на банковские карты, выпуск визитных карточек, размещение контактных данных руководителей на сайте Общества и т.д.

3.2. Условием прекращения обработки персональных данных Обществом является его ликвидация, достижение целей обработки персональных данных, отзыв субъектом персональных данных согласия на обработку или истечение срока действия согласия на обработку персональных данных.

3.3. Общество является Оператором персональных работников Общества, кандидатов для приема на работу в Общество при наличии их письменного согласия, посетителей Общества с их письменного согласия, физических лиц, с которыми Общество заключает договоры на выполнение работ или оказание услуг с их письменного согласия. Исключение составляют случаи, предусмотренные законодательством Российской Федерации.

3.4. На основании договора Общество может поручать обработку персональных данных третьим лицам. Существенным условием договора об оказании услуг по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности персональных данных и безопасности персональных данных при их обработке.

3.5. Порядок получения (сбора) персональных данных:

3.5.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных настоящим Положением, и иных случаях, предусмотренных законами.

3.5.2. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Обществу. Общество обязано получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Общество обязано сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

3.5.3. Письменное согласие работника на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в Федеральном законе от 27.07.2006 N 152-ФЗ.

3.5.4. Письменное согласие на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального закона от 27.07.2006 N 152-ФЗ и включаются сведения, предусмотренные Федеральным законом от 27.07.2006 N 152-ФЗ. Требования к содержанию такого согласия устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

3.5.5. Письменное согласие на обработку персональных данных, разрешенных для распространения, субъект предоставляет Обществу лично.

3.5.6. Общество обязано не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

3.5.7. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

3.5.8. Согласие на обработку персональных данных, а также на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления Обществу требования об Отзыве согласия на обработку персональных данных.

3.6. Общество не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни, за исключением случаев, установленных действующим законодательством. Общество не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

3.7. Общество должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, перечень персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение. Общество проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами. Представление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

3.8. Субъект персональных данных предоставляет сотруднику Общества, уполномоченному вести обработку персональных данных, достоверные сведения о себе.

3.9. На основании полученной информации ответственный сотрудник Общества осуществляет регистрацию субъекта персональных данных в информационной системе Общества после получения письменного согласия последнего.

3.10. Персональные данные работников Общества обрабатываются в следующих структурных подразделениях и следующими лицами:

3.10.1. Отделение построения.

3.10.2. Юридическая служба - сведения, необходимые для оформления документов Общества, в том числе нотариальных.

3.10.3. Финансовое отделение - сведения, используемые при проведении расчетов с работниками.

3.10.4. Офис-менеджер, секретарь, помощник генерального директора – сведения, используемые для оформления загранпаспортов работникам, авиа/ ж/д- билетов и иных документов Общества.

3.10.5. Руководители структурных подразделений Общества - сведения в полном объеме в отношении персональных данных работников, числящихся в соответствующих структурных подразделениях Общества.

3.11. Указанные в пункте 3.10 настоящего Положения подразделения осуществляют обработку, включая сбор, накопление, хранение, систематизацию, уточнение и передачу персональных данных работников в объемах и целях, предусмотренных законодательством Российской Федерации и локальными нормативными актами Общества, а также обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

3.12. При необходимости допускается обработка персональных данных в других подразделениях Общества при условии их обработки лицами, допущенными к работе с персональными данными, и с соблюдением требований настоящего Положения.

3.13. Общество обязуется прекратить сбор персональных данных в случае увольнения субъекта персональных данных.

3.14. При определении объема и содержания обрабатываемых персональных данных работника Общество руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

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

3.14.2. Защита персональных данных работника от неправомерного их использования, утраты обеспечивается Обществом за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

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

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

4. Передача и хранение персональных данных.

4.1. При передаче персональных данных ответственные работники Общества должны соблюдать следующие требования:

4.1.1. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

4.1.2. Запрещена обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем.

4.1.3. Осуществлять передачу персональных данных субъектов в пределах Общества в соответствии с настоящим Положением, внутренними локальными нормативными актами и должностными инструкциями.

