

УТВЕРЖДАЮ

Генеральный директор ООО «ЮТС»

Крылов А.В.

« 9 » декабря 2016 г.



**ПОЛОЖЕНИЕ
ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ООО «ЮТС»**

Москва 2016

ОГЛАВЛЕНИЕ

1	ВВЕДЕНИЕ	3
2	ТЕРМИНЫ И СОКРАЩЕНИЯ	4
3	ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ ООО «ЮТС»А	7
3.1	Основания и цели обработки персональных данных Клиентов	7
3.2	Условия обработки персональных данных Клиента.....	7
3.3	Ответственный за организацию обработки персональных данных	9
3.4	Права и обязанности Клиента	9
3.5	Порядок запроса сведений Клиентом.....	9
3.6	Обработка персональных данных Клиентов третьим лицом	10
4	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	11
5	НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ.....	13

1 ВВЕДЕНИЕ

Политика по обработке и защите персональных данных Клиентов (далее – Политика) определяет правила и порядок обработки ПДн Клиентов ООО «ЮТС», а также требования к способам обработки.

Настоящая политика разработана в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 24.11.1996 N 132-ФЗ "Об основах туристской деятельности в Российской Федерации";
- Постановлением Правительства РФ от 18.07.2007 № 452 "Об утверждении правил оказания услуг по реализации туристического продукта";
- Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Руководящим документом ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден Заместителем директора ФСТЭК России 15 февраля 2008 г.;
- Руководящим документом ФСТЭК России. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден Заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К)» ФСТЭК России;

2 ТЕРМИНЫ И СОКРАЩЕНИЯ

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание: Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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

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

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

Система защиты информационных систем ООО «ЮТС» – совокупность программных, аппаратных и технических средств защиты информации, используемых для обеспечения информационной безопасности информационных систем ООО «ЮТС».

Сотрудник ответственный за организацию обработки ПДн – должностное лицо ООО «ЮТС», ответственное за организацию обработки ПДн в ООО «ЮТС».

Субъект персональных данных (субъект ПДн) – лицо, обработка персональных данных которого осуществляется в ООО «ЮТС», (Клиенты ООО «ЮТС»: физические лица/их представители, представители юридических лиц, индивидуальные предприниматели, предоставляющие свои персональные данные для обработки в ООО «ЮТС»).

Турист (субъект ПДн) - лицо, посещающее страну (место) временного пребывания в лечебно-оздоровительных, рекреационных, познавательных, физкультурно-спортивных, профессионально-деловых, религиозных и иных целях без занятия деятельностью, связанной с получением дохода от источников в стране (месте) временного пребывания, на период от 24 часов до 6 месяцев подряд или осуществляющее не менее одной ночевки в стране (месте) временного пребывания;

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных ООО «ЮТС».

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.

Туризм - временные выезды (путешествия) граждан Российской Федерации, иностранных граждан и лиц без гражданства (далее - лица) с постоянного места жительства в лечебно-оздоровительных, рекреационных, познавательных, физкультурно-спортивных, профессионально-деловых, религиозных и иных целях без занятия деятельностью, связанной с получением дохода от источников в стране (месте) временного пребывания;

Туристская деятельность - туроператорская и турагентская деятельность, а также иная деятельность по организации путешествий;

Туристский продукт (Турпродукт) - комплекс услуг по перевозке и размещению, оказываемых за общую цену (независимо от включения в общую цену стоимости экскурсионного обслуживания и (или) других услуг) по договору о реализации туристского продукта;

Список принятых сокращений

ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные

3 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ ООО «ЮТС»

3.1 Основания и цели обработки персональных данных Клиентов

Персональные данные Клиента могут обрабатываться в ООО «ЮТС» в следующих случаях (на основаниях), установленных Федеральным законом №152-ФЗ «О персональных данных»:

- обработка персональных данных Клиента осуществляется с его согласия;
- обработка персональных данных необходима для достижения целей, предусмотренных законом Российской Федерации, для осуществления и выполнения возложенных законодательством Российской Федерации на ООО «ЮТС» функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- обработка персональных данных необходима для заключения договора по инициативе Клиента или договора, по которому Клиент будет являться выгодоприобретателем или поручителем;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Персональные данные Клиента могут обрабатываться в ООО «ЮТС» только для целей, непосредственно связанных с туристической деятельностью ООО «ЮТС», в частности, для оказания заявленных услуг и осуществления видов деятельности, указанных в Уставе ООО «ЮТС».

Клиент предоставляет ООО «ЮТС» ПДн только в объеме, необходимом для реализации турпродукта.

3.2 Условия обработки персональных данных Клиента

В ООО «ЮТС» осуществляется смешанная обработка (как автоматизированная, так и неавтоматизированная) ПДн Клиента.

