# ПОЛОЖЕНИЕ
# о защите, хранении, обработке и передаче персональных данных в Обществе с ограниченной ответственностью "Ювеста"

Настоящее Положение разработано на основании Конституции Российской Федерации, Трудового кодекса РФ, Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

## Термины и определения

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые Компанией в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Клиент** – лицо, являющееся потребителем услуг либо потенциальным потребителем услуг Компании.

**Компания** – Общество с ограниченной ответственностью "Ювеста"

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** - обязательное для соблюдения Компанией или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – 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.

**Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

**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.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** – 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.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

**Субъект** – Работник или Клиент Компании, чьи персональные данные обрабатываются Компанией.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Работник** – лицо, состоящее с Компанией в трудовых отношениях.

**Трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

## 1. Общие положения

1.1. Настоящее положение применяется к защите персональных данных Субъекта. Целью настоящего Положения является обеспечение защиты прав человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. К персональным данным относятся:

- сведения, содержащиеся в удостоверении личности;

- информация, содержащаяся в трудовой книжке Работника;

- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;

- документы воинского учета - при их наличии;

- информация об образовании, квалификации или наличии специальных знаний или подготовки;

- информация медицинского характера (в отношении Работников, в случаях, предусмотренных законодательством);

- иные документы, содержащие сведения, необходимые для определения трудовых отношений;

- информация о размере заработной платы Работника;

- фамилия, имя, отчество Клиента;

- дата рождения Клиента;

- информация месте жительства Клиента, номер контактного телефона;

- паспортные данные Клиента, необходимые для оформления перевозочных документов.

1.3. Объектами защиты являются – информация, обрабатываемая в информационной системе персональных данных, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в информационной системе персональных данных.

1.4. Объекты защиты включают:

1) Обрабатываемая информация.

2) Технологическая информация.

3) Программно-технические средства обработки.

4) Средства защиты персональных данных.

5) Каналы информационного обмена и телекоммуникации.

6) Объекты и помещения, в которых размещены компоненты ИСПДн.

1.5. Все персональные сведения о Субъекте Компания может получить только от него самого. В случаях, когда Компания может получить необходимые персональные данные Субъекта только у третьего лица, Компания должна уведомить об этом Субъекта и получить от него письменное согласие.

1.6. Компания обязана сообщить Субъекту о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа Субъекта дать письменное согласие на их получение.

1.7. Персональные данные Субъекта являются конфиденциальной информацией и не могут быть использованы Компанией, или любым иным лицом в личных целях.

1.8. При определении объема и содержания персональных данных Субъекта, Компания руководствуется настоящим Положением, Трудовым кодексом РФ, Гражданским кодексом РФ, иными федеральными законами и Конституцией РФ.

1.9. Субъект не должен отказываться от своих прав на сохранение и защиту тайны.

1.10. Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

1.11. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование,

копирование, распространение персональных данных, а также иных несанкционированных действий.

1.12. Структура, состав и основные функции системы защиты персональных данных определяются исходя из класса информационной системы персональных данных. Система защиты персональных данных включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

**конфиденциальность** информации (защита от несанкционированного ознакомления);

**целостность** информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

**доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

## 2. Задачи системы защиты персональных данных

2.1. Основной целью системы защиты персональных данных является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

2.2. Для достижения основной цели система безопасности персональных данных информационной системы персональных данных должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования информационной системы персональных данных посторонних лиц (возможность использования автоматизированной системы и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационной системы персональных данных (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационной системы персональных данных для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

1) к информации, циркулирующей в информационной системе персональных данных;

2) средствам вычислительной техники информационной системы персональных данных;

3) аппаратным, программным и криптографическим средствам защиты, используемым в информационной системе персональных данных;

- регистрацию действий пользователей при использовании защищаемых ресурсов информационной системы персональных данных в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в информационной системе персональных данных программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту информационной системы персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- защиту информационной системы персональных данных, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз безопасности информационной системы персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

## 3. Хранение, обработка и передача персональных данных Субъекта

3.1. Обработка персональных данных должна осуществляться на основе принципов:

1) законности способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Обработка персональных данных Субъекта осуществляется для обеспечения соблюдения законов и иных нормативно-правовых актов в **целях**:

- содействия Работнику в трудоустройстве, обучении и продвижении по службе;

- обеспечения личной безопасности Работника;

- контроля качества и количества выполняемой работы;

- оплаты труда;

- обеспечения сохранности имущества;

- пользования льготами, предусмотренными законодательством РФ и актами Компании;

- надлежащего оказания услуг Компанией Клиенту по договору оказания услуг;

- защита Работников и Клиентов, их прав и интересов, имущества от неблагоприятных воздействий;

- оказания услуг Клиентам по оформлению и бронированию авиа и железнодорожных перевозок, такси, размещения в отелях;

- поддержания обратной связи с Субъектом.

3.3. Обработка персональных данных субъектов осуществляется Компанией как в виде автоматизированной обработки персональных данных (оформление, бронирование, продажа перевозочных документов на сайте https://pechkin56.ru/), так и неавтоматизированной обработки персональных данных (оформление, бронирование, продажа перевозочных документов кассирами билетными по месту нахождению Компании, обработка персональных данных уполномоченными сотрудниками Компании).

3.4. Персональные данные Работника хранятся у сотрудника, на которого возложены обязанности кадрового делопроизводства:

- в сейфе на бумажных носителях хранится трудовая книжка;

- личная карточка хранится в шкафу, запираемом на ключ;

- на электронных носителях с ограниченным доступом.