4.1.4. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

4.1.5. Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и внутренними локальными нормативными актами, ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.1.6. 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 Трудовым кодексом Российской Федерации и иными федеральными законами.

4.1.7. Письменно уведомлять лиц, получающих персональные данные работника (либо иных категорий лиц), о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и о необходимости обеспечения в отношении них выполнения требований Федеральных законов и иных нормативно-правовых актов Российской Федерации в области персональных данных, в том числе соблюдения режима конфиденциальности в отношении этих данных (Приложение 3).

4.1.8. Передача персональных данных работников негосударственному пенсионному фонду и страховой компании в целях выполнения в отношении работников условий коллективного договора, осуществляется в соответствии с заключенными с этими организациями договорами и соглашениями о конфиденциальности при наличии письменного согласия работников.

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

4.2. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

4.3. Персональные данные субъектов обрабатываются и хранятся в информационных системах в электронном виде (на серверах, персональных компьютерах, а также на внешних магнитных, оптических и других цифровых носителях), а также на бумажных носителях в специально оборудованных шкафах и сейфах в Обществе с ограниченным доступом.

4.4. Личные карточки Т-2 хранятся в бумажном виде в запирающихся шкафах, обеспечивающих защиту от несанкционированного доступа.

4.5. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно Положению «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ 15.09.2008 г. №687.

4.6. Срок хранения персональных данных субъекта определяется на основе соответствующих федеральных законов и внутренних локальных нормативных актов Общества.

4.7. Персональные данные, представленные работником, обрабатываются автоматизированным и без использования средств автоматизации способом. Работодатель не принимает, не снимает и не хранит копии личных документов работников. Документы, которые работник предъявляет работодателю для хранения в оригинале (справки, медицинские заключения и т.д.) хранятся в личном деле работника в течение 50 лет после расторжения трудового договора с работником.

4.8. После истечения нормативного срока хранения документов, которые содержат персональные данные работника, документы подлежат уничтожению. Для этого работодатель создает экспертную комиссию и проводит экспертизу ценности документов. В ходе проведения экспертизы комиссия отбирает дела с истекшими сроками хранения и по итогам отбора составляет акт о выделении к уничтожению дел, не подлежащих хранению, после чего документы измельчаются в шредере. Персональные данные работников в электронном виде стираются с информационных носителей, либо физически уничтожаются сами носители, на которых хранится информация.

5. Доступ к персональным данным.

5.1. Право доступа к персональным данным субъектов имеют сотрудники Общества, входящие в перечень лиц, осуществляющих обработку персональных данных работников Общества (п. 3.10 Положения).

5.2. Работники Общества, получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).

5.3. К числу массовых потребителей персональных данных вне Общества относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, республиканских и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

5.4. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

5.5. Субъект может получить доступ к своим персональным данным на основании письменного запроса или при обращении, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

5.6. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в трудовых отношениях с оператором (номер трудового договора и дата его заключения, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.7. Обращение субъекта или поступивший запрос рассматривается должностным лицом Общества, ответственным за обеспечение безопасности персональных данных.

5.8. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ответственный за обеспечение безопасности персональных данных в информационной системе готовит в письменной форме мотивированный ответ, содержащий ссылку на положение федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

5.9. Общество предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

5.10. В срок не более семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Общество вносит в них необходимые изменения. С этой целью ответственный за обеспечение безопасности персональных данных дает поручение должностному лицу Общества, входящему в Перечень лиц, осуществляющих обработку персональных данных, внести изменения в персональные данные субъекта.

5.11. В срок, не более семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Общество уничтожает такие персональные данные и уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах.

5.12. Общество сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

5.13. Лица, допущенные к работе с персональными данными, обязаны:

5.13.1 знать законодательство Российской Федерации и локальные нормативные акты Общества по защите персональных данных;

5.13.2 обеспечивать сохранность закреплённого массива носителей с персональными данными, исключать возможность ознакомления с ними других лиц;

5.13.3 докладывать своему непосредственному руководителю и сотрудникам по режиму и защите информации Общества обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

6. Права оператора персональных данных.

