

## **Положение об обработке и защите персональных данных клиентов в ООО «СевСтар ИТ»**

### **1 Назначение**

Данное Положение об обработке и защите персональных данных клиентов в ООО «СевСтар ИТ» (далее - Положение) определяет порядок и условия обработки персональных данных клиентов (далее - ПДн) как с использованием, так и без использования средств автоматизации.

Данное Положение разработано с целью обеспечения защиты ПДн ООО «СевСтар ИТ» в соответствии с требованиями действующего законодательства Российской Федерации.

### **2 Общие положения**

#### **2.1 Область применения**

Требования данного Положения распространяются на ответственных лиц - сотрудников ООО «СевСтар ИТ».

В сфере действия данного Положения находятся все информационные системы ПДн Оператора, в частности:

- Корпоративная информационная система (далее - КИС) ПДн Оператора.
- Другие информационные системы, попадающие под действие Федерального закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ и подзаконных актов.

Ответственным за организацию обработки ПДн является подразделение, в чьи обязанности входит организация работы с клиентами и обслуживание клиентов.

Внутренний контроль и аудит соответствия обработки ПДн законодательству и внутренним нормативным документам осуществляют сотрудники соответствующих подразделений в рамках своей компетенции и функциональной области ответственности.

Данное Положение устанавливает требования по обработке ПДн в информационных системах ПДн и на бумажных носителях.

Статус данного документа для РФ - «Для руководства».

#### **2.2 Нормативные ссылки**

Настоящее Положение разработано с учетом следующих нормативных документов:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ;
- Федеральный закон Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;
- Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119;
- Постановление Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687;
- Приказ ФСТЭК РФ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21.
- Положение о конфиденциальной информации ООО «СевСтар ИТ».

#### **2.3 Термины, определения и сокращения**

Для целей данного Положения в нем используются следующие термины и сокращения:

Клиент - пользователь услугами, с которым заключен договор об оказании таких услуг.

ПДн - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (Клиенту).

Блокирование - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Доступ к информации - возможность получения информации и ее использования.

Использование ПДнк - действия (операции) с ПДнк, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении клиента или других лиц либо иным образом затрагивающих права и свободы Клиента или других лиц.

КИСПДнк – Корпоративная информационная система ПДнк, в которой производится сбор и хранение информации об клиентах и истории взаимоотношений с ними, об использовании телекоммуникационных услуг и их тарификации, о выставлении счетов Клиентам и об обработке платежей.

Конфиденциальность ПДнк - обязательное для соблюдения оператором или иным получившим доступ к ПДнк лицом требование не допускать их распространения без согласия клиента или наличия иного законного основания.

Несанкционированный доступ к информационным активам - доступ к информации, нарушающий установленные правила разграничения доступа.

Обезличивание ПДнк - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДнк конкретному Клиенту.

Обработка ПДнк - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДнк, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДнк.

Оператор - Общество с ограниченной ответственностью «СевСтар ИТ», самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПДнк, а также определяющее цели обработки ПДнк, состав ПДнк, подлежащих обработке, действия (операции), совершаемые с ПДнк.

Пользователь КИСПДнк - лицо, участвующее в функционировании КИСПДнк или использующее результаты ее функционирования.

Потенциальный клиент - физическое лицо, имеющее намерения стать клиентом.

Предоставление ПДнк - действия, направленные на раскрытие ПДнк определенному лицу или определенному кругу лиц.

Распространение ПДнк - действия, направленные на раскрытие ПДнк неопределенному кругу лиц.

Ответственное лицо Оператора - сотрудник Оператора, в функциональные обязанности которого входит обработка ПДнк.

ИО - Инженерный отдел ООО «СевСтар ИТ».

Защищенная электронная почта - дополнительный сервис, позволяющий защищать почтовые сообщения посредством шифрования и электронной подписи сертифицированными средствами криптографической защиты информации.

