УТВЕРЖДАЮ:

Генеральный директор

ООО «Санаторий ПлазаСПА»


В.Н. Григорьян

«15» 08 2014 г

ПОЛОЖЕНИЕ
ПО ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ООО «Санаторий ПлазаСПА»

Железноводск 2014

ОГЛАВЛЕНИЕ

1 ВВЕДЕНИЕ

Положение по обработке и защите персональных данных (далее-Положение)определяет правила и порядок обработки ПДнСубъектов ПДнООО «Санаторий ПлазаСПА»(далее – Организация), а также требования к способам обработки.

Настоящее Положение разработано в соответствии с:

– Конституцией Российской Федерации;

– Трудовой кодекс Российской Федерации;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ;

– Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» (в ред. Федерального закона от 25.07.2011 N 261-ФЗ);

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

– Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Руководящий документ 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;

– Руководящий документ 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.;

– «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» ФСТЭК России;

– Руководящий документ ФСБ РФ. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утвержден руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/5-144;

– Руководящий документ ФСБ РФ. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных. Утвержден руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

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 Организации 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 – 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 – ООО «Санаторий ПлазаСПА», 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 системОрганизации – совокупность программных, аппаратных и технических средств защиты информации, используемых для обеспечения информационной безопасности информационных систем Организации.

Субъект персональных данных (субъект ПДн) – лицо, обработка персональных данных которого осуществляется оператором персональных данных(клиенты,их представители, работники Организации и другие физические лица, предоставляющие свои персональные данные для обработки Организацией).

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.

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.

Уровень защищенности – под уровнем защищенности персональных данныхпонимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Список принятых сокращений

ИБ	Информационная безопасность
НСД	Несанкционированный доступ
СЗИ	Средства защиты информации
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

3 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Основания и цели обработки персональных данных

Персональные данныеСубъекта ПДн могут обрабатываться в Организации в следующих случаях (на основаниях), установленных Федеральным законом №152-ФЗ «О персональных данных»:

– обработка персональных данных Субъекта ПДн осуществляетсяс его согласия;

– обработка персональных данных необходима для достижения целей, предусмотренных законом Российской Федерации, для осуществления и выполнения возложенных законодательством Российской Федерации на Организацию 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 Субъекта ПДн или договора, по которому Субъект ПДн 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 Субъекта ПДн могут обрабатываться в Организациитолькодля целей, непосредственно связанных с деятельностью Организации, в частности, для оказания заявленных услуг и осуществления видов деятельности, указанных в Уставе Организации.

Субъект ПДн предоставляет ОрганизацииПДн только в объеме, необходимом для достижения названных целей.Более подробно цели обработки, а также состав, категория, сроки хранения и основания для обработки ПДнсубъекта ПДн определены в «Перечне сведений, относящихся к защищаемой информации ООО «Санаторий ПлазаСПА»». Основание для обработки ПДн в Организации зависит от особенностей построения технологического процесса обработки каждой ИСПДн, которые описаны в «Перечне ИСПДнООО «Санаторий ПлазаСПА», подлежащих защите».

По факту обработки персональных данных в Организации, должно быть отправлено соответствующее уведомление в Роскомнадзор установленного образца. Ответственным за формирование, отправку и при необходимости последующую корректировку уведомления является Ответственный за обработку персональных данных в ООО «Санаторий ПлазаСПА».

3.2 Условия обработки персональных данных

В Организацииосуществляется как автоматизированная,так и неавтоматизированная обработка ПДнсубъекта ПДн.

Сбор, хранение, использование и распространение, в том числе передача третьим лицам, ПДнСубъекта ПДнбез письменного его согласия или любого другого основания, установленного Федеральным законом №152-ФЗ «О персональных данных» и в частности разделом 3.1 настоящегоПоложения, в Организациизапрещена.

В Организации ведется сбор и обработка биометрических испециальных категорий ПДнСубъекта ПДн, в том числе информации его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

Работники Организации, в должностные обязанности которых входит обработка ПДнСубъекта ПДн, при приеме на работу должны подписыватьсоглашение о неразглашении персональных данных Субъекта ПДн (Клиента или Работника).Работники, осуществляющие обработку персональных данных Клиентов ООО «Санаторий ПлазаСПА»подписывают «Соглашение о неразглашении персональных данных Клиента», формат которого представлен в Приложении А.Работники осуществляющие обработку персональных данных Работников ООО «Санаторий ПлазаСПА» подписывают «Соглашение о неразглашении персональных данных Работника», формат которого представлен в Приложении Б.

Подписанные Соглашения хранятся в Личных делах Работников, копии хранятся у Работника ответственного за организацию обработки персональных данных.

