

## ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Сочи

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным лиц, состоящих в трудовых, договорных и иных гражданско-правовых отношениях с ИП Хамалян Э.О. (далее по тексту - Работодатель).

1.2. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты, а также обеспечение защиты прав Работника при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, Федерального закона «Об информации, информатизации и защите информации», Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Настоящее Положение утверждается и вводится в действие приказом Генерального директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

### 2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под персональными данными работников понимается информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;

- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- результаты медицинских обследований;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

### 3. ПРАВА И ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

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

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

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

3.1.3. Все персональные данные работника следует получать у него самого. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.1.4. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.1.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

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

3.1.7. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

### 4. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

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

4.2. Работник должен быть ознакомлен под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

4.3. В целях защиты персональных данных, хранящихся у Работодателя, Работник имеет право:

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных федеральным законом, трудовым законодательством.
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса или иного федерального закона.
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны;
- требовать об извещении Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в суде любые неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных.

4.4. Работник обязан передавать Работодателю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

4.5. В случае предоставления заведомо подложных данных при заключении Трудового договора о своей трудовой деятельности, профессиональной подготовке, образовании, состоянии здоровья, о праве занимать определенные должности или заниматься определенной деятельностью по приговору суда Работодатель имеет право в одностороннем порядке расторгнуть Трудовой договор с этим Работником.

4.6. Работник обязан в течение десяти дней после изменения фамилии, имени, отчества, даты рождения, образовании и других изменениях поставить Работодателя в известность с целью внесения новых данных в учетную документацию.

4.7. В целях защиты частной жизни, личной и семейной тайны Работник не должен отказываться от своего права на обработку персональных данных только с его согласия, поскольку это может повлечь причинение морального, материального вреда.

## 5. СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Обработка персональных данных Работника - это получение, хранение, комбинирование, передача или любое другое использование персональных данных Работника.

5.2. Работник предоставляет Работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами. Предоставление работником подложных документов или ложных сведений при поступлении на работу является основанием для расторжения трудового договора.

5.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.4. При поступлении на работу работник заполняет Анкету работодателя.

5.5. Анкета представляет собой перечень вопросов о персональных данных работника.

5.6. Анкета заполняется работником собственноручно. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений

или зачеркиваний, прочерков, помарок в строгом соответствии с записями, которые содержатся в его личных документах.

5.7. Все персональные данные работника следует получить у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение (ст. 86 ТК РФ п. 3.)

5.8. Анкета работника храниться у работодателя. К анкете прилагается фотография работника размером 3x4.

5.9. Работодатель имеет право снять ксерокопии с предоставляемых работником документов в целях проверки их подлинности и достоверности данных в Анкете.

5.10. Анкета и копии документов хранится у работодателя в течение всей трудовой деятельности работника.

## 6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

6.2. К обработке, передаче и хранению персональных данных работника могут иметь доступ:

- сотрудники отдела безопасности;
- сотрудники отдела персонала;
- сотрудники бухгалтерии;
- сотрудники IT отдела.

6.3. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

6.4. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

6.5. Передача персональных данных Работника возможна только с согласия Работника или в случаях, прямо предусмотренных трудовым законодательством, федеральными законами.

6.6. При передаче персональных данных Работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные Работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные Работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными Работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным Работника только специально уполномоченным лицам, определенным приказом генерального директора, при этом указанные лица должны иметь право получать только те персональные данные Работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.

6.7. При передаче персональных данных Работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника или в случаях, установленных федеральным законом.

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

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

6.10. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

6.11. При принятии решений, затрагивающих интересы Работника, Работодатель не имеет права основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

## 7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Внутренний доступ (доступ внутри организации).

7.1.1. Право доступа к персональным данным сотрудника имеют:

- Генеральный директор организации;
- Заместитель генерального директора по безопасности;
- Главный бухгалтер;
- Бухгалтер по расчетам с персоналом;
- Руководитель отдела персонала;
- Ведущий менеджер по персоналу;
- Менеджер по персоналу;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных;
- сотрудники организации указанные в п.6.2.

7.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом Генерального директора организации.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне организации относятся государственные и негосударственные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;

- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

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

7.2.3. Другие организации.