Уничтожение ПДнк - действия, в результате которых становится невозможным восстановить содержание ПДнк клиента в информационной системе ПДнк и (или) в результате которых уничтожаются материальные носители ПДнк.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку ПДнк клиента.

### **3 Общие требования к обработке ПДнк**

Обработку ПДнк Оператора осуществляют на основе следующих принципов:

- законность целей и способов обработки ПДнк;
- соответствие целей обработки ПДнк целям, заранее определенным и заявленным при сборе ПДнк, а также полномочиям оператора;
- соответствие объема и характера обрабатываемых ПДнк, способов обработки ПДнк целям обработки ПДнк;
- достоверность ПДнк, их достаточность для целей обработки, недопустимость обработки ПДнк, избыточных по отношению к целям, заявленным при сборе ПДнк;
- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем ПДнк;
- иных принципов, определенных действующим законодательством.

Цели сбора, обработки и правовое обоснование обработки ПДнк: Оператор собирает и хранит ПДнк, необходимые для оказания Клиенту услуг, а также

для осуществления и исполнения возложенных на Оператора законодательством Российской Федерации функций, полномочий и обязанностей на основании и в соответствии со ст.ст. 23, 24 Конституции Российской Федерации; Федеральным законом "О персональных данных"; Федеральным законом "О связи" и другими нормативно-правовыми актами. При этом в соответствии с п. 5 ч. 1 ст. 6 Федерального закона "О персональных данных" обработка ПДн, необходимая для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Клиент, а также для заключения договора по инициативе Клиента или договора, по которому Клиент будет являться выгодоприобретателем или поручителем, осуществляется без согласия Клиента.

Оператор может использовать ПДн в следующих целях:

- Идентификация Клиента в рамках оказания услуг Компанией.
- Связь с Клиентом в случае необходимости, в том числе направление уведомлений, информации и запросов, связанных с оказанием услуг, а также обработка заявлений, запросов и заявок Клиента.
- Проведение исследований на основе обезличенных ПДн.

Состав ПДн клиента:

- Фамилия, имя, отчество;
- дата и место рождения;
- реквизиты документа, удостоверяющего личность;
- Кем и когда выдан документ, удостоверяющий личность;
- Адрес регистрации/места жительства;
- Номер телефона;
- Уникальный номер клиента;
- Иные идентификационные данные клиента.

Процесс обработки ПДн включает в себя следующие действия:

- Сбор
- Запись
- Систематизация
- Накопление
- Хранение
- Уточнение (обновление, изменение)
- Извлечение
- Использование
- Передача (распространение предоставление, доступ)
- Обезличивание
- Блокирование
- Удаление
- Уничтожение.

Различают следующие виды ПДн:

- на бумажном носителе;
- в электронном виде в ИСПДн.

Для обеспечения доступа Ответственных лиц Оператора к ПДн, ТО Оператора в начале каждого года формирует Перечень должностей Ответственных лиц, которые используют ПДн в служебных целях.

В Перечень включают должности Ответственных лиц, которые используют ПДн непосредственно для выполнения конкретных функций в соответствии с Положением о подразделении и/или Должностной инструкцией.

Перечень должностей Ответственных лиц, которые обрабатывают ПДн, утверждает Генеральный директор Оператора.

Каждое Ответственное лицо, должность которого включена в «Перечень должностей Ответственных лиц, обрабатывающих ПДн», несет персональную ответственность за соблюдение требований настоящего Положения и обеспечение мер по защите ПДн.

Лица, виновные в нарушении требований настоящего Положения, несут предусмотренную законодательством Российской Федерации ответственность.

Оценка вреда, который может быть причинен клиенту при нарушении требований,

установленных законодательством к обработке его ПДнк, осуществляется ответственным лицом за организацию обработки ПДнк экспертным путем в каждом выявленном случае нарушений таких требований. При этом производится соотнесение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством.