Сбор, хранение, использование и распространение, в том числе передача третьим лицам, ПДн Клиента без письменного его согласия или любого другого основания, установленного Федеральным законом №152-ФЗ «О персональных данных» и, в частности, разделом 3.1 настоящей Политики, в ООО «ЮТС» запрещена.

В ООО «ЮТС» не ведется сбор и обработка биометрических и специальных категорий ПДн Клиента, в том числе информации его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

В должностных инструкциях сотрудников ООО «ЮТС», осуществляющих обработку персональных данных Клиентов ООО «ЮТС», установлены ответственность за разглашение обрабатываемых персональных данных Клиента и меры необходимые для безопасной обработки ПДн в

ООО «ЮТС». Сотрудники ООО «ЮТС», не ознакомленные с нормативными документами регламентирующими обработку персональных данных Клиента, к обработке ПДн не допускаются.

При предоставлении согласия на обработку ПДн Клиента (в случае если нет других оснований на обработку ПДн ООО «ЮТС», установленных Федеральным законом №152-ФЗ «О персональных данных» и в частности разделом 3.1 настоящей Политики), должны соблюдаться следующие условия:

– Клиент ООО «ЮТС» принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным.

– Согласие на обработку персональных данных может быть дано Клиентом или его представителем в письменной форме или в любой другой форме, позволяющей подтвердить факт его получения. Шаблон «Согласия Клиента на обработку персональных данных» представлен в Приложении А.

– В случае получения согласия на обработку персональных данных от представителя Клиента, полномочия данного представителя на дачу согласия от имени Клиента должны быть проверены ООО «ЮТС».

В случае выявления недостоверных ПДн или неправомерных действий ООО «ЮТС» с ними при обращении или по запросу Клиента, ООО «ЮТС» обязано осуществить блокирование ПДн.

В случае подтверждения факта неточности персональных данных ООО «ЮТС» на основании сведений предоставленных Клиентом или его представителем, либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязан уточнить персональные данные, либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ООО «ЮТС») в течение *семи рабочих дней* со дня представления таких сведений и снять блокирование персональных данных.

В случае достижения цели обработки персональных данных, ООО «ЮТС» обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ООО «ЮТС») и уничтожить персональные данные, или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ООО «ЮТС») в срок, не превышающий *тридцати дней* с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством или условиями договора с субъектом ПДн, либо другими законными основаниями, предусмотренными Федеральным законом №152-ФЗ «О персональных данных» и, в частности, разделом 3.1 настоящей Политики.

В случае отзыва Клиентом согласия на обработку его персональных данных, ООО «ЮТС» обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению ООО «ЮТС») и в случае, если хранение персональных данных более не требуется для целей обработки персональных данных в срок, не превышающий *тридцати дней* с даты поступления указанного отзыва, если иное не предусмотрено законом или условиями договора с Клиентом, либо другими законными основаниями, предусмотренными Федеральным законом №152-ФЗ «О персональных данных» и, в частности, разделом 3.1 настоящей Политики. Об уничтожении ПДн ООО «ЮТС» обязано уведомить Клиента.

В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, ООО «ЮТС» осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более *чем шесть месяцев*, если иной срок не установлен федеральными законами.

3.3 Ответственный за организацию обработки персональных данных

Сотрудник ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных в ООО «ЮТС»;
- доводить до сведения сотрудников ООО «ЮТС» положения законодательства Российской Федерации о персональных данных, внутренних нормативных документов и требований по защите персональных данных;
- организовывать прием и обработку обращений и запросов Клиентов или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.4 Права и обязанности Клиента

Клиент при обработке его ПДн в ООО «ЮТС» имеет право:

- на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
 - 1) подтверждение факта обработки персональных данных в ООО «ЮТС»;
 - 2) правовые основания и цели обработки персональных данных;
 - 3) цели и применяемые в ООО «ЮТС» способы обработки персональных данных;
 - 4) наименование и место нахождения компании, сведения о лицах (за исключением работников ООО «ЮТС»), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ООО «ЮТС» или на основании федерального закона;
 - 5) сроки обработки персональных данных, в том числе сроки их хранения;
 - 6) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
 - 7) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению ООО «ЮТС», если обработка поручена или будет поручена такому лицу;
 - 8) иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.
- на отзыв данного ранее согласия на обработку ПДн, если иное не предусмотрено условиями договора с Клиентом или другими законными основаниями, предусмотренными Федеральным законом №152-ФЗ «О персональных данных» и, в частности, разделом 3.1 настоящей Политики.

Сведения должны быть предоставлены Клиенту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных. Порядок запроса указанных сведений представлен в разделе 3.5 настоящей политики.