Работники, не подписавшие данное соглашение, к обработке ПДн не допускаются.

Все ПДнСубъекта, обработка которых ведется в Организации, должны быть получены у него самого, после предоставления им письменного согласия.

Во все договора и анкеты Организации, заключаемые с Субъектами ПДнОрганизации (физическими лицами, их представителями; индивидуальными предпринимателями; юридическими лицами и т.д.),должен быть включен пункт о согласииСубъекта ПДн на обработку переданных им в Организацию его персональных данных с возможностью передачи третьим лицам (третьи лица должны быть конкретизированы).

В тех случаях, когда необходимо получение отдельного согласия Субъекта ПДн (нет других оснований на обработку ПДн, установленных Федеральным законом №152-ФЗ «О персональных данных» и в частности разделом 3.1 настоящегоПоложения), должны соблюдаться следующие условия:

– Субъект ПДн 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 Субъектом ПДн или его представителем в письменной форме или в любой другой форме, позволяющей подтвердить

факт его получения. Шаблон «Согласия субъекта ПДн на обработку своих персональных данных» представлен в Приложении В.

– в случае получения согласия на обработку персональных данных от представителя Субъекта ПДн, полномочия данного представителя на дачу согласия от имени Субъекта ПДн должны быть проверены Организацией.

– согласие на обработку персональных данных должно содержать:

– фамилию, имя, отчество, адрес Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес Представителя Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого Представителя (при получении согласия от Представителя Субъекта ПДн);

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие Субъекта ПДн;

– наименование и адрес третьего лица, осуществляющего обработку персональных данных по поручению Организации, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Организацией способов обработки персональных данных;

– срок, в течениекоторого действует согласиеСубъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись Субъекта ПДн.

В Согласиитакже должно быть указано, что все сообщенные СубъектомПДнперсональные данные, Организация может обрабатывать(в т.ч. хранить), в любой форме, при этом Субъект ПДн, соглашается с условиями обработки, хранения, способов защиты его ПДн и с тем, что Организация имеет право на передачу его персональных данных третьим лицам на основании требований Законодательства РФ и бизнес-процессов Организации.

Для автоматизированной и неавтоматизированной обработки в Организации принимаются только договора и анкеты, содержащие пункт согласия на обработку ПДни подписанные Субъектом.

В случае выявления недостоверных ПДн или неправомерных действий Организациис ними при обращениили по запросу субъекта ПДн,Организацияобязанаосуществить блокирование ПДн.

В случае подтверждения факта неточности персональных данныхОрганизация на основании сведений, представленных Субъектом ПДн 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 Организации) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае достижения цели обработки персональных данных,Организация обязана прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и уничтожить персональные данные, или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцатидней 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 частностиразделом 3.1 настоящегоПоложения.

В случае отзыва Субъектом персональных данных согласияна обработку его персональных данных,Организацияобязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) в срок, не превышающий тридцати дней с даты поступления указанного отзыва,если иное не предусмотрено законом 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 Частной политики. Об уничтожении ПДнОрганизация обязана уведомить Субъекта ПДн.

В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

3.3 Ответственный за обработку персональных данных

Ответственным за организацию обработки персональных данныхв рамках Структурного подразделения Организации согласно требованиям настоящего Положения, является Руководитель данного Структурного подразделения.

Ответственный за обработку персональных данных обязан:

– осуществлять внутренний контроль за соблюдением Организацией и ее Работникамизаконодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доводить до сведения Работников Организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, внутренних требований к защите персональных данных;

– организовывать прием и обработку обращений и запросов Субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.4Права и обязанности субъекта ПДн

Субъект ПДн при обработке его ПДнвОрганизациииимеет право:

– на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данныхОрганизацией;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Организацией способы обработки персональных данных;

4) наименование и место нахождения Организации, сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией 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 Организации, 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 Субъектом ПДн или другими законными основаниями, предусмотренными Федеральным законом №152-ФЗ «О персональных данных» и в частности разделом 3.1 настоящей Частной политики.

Сведения должны быть предоставлены Субъекту ПДнОрганизацией 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.

3.5Порядок запроса сведений Субъектом ПДн

Сведения, запрашиваемые субъектом ПДн в соответствие с разделом 3.2 настоящей Частной политики, предоставляются СубъектуПДнили его представителю Организацией при

обращении либо при получении запроса Субъекта ПДнили его представителя. Запрос (Заявление)должен содержать:

– номер основного документа, удостоверяющего личностьСубъекта ПДн или его представителя;

– сведения о дате выдачи указанного документа и выдавшем его органе;

– почтовый адрес Субъекта ПДн;

– сведения, подтверждающие участие Субъекта ПДн в отношениях с Организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Организацией;

– подпись Субъекта ПДн или его представителя.

