

УТВЕРЖДАЮ

Директор ООО «Туристский центр Радуга»

 Дрогаева Л.А.



30 ноября 2025 года

Положение о защите персональных данных сотрудников

1. Общие положения

Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников ООО «Туристский центр Радуга». Под сотрудниками подразумеваются лица, имеющие трудовые отношения с ООО «Туристский центр Радуга».

1.1. Цель

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

1.2. Основания

Основанием для разработки данного Положения являются:

- Конституция РФ от 12.12.1993;
- Трудовой кодекс РФ № 197 – ФЗ от 01.02.2002;
- Кодекс РФ об административных правонарушениях № 195 – ФЗ от 30.12.2001 г.;
- Указ Президента РФ № 188 от 06.09.1997 «Об утверждении перечня сведений конфиденциального характера».
- ФЗ № 152 от 27/07/2006 «О персональных данных»

1.3. Порядок ввода в действие Положения о защите персональных данных и изменений к нему

Положение о защите персональных данных и изменения к нему вводятся приказом по фирме и утверждаются директором. Все сотрудники организации должны быть ознакомлены под расписку с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных

Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным относятся:

- образование;
- специальность;
- занимаемая должность;

- адрес местожительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- размер заработной платы;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т-2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным сотрудника.

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

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. Цель, перечень, способ, сроки обработки персональных данных

Целью обработки персональных данных сотрудника является организация учета сотрудников ООО «Туристский центр Радуга» для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными

законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных».

Перечень обработки персональных данных: фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, семейное положение, доходы, пол, адрес электронной почты, адрес места жительства, адрес регистрации, номер телефона, СНИЛС, ИНН, гражданство, данные документа, удостоверяющего личность, данные документа, содержащиеся в свидетельстве о рождении, реквизиты банковской карты, номер расчетного счета, номер лицевого счета, профессия, должность, сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации), отношение к воинской обязанности, сведения о воинском учете, сведения об образовании.

Способ обработки персональных данных: смешанный, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

Перечень действий с персональными данными: распространение, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Срок обработки ПДн: срок действия трудового договора, срок хранения ПДн: 50 лет.

4. Порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований

Уничтожение персональных данных осуществляет комиссия, утверждённая приказом №1А от 01.01.2022 «О создании комиссии по уничтожению персональных данных».

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение носителей);
- 3) передача на специализированные полигоны (свалки).

При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Общества должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, работники структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях) или путем механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была невозможна.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

5. Принципы обработки персональных данных

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

Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника 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 сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

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

Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

При принятии решений относительно сотрудника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

Пакет анкетно-биографических и характеризующих материалов (далее пакет) сотрудника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу.

Все документы хранятся в папках в алфавитном порядке фамилий сотрудников.

Пакет пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

При обработке персональных данных сотрудников работодатель в лице директора вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников на базе современных информационных технологий.

Сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

Сотрудник имеет право:

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

6. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри фирмы исключительно для обработки и использования в работе.

Внешний доступ. К числу массовых потребителей персональных данных вне ООО «Туристский центр Радуга» можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

Внутренний доступ. Внутри ООО «Северная» к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- начальник отдела кадров;
- сотрудники бухгалтерии;
- начальники структурных подразделений.

В кадровом отделе хранятся личные карточки сотрудников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке.

После увольнения документы по личному составу передаются на хранение.

7. Передача персональных данных

При передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

Передача внешнему потребителю:

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- при передаче персональных данных сотрудника потребителям (в том числе и в коммерческих целях) за пределы ООО «Туристский центр Радуга» работодатель не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника или в случаях, установленных федеральным законом;
- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;
- по возможности персональные данные обезличиваются.

Передача внутреннему потребителю. Работодатель вправе разрешать доступ к персональным данным сотрудников. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников (Приложение №1).

8. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете,

обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности предприятия.

8.1. «Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами предприятия. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения;
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

8.2. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности предприятия, посетители, сотрудники других организационных структур.

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

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим предприятия;
- порядок охраны территории, зданий, помещений, транспортных средств.

9. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

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

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

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

к Положению об обработке и защите

персональных данных работников

ООО «Туристский центр Радуга»

от «30» ноября 2025 г.

**Обязательство о неразглашении персональных данных сотрудников
ООО «Туристский центр Радуга»**

Я, _____, проживающий(-ая)
Ф.И.О.

по адресу, _____
паспорт серии _____

«__» _____ года работая в должности _____

, в период настоящих трудовых отношений и в течение 5 лет после их окончания, в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», обязуюсь:

1) не раскрывать третьим лицам и не распространять персональные данные сотрудников ООО «Туристский центр Радуга», полученные при исполнении мной трудовых обязанностей;

2) при работе с персональными данными соблюдать требования, описанные в «Положении об обработке и защите персональных данных работников ООО «Туристский центр Радуга»;

3) выполнять относящиеся ко мне требования локальных нормативных актов, касающихся обработки персональных данных;

4) в случае попытки посторонних лиц получить от меня персональные данные работников ООО «Туристский центр Радуга», сведения о порядке обработки и защиты персональных данных немедленно уведомить об этом руководителя своего структурного подразделения;

5) в случае расторжения со мною трудового договора или контракта, прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, и передать все носители персональных данных работников ООО «Туристский центр Радуга» (документы, накопители данных в электронном виде, кино и фотонегативы и позитивы, и пр.), ответственному за организацию обработки персональных данных работников ООО «Туристский центр Радуга».

Я понимаю, что разглашение персональных данных работников ООО «Туристский центр Радуга», может нанести ущерб работникам ООО «Туристский центр Радуга».

Я предупрежден(а) о том, что в случае разглашения или утраты мною сведений, относящихся к персональным данным работников ООО «Туристский центр Радуга», я несу ответственность в соответствии со статьей 90 Трудового Кодекса РФ и могу быть привлечён к дисциплинарной, материальной, гражданско-правовой, административной и

уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

Настоящим подтверждаю, что с «Положении об обработке и защите персональных данных работников ООО «Туристский центр Радуга» ознакомлен(а).

«__» _____ 20__ года

(подпись)

(инициалы, фамилия)