#### **4 Обязанности оператора при получении запроса клиента**

##### **4.1 При получении от клиента запроса об обработке его ПДнк**

При получении запроса от клиента об обработке его ПДнк, Ответственное лицо Оператора обязано дать по полученным вопросам клиенту ответ в момент обращения либо в течение тридцати дней с даты получения запроса.

В случае отказа в предоставлении клиенту информации о наличии его ПДнк, порядке обработки, Ответственное лицо Оператора обязано дать в письменной форме мотивированный ответ, содержащий основание для такого отказа в срок, не превышающий тридцати дней со дня обращения клиента либо с даты получения запроса.

##### **4.2 При получении от клиента запроса о внесении изменений в ПДнк**

При обращении клиента о внесении изменений и предоставлении сведений, подтверждающих, что ПДнк являются неполными, неточными или неактуальными, Ответственное лицо Оператора обязано внести в них необходимые изменения в срок, не превышающий семи рабочих дней со дня предоставления клиентом информации.

##### **4.3 При получении от клиента запроса о незаконном получении оператором его ПДнк**

В срок, не превышающий семи рабочих дней со дня представления клиентом сведений, подтверждающих, что такие ПДнк являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Ответственные лица Оператора обязаны уничтожить такие ПДнк и уведомить клиента о внесенных изменениях и предпринятых мерах, и принять разумные меры для уведомления третьих лиц, которым ПДнк этого клиента были переданы.

##### **4.4 При получении от клиента запроса о прекращении обработки ПДнк**

При обращении клиента с просьбой прекратить обработку его ПДнк, обработка ПДнк производится в соответствии с п. 5.5, 5.6. настоящего Положения.

#### **5 Обработка ПДнк**

##### **5.1 Сбор, запись, систематизация, накопление и изменение ПДнк**

Сбор и запись ПДнк (потенциальных клиентов) осуществляют Ответственные лица за заключение договоров с Клиентами при подаче письменного (собственноручно подписанного Клиентом) заявления на предоставление услуг.

На основании заявления Клиента, оператор осуществляет обработку его ПДнк.

Клиент представляет свои ПДнк при оформлении заявления и/или оформлении договора об оказании услуг в объеме, требующемся для заключения договора в соответствии с утвержденными формами.

Систематизацию, накопление и изменение ПДнк выполняют Ответственные лица Оператора.

На основании заявления Клиента Ответственное лицо по требованию Клиента формирует записи о ПДнк на бумажном носителе (Договор об оказании услуг, Дополнительное соглашение к Договору, др.), часть информации заносит в КИС ПДнк. Уточнение (обновление, изменение) ПДнк производит Ответственное лицо по заявлению Клиента с предъявлением оригиналов необходимых документов. Внесение изменений в ПДнк выполняют с помощью пользовательского интерфейса управления КИС ПДнк в присутствии Клиента. При обработке ПДнк в бумажном виде - изменение выполняют с заменой данных на бумажном носителе в присутствии Клиента.

##### **5.2 Использование ПДнк Клиента**

Использование ПДнк возможно только для исполнения договора с Клиентом. Письменное согласие Клиента на использование его ПДнк требуется в случае при предоставлении сведений о Клиенте третьим лицам, за исключением случаев, предусмотренных действующим законодательством.

##### **5.3 Передача обработки ПДнк третьей стороне**

Передачу ПДнк осуществляют в случае, если Оператор поручает обработку ПДнк другому лицу на основании договора.

Оператор вправе поручить обработку ПДнк другому лицу с согласия Клиента, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора).

В поручении Оператора должны быть определены перечень действий (операций) с ПДнк, которые будут совершаться лицом, осуществляющим обработку ПДнк, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДнк и обеспечивать безопасность ПДнк при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДнк.

Лицо, осуществляющее обработку ПДнк по поручению Оператора, не обязано получать согласие Клиента на обработку его ПДнк.