3.5 Порядок запроса сведений Клиентом

Сведения, запрашиваемые Клиентом в соответствии с разделом 3.4 настоящей Политики, предоставляются Клиенту или его представителю при обращении либо при получении запроса Клиента

или его представителя. Шаблон Заявления на запрос сведений представлен в Приложении Б настоящего документа.

Оформленное Заявление предоставляется Сотруднику, осуществляющему сбор ПДн Клиентов в ООО «ЮТС».

Ответственный за организацию обработки персональных данных, проверяет представленное Заявление и готовит запрашиваемую Клиентом информацию в виде ответного письма, за подписью руководства ООО «ЮТС» в срок не более *тридцати дней*, в другом случае, в течение указанного срока, готовит мотивированный отказ.

Клиент вправе обратиться повторно в ООО «ЮТС» или направить повторный запрос в целях получения запрошенных сведений, и ознакомления с такими персональными данными не ранее чем через *тридцать дней* после первоначального обращения или по факту получения ответа на первоначальное обращение, в том числе, если запрошенные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления Клиенту не в полном объеме. Повторный запрос должен содержать обоснование направления повторного запроса.

ООО «ЮТС» вправе отказать Клиенту в выполнении повторного запроса, в случае не соответствия перечисленным выше условиям.

Право Клиента на доступ к его персональным данным, обрабатываемых ООО «ЮТС», может быть ограничено в соответствии с федеральными законами.

3.6 Обработка персональных данных Клиентов третьим лицом

ООО «ЮТС» вправе поручить обработку, в том числе передать, персональные данные субъекта ПДн третьему лицу, при этом должны соблюдаться следующие требования:

- передача ПДн третьим лицам возможна при согласии Клиента, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора;
- лицо, осуществляющее обработку персональных данных по поручению ООО «ЮТС», обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных»;
- в договоре ООО «ЮТС» с третьим лицом должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, и цели обработки;
- в договоре с ООО «ЮТС» с третьим лицом должна быть установлена обязанность третьего лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке.

Лицо, осуществляющее обработку персональных данных Клиента по поручению ООО «ЮТС», не обязано получать согласие Клиента на обработку его персональных данных.

4 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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.

Безопасность персональных данных, в том числе при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях обеспечивает сохранность носителей персональных данных и средств защиты информации, а также исключает возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

При обработке персональных данных в информационных системах ООО «ЮТС» осуществляется:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного в ООО «ЮТС».

5 НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Неавтоматизированная обработка ПДн в ООО «ЮТС» заключается в работе с бумажными носителями информации, которые содержат сведения, составляющие ПДн (далее – бумажные носители ПДн).

К бумажным носителям ПДн в ООО «ЮТС» относятся документы (анкеты, договоры, выписки, скан копии документов, заявления, и т. д.) на бумажных носителях, получаемые от Клиентов ООО «ЮТС»;

В ООО «ЮТС» установлены следующие требования к хранению бумажных носителей ПДн:

- срок хранения для бумажных носителей ПДн, устанавливается согласно внутренним документам ООО «ЮТС», в зависимости от состава ПДн;
- бумажные носители ПДн хранятся в специализированных запираемых шкафах или сейфах, назначается ответственный за хранение ПДн на бумажных носителях сотрудник для каждого Структурного подразделения ООО «ЮТС», в рамках которого происходит обработка бумажных носителей ПДн;
- запрещается хранение бумажных носителей ПДн в местах, доступных для ознакомления посторонними лицами;
- сотруднику ООО «ЮТС», выполняющему обработку ПДн с использованием бумажных носителей ПДн, запрещается бесконтрольно хранить их на своем рабочем месте.

В ООО «ЮТС» установлены следующие требования к уничтожению бумажных носителей ПДн:

- уничтожение бумажных носителей ПДн проводится при помощи технических средств (уничтожителей бумаги), исключающих возможность полного или частичного восстановления данных носителей;
- ответственным за уничтожение бумажных носителей ПДн назначается Сотрудник, отвечающий за хранение данных носителей ПДн;
- уничтожение бумажных носителей ПДн должно оформляться актом.

Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. В случае обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Уточнение персональных данных при осуществлении их неавтоматизированной обработки в ООО «ЮТС» производится путем обновления или изменения данных на бумажном носителе ПДн, либо путем изготовления нового бумажного носителя ПДн с уточненными ПДн.

Неавтоматизированная обработка ПДн в ООО «ЮТС» должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения персональных данных (бумажных носителей ПДн) и установить сотрудников ООО «ЮТС», осуществляющих неавтоматизированную обработку ПДн, либо имеющих к ним доступ.

При хранении бумажных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