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

7.2.5. Персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника.

7.2.6. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы Работника без его согласия. (УК РФ).

## 8. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Уничтожение персональных данных производится в случаях:

- 1) выявление неправомерной обработки персональных данных, в том числе по обращению субъекта персональных данных или его представителя либо запросу уполномоченного органа по защите прав субъектов персональных данных, если обеспечить правомерность обработки персональных данных невозможно;
- 2) требования субъекта персональных данных, если его персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- 3) отзыва субъектом персональных данных согласия на обработку его персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных;
- 4) достижения цели обработки персональных данных или утраты необходимости в достижении этих целей;
- 5) истечения сроков хранения персональных данных, установленных нормативно-правовыми актами Российской Федерации;
- 6) признания недостоверности персональных данных или получения их незаконным путем по требованию уполномоченного органа по защите прав субъектов персональных данных;
- 7) в иных установленных законодательством случаях.

8.2. Для выявления случаев, указанных в п. 8.1, в организации назначается ответственное лицо (либо создается специальное подразделение), которое отслеживает работу с персональными данными, выявляет случаи, когда необходимо уничтожить данные, обрабатывает запросы от сотрудников организации, государственных органов и субъектов персональных данных по поводу уничтожения персональных данных.

8.3. В случае необходимости уничтожения персональных данных ответственное лицо, указанное в п. 8.2 настоящего Положения, в течение 10 (Десяти) дней с момента возникновения запроса об уничтожении персональных данных обращается в комиссию по защите персональных данных, созываемую в количестве 3 (Трех) человек, для принятия решения об уничтожении персональных данных.

8.4. Комиссия в течение 3 (Трех) дней с момента получения обращения проверяет обоснованность необходимости уничтожения персональных данных и выносит соответствующее решение.

8.5. Решение комиссии об отказе в уничтожении персональных данных может быть обжаловано в судебном порядке в соответствии с действующим законодательством Российской Федерации.

8.6. Решение комиссии об уничтожении персональных данных должно быть исполнено в течение с момента получения лицом, указанным в п. 8.2 настоящего Положения.

8.7. Комиссия по уничтожению персональных данных создается на основании приказа руководителя организации и состоит из трех человек:

- Председателя комиссии – Индивидуальный Предприниматель ,

а также двух членов комиссии:

- Управляющего;

Администратора

---

8.8. Инструктаж членов комиссии по уничтожению персональных данных проводит Председатель комиссии.

8.9. В случае увольнения какого-либо члена комиссии назначается новый член комиссии, путем подписания соответствующего приказа. Инструктаж нового члена комиссии проводит Председатель комиссии.

8.10. Уничтожение персональных данных может быть осуществлено двумя способами в зависимости от типа носителя информации (бумажный или электронный):

- физическое уничтожение носителя (уничтожение через shredding (уничтожение с помощью shredder), сжигание);

- уничтожение информации с носителя (многократная перезапись в секторах магнитного диска).

8.11. Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

8.12. Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

8.13. Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правиль-

ность и полноту уничтожения перечисленных в Акте об уничтожении персональных данных (Приложение № 1 к настоящему Положению).

8.14. Уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

8.15. После уничтожения персональных данных составляется Акт об уничтожении персональных данных (далее - Акт), по форме, утвержденной руководителем организации (Приложение № 1 к настоящему Положению).

Акт подписывается всеми членами комиссии.

8.16. Лицо, указанное в п. 8.2 настоящего Положения, уведомляет лицо, обратившееся с запросом об уничтожении персональных данных, об уничтожении персональных данных в течение 10 (Десять) дней с момента составления Акта об уничтожении персональных данных.