3.5. Право доступа к персональным данным Работника имеют:

- генеральный директор Компании;

- главный бухгалтер Компании;

- начальник отдела бухгалтерского учета и финансового анализа;

- программист 1С;

- юрисконсульт Компании;

- помощник Генерального директора.

3.6. Сотрудник на которого возложены обязанности ведения кадрового делопроизводства вправе передавать:

- информацию об образовании, квалификации или наличии специальных знаний или подготовки;

- информацию о размере заработной платы Работника руководителю подразделения, в котором работает Работник.

3.7. Генеральный директор Компании, главный бухгалтер Компании и системный администратор компьютерной сети Компании может передавать персональные данные Работника третьим лицам только если это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных законодательством.

3.8. При передаче персональных данных Работника, сотрудник, на которого возложены обязанности ведения кадрового делопроизводства, Генеральный директор Компании, главный бухгалтер Компании и системный администратор компьютерной сети Компании предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

3.9. Все сведения о передаче персональных данных Работника учитываются для контроля правомерности использования данной информации лицами, ее получившими.

3.10. Сотрудник на которого возложены обязанности ведения кадрового делопроизводства обязан предоставлять персональную информацию в пенсионный фонд по форме, в порядке и объеме, установленном законодательством РФ.

3.11. Иные права, обязанности, действия Работников, в трудовые обязанности которых входит обработка персональных данных Работника, определяются должностными инструкциями.

3.12. Персональные данные Клиентов Компании хранятся в электронном виде на удаленном сервере ЗАО «Сирена-Трэвел», за сохранность которого отвечают сотрудники ЗАО «Сирена-Трэвел», на сервере Компании, за сохранность которого отвечает программист 1С Компании.

Контактные данные клиентов Компании на бумажных носителях хранятся в сейфе Компании, у сотрудника, на которого возложены обязанности кадрового делопроизводства.

Копии маршрутных квитанций с персональными данными Клиентов хранятся в архиве Компании. Ответственным за хранение маршрутных квитанций с персональными данными Клиентов является главный бухгалтер Компании.

3.13. Персональные данные Клиентов Компании, хранятся на сервере Компании не более 5 лет, после чего уничтожаются путем форматирования соответствующего сектора данных.

Копии маршрутных квитанций с персональными данными Клиентов хранятся в архиве Компании не более 5 лет, после чего уничтожаются методом шредирования.

3.14. Компания может передавать персональные данные Клиента третьим лицам только если это необходимо в целях оказания услуг Клиентам по оформлению и бронированию авиа и железнодорожных перевозок, такси, размещения в отелях, а также в случаях, установленных законодательством.

3.15. Право доступа к персональным данным Клиента, являющегося получателем услуг Компании имеет:

- Генеральный директор Компании;

- главный бухгалтер Компании;

- кассир билетный Компании;

- юрисконсульт Компании;

- сотрудники отдела учета выручки Компании;

- программист 1С Компании.

3.16. Генеральный директор Компании вправе передавать бланки с персональными данными Клиента главному бухгалтеру Компании для организации налоговой отчетности.

3.17. При передаче персональных данных Клиента сотрудники Компании предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

3.18. Иные права, обязанности, действия Работников, в трудовые обязанности которых входит обработка персональных данных Клиента, определяются должностными инструкциями.

3.19. Все сведения о передаче персональных данных Клиента учитываются для контроля правомерности использования данной информации лицами, ее получившими.

## 4. Обязанности Компании по хранению и защите персональных данных Субъекта

4.1. Компания обязана за свой счет обеспечить защиту персональных данных Субъекта от неправомерного их использования или утраты, в порядке, установленном законодательством РФ.

4.2. Компания обязана ознакомить Субъекта и его представителей с настоящим Положением и их правами в области защиты персональных данных.

4.3. Компания обязана осуществлять передачу персональных данных Субъекта только в соответствии с настоящим Положением и законодательством РФ.

4.4. Компания обязана предоставлять персональные данные Субъекта только уполномоченным лицам, и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим Положением и законодательством РФ.

4.5. Компания не вправе получать и обрабатывать персональные данные Субъекта о его политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, Компания вправе получать и обрабатывать персональные данные Субъекта о его личной жизни, только с письменного согласия Субъекта.

4.6. Компания не имеет права получать и обрабатывать персональные данные Субъекта о его членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

4.7. Компания не вправе предоставлять персональные данные Субъекта в коммерческих целях, без письменного согласия Субъекта.

4.8. Компания обязана обеспечить Субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством.

4.9. Компания обязана по требованию Субъекта предоставить ему полную информацию о его персональных данных и обработке этих данных.

## 5. Права Субъекта на защиту его персональных данных

5.1. Субъект в целях обеспечения защиты своих персональных данных, хранящихся у Компании, имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

## 6. Ответственность Компании и ее сотрудников

6.1. Защита прав Субъекта, установленных настоящим Положением и законодательством РФ, осуществляется судом, в целях пресечения неправомерного использования персональных данных Субъекта, восстановления нарушенных прав и возмещения причиненного ущерба, в том числе морального ущерба.

6.2. В случае нарушения норм, регулирующих обработку, хранение, передачу и защиту персональных данных Субъекта Компанией и иными лицами, они несут ответственность в соответствии с действующим законодательством.