Шаблон Заявления на запрос сведений представлен в Приложении Г настоящего документа. По усмотрению Клиента Заявление на запрос сведений заполняется согласно представленному Шаблону или в произвольной форме.

Оформленное Заявление предоставляется Работнику, осуществляющему сбор ПДн субъекта (Работнику Организации по работе с клиентами, в случае если Субъект ПДн является Клиентом Организации), который передает Заявление Ответственному за организацию обработки персональных данных в течение 2 рабочих дней с момента получения Заявления от Субъекта ПДн. Ответственный за обработкуперсональных данных,проверяет представленноеЗаявление и готовит запрашиваемую Субъектом ПДн информацию,в виде ответного письма за подписью Руководства Организациив срок не более 15 рабочих дней, в другом случае, в течение указанного срока, готовит мотивированный отказ.

После этого передает ответное письмов Секретариат, для почтовой отправки письма Субъекту ПДн. Срок отправки письма СекретариатОрганизации с момента его получения от Ответственного за организацию обработки персональных данных не более 3 рабочих дней.

В случае, если запрошенные сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления Субъекту ПДн по его запросу, Субъект ПДн вправе обратиться повторно в Организацию или направить повторный запрос в целях получения запрошенных сведений, и ознакомления с такими персональными данными не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса.

Субъект ПДн вправе обратиться повторно в Организацию или направить в Организацию повторный запрос в целях получения сведений, касающихся обработки его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными, не ранее чем через 30 дней после первоначального обращения, или по факту получения ответа на первоначальное обращение, и только в том случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Организация вправе отказать Субъекту ПДн в выполнении повторного запроса, в случае не соответствия перечисленным выше условиям. Такой отказ должен быть

мотивированным. Организация обязана предоставить Субъекту ПДн доказательства обоснованности отказа в выполнении повторного запроса.

Право Субъекта ПДн на доступ к его персональным данным, обрабатываемымОрганизацией, может быть ограничено в соответствии с федеральными законами, в том числе если:

– обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (в случае если Субъектом ПДнявляется Клиент Организации);

– доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

3.6 Обработка персональных данных Субъектов ПДнтретьим лицом

Организация вправе поручить обработку, в том числе передать, персональные данныеСубъекта ПДн третьему лицу, при этомдолжны соблюдаться следующие требования:

– передача ПДн третьим лицам возможна при согласии Субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (поручение Организации на обработку ПДн);

– лицо, осуществляющее обработку персональных данных по поручению Организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных»;

– в поручении Организации должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться третьим лицом, и цели обработки;

– в поручении Организации должна быть установлена обязанность третьего лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке.

В случае если Организация поручает обработку персональных данных Субъекта ПДнтретьему лицу, ответственность перед Субъектом персональных данных за действия указанного лица несет Организация. Лицо, осуществляющее обработку персональных данных по поручению Организации, несет ответственность перед Организацией.

Лицо, осуществляющее обработку персональных данных Субъекта ПДнпо поручению Организации, не обязано получать согласие Субъекта ПДн на обработку его персональных данных.

Регулирующие и надзорные органы могут иметь доступ к персональным данным Клиентов только на основании федерального закона и только в сфере своей компетенции.По факту получения запроса от регулирующих и надзорных органов на доступ к сведениям относящимся к обработке ПДн, Ответственный за обработкуПДн в ООО «Санаторий ПлазаСПА» готовит запрашиваемую информацию, в виде ответного письма за подписью Руководства Организациив срок установленный запросом. После этого передает ответное письмо в Секретариат, для почтовой отправки письма. Срок отправки письма канцелярией

Организации с момента его получения от Ответственного за организацию обработки персональных данных не более 3 рабочих дней.

4 АВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Автоматизированная обработка ПДн в Организацииосуществляется в рамках ИСПДн, представленных в «Перечне ИСПДнООО «Санаторий ПлазаСПА», подлежащих защите». При этом для каждой из ИСПДн документально определены:

- уровень защищенностиИСПДн;
- состав обрабатываемых ПДн;
- категория обрабатываемых ПДн;
- режим обработки ПДн;
- количество Субъектов ПДн;
- основание для обработки ПДн;
- состав программно-технических (аппаратных, программных и аппаратно-программных) средств ИСПДн;
- структурная схема ИСПДн;
- схема информационных потоков ИСПДн и роли;
- процесс обработки ПДн.

