Утверждаю:
Президент АО «ЦСТЭ»
(холдинг)
В.Г. Пугиев
«24» VI 20 14 г.

Политика обработки и защиты персональных данных в Акционерном обществе «Центральный совет по туризму и отдыху» (холдинг) (далее Общество) и в его обособленных структурных подразделениях (далее Филиалы), расположенных вне места нахождения Общества.

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним локальным актом Общества, определяющим ключевые направления деятельности Общества и Филиалов в области обработки и защиты персональных данных (далее – ПДн), операторами которых они являются.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Обществе и Филиалах, в том числе защиты прав на неприкосновенность частной, личной и семейной жизни.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Обществом и Филиалами как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Обработка ПДн в Обществе и Филиалах осуществляется в связи с выполнением Обществом и Филиалами функций, предусмотренных его учредительными документами и Положениями о Филиалах, и определяемых:

-Трудовым Кодексом Российской Федерации;

– Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;

– Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в Обществе и Филиалах осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Общество выступает в качестве Работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Обществом и Филиалами своих прав и обязанностей, определенных законодательством об акционерных обществах, ГК РФ, Положениями о филиалах и другими нормативными правовыми актами РФ.

1.5. Общество имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Общества по адресу: г. Россия, г. Москва, ул. Озерковская наб., дом 50, стр.1., электронная версия Политики – на сайте по адресу: cctr.ru а его заверенные в установленном порядке копии - по месту нахождения Филиалов.

1.7. Общество и Филиалы самостоятельно разрабатывают другие локальные правовые акты и документы, связанные с получением, использованием и защитой ПДн своих работников и других физических лиц, с которыми они заключают соответствующие договоры или оказывают те или иные услуги.

2. Термины и принятые сокращения

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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 – Общество и Филиалы, осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

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

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

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

Автоматизированная обработка персональных данных – обработка персональных данных с помощью технических средств;

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

Клиент – физическое лицо, которому Обществом и Филиалами реализуются права на оказание санаторно-курортных услуг и оказываются эти и

другие услуги. Согласие на обработку его персональных данных может отражаться в договоре купли-продажи прав на оказание санаторно-курортных услуг или в письменном заявлении клиента на имя Президента Общества или директора Филиала;

Медицинская деятельность - профессиональная деятельность, осуществляемая Филиалами Общества на основании лицензий, выданных Обществу в соответствии с п.2 ст.12 Федерального закона «О лицензировании отдельных видов деятельности»;

Медицинский персонал - это лица, которые организуют и оказывают Клиенту услуги по первичной, в том числе доврачебной, врачебной и специализированной, медико-санитарной помощи при санаторно-курортном лечении (долечивании) и оздоровлении в соответствии с лицензией на осуществление медицинской деятельности ЛО-26-01-003873 от 07 декабря 2016 г. и Приложениями к ней, выданной Министерством здравоохранения Ставропольского края, и лицензией на осуществление медицинской деятельности ЛО-50-01-007933 от 11 августа 2016 г. и Приложениями к ней, выданной Министерством здравоохранения Московской области .

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Обществе и Филиалах является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Общество и Филиалы руководствуются следующими принципами:

– законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

– системность: обработка ПДн в Обществе и Филиалах осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных

системах Общества и Филиалах, других имеющихся в Обществе и Филиалах систем и средств защиты;

– непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

– своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников Общества и Филиалов в пределах их обязанностей, связанных с обработкой и защитой ПДн;

– минимизация прав доступа: доступ к ПДн предоставляется Работникам Общества и Филиалов только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Общества и Филиалов , а также объема и состава обрабатываемых ПДн;

– специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками Общества и Филиалов, имеющими необходимые для этого квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика Общества и Филиалов предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

– наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются;

-конфиденциальность ПДн. Работники Общества и Филиалов, получившие доступ к ПДн обязаны не допускать их распространение без письменного согласия субъекта ПДн, если иное не предусмотрено федеральными законами.

3.3. В Обществе и Филиалах не производится обработка ПДн, не совместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Обществе и Филиалах, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Обществом и Филиалами ПНд уничтожаются или обезличиваются.

3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Общество и Филиалы принимают необходимые меры по удалению или уточнению неполных или неточных ПДн.

4.Обработка персональных данных

4.1. Получение ПДн.

4.1.1. Все ПДн следует получать от самого субъекта - физического лица или его законного представителя (родителей, попечителя, опекуна) на основании документов, подтверждающих представительство. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть письменно уведомлен об этом Обществом и Филиалами или от него должно быть получено письменное согласие.

4.1.2. Общество и Филиалы должны сообщить субъекту или его представителям о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта или его представителей дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, и др.);

г) реквизиты полиса ОМС (ДМС);

д) данные о состоянии здоровья, заболеваниях;

е) согласие на предоставление и обработку ПДн;

ж) другие документы, полученные или оформленные с соблюдением законодательства РФ при приеме на работу субъекта или в процессе его трудовой деятельности, при поступлении его на лечение (оздоровление) или отдых в Филиалы, осуществляющие медицинскую деятельность от имени Общества.

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Обществом и Филиалами документам, определяется в соответствии с законодательством РФ и внутренними локальными актами Общества и Филиалов.

Одним из локальных актов является Положение о персональных данных, которое разрабатывается и утверждается Обществом и Филиалами самостоятельно.