6.1. Общество вправе:

6.1.1. Отстаивать свои интересы в суде.

6.1.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

6.1.3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом.

6.1.4. Использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законом.

6.1.5. Осуществлять внутренний контроль за соблюдением настоящего Положения согласно должностному регламенту специалиста по обеспечению безопасности персональных данных.

6.1.6. Проводить расследование инцидентов безопасности персональных данных.

7. Права работника в целях обеспечения защиты его персональных данных.

7.1. Работник имеет право:

7.1.1. На полную информацию о своих персональных данных и обработке этих данных.

7.1.2. На свободный бесплатный доступ к этим данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом. Доступ предоставляется при непосредственном обращении работника или по его письменному запросу;

7.1.3. На требование об исключении или исправлении неверных, или неполных персональных данных, обработанных с нарушением Трудового кодекса РФ и настоящего Положения.

7.1.4. На требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, о всех произведенных в них исключениях, исправлениях или дополнениях.

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

7.1.6. На обжалование в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных, а также иные права, предусмотренные законодательством.

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

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут персональную дисциплинарную, административную, гражданско-правовую или уголовную ответственность, согласно действующему законодательству Российской Федерации за разглашение персональных данных работников ООО «Новый дом» без их согласия.

8.2. Работники Общества, осуществляющие обработку персональных данных, обязаны подписать соглашение о неразглашении персональных данных.

9. Защита персональных данных

9.1. Работодатель определяет тип угроз безопасности и уровень защищенности персональных данных, которые хранятся в информационных системах, и предпринимает меры по защите информации.

Угрозы защищенности персональных данных

Угрозы 1-го типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

Угрозы 2-го типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

Угрозы 3-го типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

Уровни защищенности персональных данных

1-й уровень защищенности. Если работодатель отнес информационную систему к 1-му типу угрозы или если тип угрозы 2-й, но работодатель обрабатывает специальные категории персональных данных более 100 тысяч физических лиц без учета работников.

2-й уровень защищенности. Если тип угрозы 2-й и работодатель обрабатывает специальные категории персональных данных работников вне зависимости от их количества или специальные категории персональных данных менее чем 100 тысяч физических лиц или любые другие категории персональных данных более чем 100 тысяч физических лиц или при 3-м типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тысяч физических лиц.

3-й уровень защищенности. Если при 2-м типе угрозы работодатель обрабатывает общие персональные данные работников или менее чем 100 тысяч физических лиц или при 3-м типе угрозы работодатель обрабатывает специальные категории персональных данных работников или менее чем 100 тысяч физических лиц или при 3-м типе угрозы работодатель обрабатывает биометрические персональные данные или при 3-м типе угрозы работодатель обрабатывает общие персональные данные более чем 100 тысяч физических лиц.

4-й уровень защищенности. Если при 3-м типе угрозы работодатель обрабатывает только общие персональные данные работников или менее чем 100 тысяч физических лиц.

9.2. При 4-м уровне защищенности персональных данных работодатель:

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

9.3. При 3-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пункте 9.2 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности персональных данных в информационной системе.

9.4. При 2-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пунктах 9.2, 9.3 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

9.5. При 1-м уровне защищенности персональных данных, дополнительно к мерам, перечисленным в пунктах 9.2—9.4 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к персональным данным в системе;
- создает отдел, ответственный за безопасность персональных данных в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

9.6. В целях защиты персональных данных на бумажных носителях работодатель:

- приказом назначает ответственного за обработку персональных данных;
- ограничивает доступ в помещения, где хранятся документы, которые содержат персональные данные работников;
- хранит документы, содержащие персональные данные работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

9.7. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.

9.8. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к персональным данным работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников не допускаются.

9.9. Допуск к документам, содержащим персональные данные работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.

9.10. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

9.11. Передача информации, содержащей сведения о персональных данных работников, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.