## 9. СРОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Персональные данные хранятся в течение следующих сроков:

- Договоры гражданско-правового характера о выполнении работ, оказании услуг физическими лицами, акты сдачи-приемки выполненных работ, оказанных услуг - 75 лет;
- Трудовые договоры, служебные контракты, соглашения об их изменении, расторжении – 75 лет;
- Документы (заявления, анкеты, справки, копии документов, удостоверяющих личность, копии документов о трудовой деятельности, квалификации, образовании) претендентов на замещение вакантной должности, не допущенных к участию в конкурсе и не прошедших конкурсный отбор - 3 года;
- Документы (заявления, анкеты, справки, копии документов, удостоверяющих личность, копии документов о трудовой деятельности, квалификации, образовании) лиц, не принятых на работу – 1 год;
- Документы (списки, представления, характеристики, анкеты, резюме) по формированию кадрового резерва организации – 5 лет;
- Личные карточки работников - 75 лет;
- Личные дела руководителей и работников организаций – 75 лет;
- Подлинные личные документы (трудовая книжка, дипломы, аттестаты, удостоверения, свидетельства) – до востребования. Не востребованные работниками – 75 лет;
- Приказы, распоряжения по личному составу; документы (докладные записки, справки, заявления) к ним:
  - о приеме, переводе, перемещении, ротации, совмещении, совместительстве, увольнении, оплате труда, аттестации, повышении квалификации, присвоении классных чинов, разрядов, званий, поощрении, награждении, об изменении анкетно-биографических данных, отпусках по уходу за ребенком, отпусках без сохранения заработной платы – 75 лет;
  - о ежегодно оплачиваемых отпусках, отпусках в связи с обучением, дежурствах, не связанных с основной (профильной) деятельностью – 5 лет;
  - о служебных проверках – 5 лет;
  - о направлении в командировку работников - 5 лет;
  - о дисциплинарных взысканиях – 3 года.
- Персональные данные гостей – 1 год;

- Персональные данные посетителей, клиентов, контрагентов – 30 дней.

## 10. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Защита персональных данных Работника от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом, трудовым законодательством.

10.2. В целях обеспечения сохранности и конфиденциальности персональных данных работников все операции по оформлению, формированию, ведению и хранению данной информации выполняются только сотрудниками отдела персонала, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

10.3. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке организации и в том объеме, который позволяет не разглашать излишний объем персональных сведений о Работнике.

10.4. Передача информации, содержащей сведения о персональных данных работников по телефону, факсу, электронной почте без письменного согласия Работника запрещается.

10.5. Сведения по личному составу, содержащие персональные данные работников, хранятся в запирающихся шкафах (сейфах) отдела персонала, обеспечивающих защиту от несанкционированного доступа.

10.6. Персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

10.7. Внутренняя защита.

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

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- не допускается выдача личных дел сотрудников на рабочие места руководителей.

10.7.2. Личные дела могут выдаваться на рабочие места только Генеральному директору, Заместителю генерального директора по безопасности и в исключительных случаях, по письменному разрешению Генерального директора, руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

10.7.3. Защита персональных данных сотрудника на электронных носителях:

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю отдела персонала и руководителю службы информационных технологий.

10.8. Внешняя защита.

10.8.1. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур.

10.8.2. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

10.8.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи магнитных карт;
- технические средства охраны;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

10.9. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

10.10. Персональные данные, предоставляемые для статистических или иных научных целей должны быть обезличены. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

## 11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ.

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

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

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

11.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

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

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

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

СОГЛАСОВАНО:

Приложение № 1  
к Положению об обработке и защите  
персональных данных  
№ 1 утвержденного 01.06.2026г.

**АКТ**  
**об уничтожении персональных данных (форма)**

г. Сочи

«\_\_» \_\_\_\_\_ 20\_\_ г.

Комиссия, созданная на основании Приказа № 1 от «\_\_» \_\_\_\_\_ 202\_ г., в составе Председателя комиссии – Индивидуального предпринимателя Хамалян Э.О. членов комиссии: Управляющего Самариной М.С. Администратора Минасян М.М, составила настоящий Акт об уничтожении персональных данных субъектов персональных данных (гостей), обрабатываемых гостиницей Парадиз находящемуся по адресу: Г. Сочи, ул. Бестужева, д 1Б. , в течение 2025 года.

№ п/п	Перечень категорий уничтоженных персональных данных	Вид носителя персональных данных	Дата уничтожения	Способ уничтожения	Причина уничтожения
1	Согласно Приложению № 1 к настоящему Акту	Бумажный		Уничтожение с помощью shreddera	Достижение цели обработки персональных данных

Акт подлежит хранению до 01.01. 2031г.

Приложение № 1: Персональные данные: Ф.И.О., дата рождения, серия и номер документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе – 15000листов.