4.2. Обработка ПДн

4.2.1. Обработка ПДн осуществляется:

– с письменного согласия субъекта ПДн на обработку его ПДн или законных его представителей (родителей, опекунов, попечителей), подтверждающих представительство соответствующими документами;

– в случаях, когда обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе (далее – ПДн, сделанные общедоступными субъектом ПДн.

Доступ Работников Общества и Филиалов к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями локальных актов Общества и Филиалов.

Допущенные к обработке ПДн Работники Общества и Филиалов под роспись знакомятся с документами Общества и Филиалов, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников Общества и Филиалов.

Обществом и Филиалами производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

Образцы форм согласия на обработку ПДн должны находиться у работников Общества и Филиалов, ответственных за **сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, передачу, обезличивание, блокирование, уничтожение,**

защиту ПДн), а также в регистратуре Филиалов, которые после их заполнения вклеиваются в историю болезни субъекта ПДн.

4.2.2 Цели обработки ПДн:

Целью обработки ПДн субъектов (включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, передачу, обезличивание, блокирование, уничтожение, защиту ПДн) является :

– наиболее полное исполнение обязательств и компетенций в соответствии с федеральными законами по вопросам охраны здоровья граждан Российской Федерации, обращения лекарственных средств, обязательного медицинского страхования и другим; предоставления платных медицинских и других услуг;

– осуществление трудовых отношений;

– осуществление гражданско-правовых отношений;

- предоставление платных услуг по приему, размещению, питанию, лечению (долечиванию), оздоровлению и отдыху субъектам ПДн;

- предоставление других платных услуг субъектам ПДн.

4.2.3. Категории субъектов персональных данных

В Обществе и Филиалах обрабатываются ПДн следующих субъектов:

– физические лица, состоящие с Обществом и Филиалами в трудовых отношениях;

– физические лица, состоящие с Обществом и Филиалами в гражданско-правовых отношениях;

– физические лица, уволившиеся из Общества и Филиалов;

– физические лица, являющиеся кандидатами на работу в Общество и Филиалы;

- физические лица, которым Филиалами предоставляются услуги по приему, размещению, питанию, лечению (долечиванию), оздоровлению и отдыху ;

- физические лица, которым Обществом и Филиалами предоставляются другие услуги.

4.2.4. ПДн, обрабатываемые Обществом:

– данные, полученные для осуществления отбора кандидатов на работу в Общество;

– данные, полученные при осуществлении трудовых и гражданско-правовых отношений;

-данные, полученные при предоставлении услуг.

Полный перечень ПДн, которые Общество и Филиалы вправе получить от субъекта ПДн, в соответствии с законом, определяется приказами Президента Общества и директоров Филиалов.

4.2.5. Обработка персональных данных ведется:

- с использованием средств автоматизации;

– без использования средств автоматизации.

4.3. Хранение ПДн.

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа..

4.3.3. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.4. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.4. Уничтожение ПДн.

4.4.1. Уничтожение документов (носителей), содержащих ПДн. производится путем сожжения, дробления (измельчения), превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии и утвержденным Президентом Общества или директорами Филиалов.

4.5. Передача ПДн

4.5.1. Общество и Филиалы передают ПДн третьим лицам в следующих случаях:

– субъект персональных данных выразил свое письменное согласие на такие действия;

–передача предусмотрена федеральными законами и иными нормативными правовыми актами Российской Федерации.

4.5.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

– Пенсионный фонд РФ для учета (на законных основаниях);

– Налоговые органы РФ (на законных основаниях);

– Фонд социального страхования (на законных основаниях);

– Территориальный фонд обязательного медицинского страхования (на законных основаниях);

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

– банки для начисления заработной платы (на основании договора);

– судебные и правоохранительные органы в случаях, установленных законодательством РФ;

– бюро кредитных историй (с согласия субъекта);

– юридические лица, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

5. Защита ПДн.

5.5. Основными мерами защиты ПДн, используемыми Обществом и Филиалами, являются:

5.5.1. Назначение лица, ответственного за обработку ПДн, определение списка лиц, допущенных к работе с ПДн, разграничение прав доступа к обрабатываемы ПДн.

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн.

5.5.3 Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД.

5.5.4. Учет машинных носителей ПДн, обеспечение их сохранности;

5.5.5. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн

5.5.6. Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.5.7. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.8. Обучение работников Общества и Филиалов непосредственно осуществляющих обработку ПДн, положениям законодательства Российской Федерации о ПДн, в том числе требованиям к защите ПДн, документами, определяющими политику Общества в отношении обработки ПДн, локальным актам по вопросам обработки ПДн.

5.5.9. Осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПДн и обязанности Общества и Филиалов

6.1. Основные права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

– подтверждение факта обработки ПДн Обществом или Филиалами;

– правовые основания и цели обработки ПДн;

– цели и применяемые Обществом или Филиалами способы обработки ПДн;

– наименование и место нахождения Общества или Филиалов, сведения о лицах (за исключением работников Общества и Филиалов), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом и Филиалами или на основании фПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДнв, предусмотренных Федеральным законом «О персональных данных»;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества или Филиала, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные федеральными законами.

Субъект ПДн вправе требовать от Общества или Филиала уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются

необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Общества и Филиалов

Общество и Филиалы обязаны:

– при сборе ПДн предоставить информацию об обработке субъекту ПДн;

– в случаях если ПДн были получены не от субъекта ПДн письменно уведомить субъекта;

– при отказе в предоставлении ПДн разъяснить субъекту последствия такого отказа;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

– давать письменные ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

Документ Подготовлен:
В.М.Гудумак