В случае если Оператор поручает обработку ПДнк другому лицу, ответственность перед Клиентом за действия указанного лица несет Оператор. Лицо, осуществляющее обработку ПДнк по поручению Оператора, несет ответственность перед Оператором.

В случае, когда в соответствии с договором на оказание услуг, проведении работ сторонами будет передаваться ПДнк, необходимо заключение Соглашения о конфиденциальности.

#### **5.4 Обезличивание ПДнк данных Клиентов**

Обезличивание ПДнк выполняют в КИСПДнк для подготовки статистических отчетов. Обезличивание проводят Ответственные лица, подготавливающие данные отчеты.

#### **5.5 Блокирование ПДнк**

На основании заявления Клиента о прекращении действия договора, осуществляется блокирование обработки его ПДнк. Блокирование ПДнк выполняет Ответственное лицо Оператора, путем ввода в КИС даты расторжения договора на оказание услуг. Такие ПДнк подлежат обработке в течение срока исковой давности, установленного действующим законодательством.

#### **5.6 Правила хранения ПДнк**

Хранение ПДнк на бумажном носителе осуществляют в надежно укрепленных помещениях, доступ в которые имеют только Ответственные лица Оператора.

В электронном виде ПДнк хранятся в КИСПДнк. Срок хранения - не менее 5 лет после истечения срока действия договора, заявления (оферты).

#### **5.7 Уничтожение ПДнк**

Уничтожение ПДнк выполняет Ответственное лицо Оператора после достижения цели обработки ПДнк или по истечении срока хранения.

Уничтожение носителей информации, содержащих ПДнк, оформляется Актом об уничтожении материального носителя информации.

Материальные носители информации в бумажном виде, содержащие ПДнк, уничтожают путем измельчения, не позволяющего их последующего восстановления (например, с использованием бумагорезательной машины (БРМ)).

Уничтожение ПДнк организуют и обеспечивают Ответственные лица, обеспечивающие обработку и хранение ПДнк.

Электронные файлы с ПДнк удаляют с помощью пользовательского интерфейса управления КИСПДнк.

Уничтожение ПДнк в электронном виде Ответственное лицо выполняет в соответствии с установленным Оператором технологического процесса и требованиями эксплуатационной документацией КИС.

В случае передачи оргтехники Оператора в ремонт в стороннюю организацию, Ответственное лицо за организацию обработки ПДнк обязано организовать уничтожение размещенной на передаваемом оборудовании информации с ПДнк.

### **6 Дополнительные требования по обработке ПДнк в КИСПДнк в период их ремонта и обслуживания**

При выполнении технического обслуживания оборудования КИСПДнк необходимо принять меры по изъятию из состава обслуживаемого оборудования машинных носителей информации, содержащих ПДнк.

В случае, если ремонту/замене подлежат сами машинные носители информации, а гарантированное уничтожение ПДнк на них невозможно, передача таких носителей допускается при условии наличия соглашения о конфиденциальности с организацией, осуществляющей ремонт (замену). При невозможности выполнения указанных условий такие носители подлежат списанию и физическому уничтожению.

### **7 Ответственность**

Ответственным за общую организацию обработки ПДнк у Оператора является начальник ИО.

Контроль за принимаемыми мерами по обеспечению безопасности ПДнк проводит

начальник ИО в соответствии с Положением об ИО.

## **8 Меры по обеспечению безопасности ПДнк при их обработке**

Оператор при обработке ПДнк обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДнк от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДнк, а также от иных неправомерных действий в отношении ПДнк. Обеспечение безопасности ПДнк достигается, в частности:

- определением угроз безопасности ПДнк при их обработке в КИСПДнк;
- применением организационных и технических мер по обеспечению безопасности ПДнк при их обработке в КИСПДнк, необходимых для выполнения требований к защите ПДнк, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДнк. При создании КИС с ПДнк в процессе разработки документации (технические решения, Инструкции по эксплуатации КИС, приказы о вводе в эксплуатацию КИС) устанавливаются организационные и технические меры в соответствии с ФЗ и нормативными документами, применительно к данной КИС;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДнк до ввода в эксплуатацию КИСПДнк. При создании КИС с ПДнк (до ввода в эксплуатацию КИСПДнк), определяются мероприятия по оценке эффективности, которые указываются в документации на КИС;
- учетом машинных носителей ПДнк;
- обнаружением фактов несанкционированного доступа к ПДнк и принятием мер;
- восстановлением ПДнк, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДнк, обрабатываемым в КИСПДнк, а также обеспечением регистрации и учета всех действий, совершаемых с ПДнк в КИСПДнк;
- контролем за принимаемыми мерами по обеспечению безопасности ПДнк и уровня защищенности КИСПДнк. Контроль за принимаемыми мерами по обеспечению безопасности ПДнк проводится СБ в соответствии с Положением о СБ.

## **9 Сведения о реализуемых требованиях к защите ПДнк**

Созданные Оператором условия и режим защиты информации, отнесенной к ПДнк, позволяют обеспечить защиту обрабатываемых ПДнк.

Оператором в соответствии с действующим законодательством Российской Федерации разработан и введен в действие комплекс организационно-распорядительных, функциональных и планирующих документов, регламентирующих и обеспечивающих безопасность обрабатываемых ПДнк.

Введены режим безопасности обработки и обращения с ПДнк, а также режим защиты помещений, в которых осуществляется обработка и хранение носителей ПДнк.

Назначены ответственный за организацию и обеспечение безопасности ПДнк, ответственный за организацию технической защиты ПДнк, им определены обязанности и разработаны инструкции по обеспечению безопасности информации.

Определены требования к персоналу, степень ответственности Ответственных лиц за обеспечение безопасности ПДнк.

Проведено ознакомление Ответственных лиц, осуществляющих обработку ПДнк, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных. Проводится периодическое обучение указанных Ответственных лиц с правилам обработки персональных данных.

Предприняты необходимые и достаточные технические меры для обеспечения безопасности ПДнк от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:

- Введена система разграничения доступа.
- Установлена защита от несанкционированного доступа к КИС.
- Установлена защита от вредоносного программно-математического воздействия.
- Осуществляется регулярное резервное копирование информации и баз данных.

**9 При реализации данного Положения в подразделениях Оператора создаются следующие записи (документы):**

№ п/п	Наименование записи	Кто создает	Место хранения	Срок хранения
1.	Заявка/заявление/ потенциального Клиента	Структурное подразделение, ответственное за заключение договоров с Клиентами	Структурное подразделение, ответственное за заключение/ хранение договоров с Клиентами	Не менее 5 лет после истечения срока действия договора, соглашения с данным Клиентом
2.	Договор об оказании услуг	Структурное подразделение, ответственное за заключение договоров с Клиентами	Структурное подразделение, ответственное за заключение/ хранение договоров с Клиентами	Не менее 5 лет после истечения срока действия договора, соглашения с данным Клиентом
3.	Сведения об Клиенте	Структурное подразделение, ответственное за заключение договоров с Клиентами	Корпоративная информационная система	Не менее 5 лет после истечения срока действия договора, соглашения с данным Клиентом

**10 Хранение и архивирование**

Подлинник настоящего Положения во время срока действия хранится в ИО.

**11 Рассылка и актуализация**

Периодическая проверка Положения осуществляется ИО по мере необходимости, но не реже 1-го раза в 12 месяцев.

Решение об инициации процесса внесения изменений в Положение принимает Начальник ИО на основании предложений других подразделений, результатов применения документа Оператора, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

Актуальная версия утвержденного Положения размещена на сайте [www.sevstar.net](http://www.sevstar.net). Ответственность за размещение и поддержание в актуальном состоянии размещенного на сайте [www.sevstar.net](http://www.sevstar.net). Положения, а также доведение информации о месте размещения актуальной версии до всех заинтересованных подразделений несет Начальник ИО Оператора.