Для каждой ИСПДн должны быть выполнены требования системы обеспечения информационной безопасности Организации, сформированные на основании требований Законодательства РФ и документов Комплекса БР ИББС.

В связи с тем, что персональные данные чаще всего обрабатываются в совокупности с другими категориями защищаемой информации (например,коммерческойтайной), ковсем информационным системам Организации, перечисленным в «Перечне ИСПДнООО «Санаторий ПлазаСПА», в том числе и к ИСПДн, предъявляются общие требования по обеспечению информационной безопасности (включая требования, предъявляемые к ИСПДнсоответствующего класса), если иное не установлено внутренними нормативными документами Организации. Данные требования отражаются в соответствующих Положениях ООО « Санаторий ПлазаСПА».

Используемые технические средства защиты должны иметь сертификат соответствия ФСТЭК и ФСБ России на использование в ИСПДн, в соответствии с Моделью угроз и нарушителя ИБ и классом ИСПДн, определенным в «Перечне ИСПДнООО «Санаторий ПлазаСПА», подлежащих защите».

5.1 Особенностиавтоматизированной обработки персональных данных

Сбор ПДн, занесение данных в ИСПДн и дальнейшая деятельность по обработке и удалению ПДн проводится Работниками (пользователями ИСПДн), ответственными за данный вид деятельности согласно своим должностным обязанностям.При этом круг пользователей, эксплуатирующих программно-технические средства ИСПДн в процессе выполнения своих служебных обязанностей должен быть документально определен«Перечнем должностных лицОрганизации, допущенных к обработке ПДн»,согласованным с Работником ответственным

за организацию обработки персональных данных,и утвержденным Руководством Организации. Шаблон Перечня представлен в ПриложенииД настоящего документа. Обязанности по сопровождению ИСПДн возложены на Системного администратора, который назначается соответствующим приказом Руководства из числа Работников Инженерно-технической службы.

Обязанности по обеспечению ИБ ИСПДн возложены на Администратораинформационной безопасности, который назначается соответствующим приказом Руководства.

Пользователям ИСПДнОрганизации предоставляется право работать только с теми средствами и информационными ресурсамиИСПДн, которые необходимы им для выполнения своих установленных должностных обязанностей.

К автоматизированной обработке ПДн при помощи ИСПДн допускаются РаботникиОрганизации:

– прошедшие инструктаж о правилах пользования ИСПДн;

– прошедшие инструктаж о правилах обеспечения ИБ ИСПДн;

– подписавшие «Соглашение о неразглашении персональных данных Клиента»и/или «Соглашение о неразглашении персональных данных Работника»;

– ознакомившиеся под роспись с «Руководством пользователя ИСПДнООО «Санаторий ПлазаСПА»по ИБ».

Инструктаж о правилах пользования ИСПДн проводит Системный администратор. По результатам инструктажа делается запись в «Журнале инструктажа о правилах пользования ИСПДн», шаблон которого представлен в ПриложенииЕ.

Инструктаж о правилах обеспечения ИБ ИСПДнпроводит Администраторинформационной безопасности. По результатам инструктажа делается запись в «Журнале инструктажа о правилах обеспечения ИБ ИСПДн», шаблон которого представлен в ПриложенииК.

Инструктаж о правилах обеспечения ИБ ИСПДнпроводит Администраторинформационной безопасностиИСПДн.

Ответственность за обеспечение защиты информации в процессе эксплуатации средств вычислительной техники, предназначенных для обработки ПДн, возлагается на Пользователей, производящих ее обработку.

Любое лицо из числа ПользователейИСПДнОрганизации должно сообщать о ставшем ему известном факте нарушения или обхода СЗИ Администраторуинформационной безопасности и своему непосредственному Руководителю.

Доступ к программно-техническим средствам ИСПДнОрганизации должен быть персонифицирован: каждый Пользователь должен иметь и предъявлять при обращении к программно-техническим средствам ИСПДнОрганизации атрибуты безопасности, включающие уникальный идентификатор пользователя, пароль (пароли) и (или) аутентифицирующую

информацию. Атрибуты безопасности пользователя должны сохраняться им в тайне от посторонних лиц.

5.2 Требования по защите ИСПДн

Сопровождение СЗИ на стадии эксплуатации ИСПДнОрганизации, включая ведение служебной информации средств защиты от НСД (генерацию и смену паролей и ключей пользователей), оперативный контроль за функционированием системы защиты информации, контроль соответствия общесистемной программной среды эталону (контроль целостности программного обеспечения), настройку программных и программно-технических средств, создание замкнутой программной среды, а также контроль за ходом технологического процесса обработки информации путем регистрации и анализа действий пользователей по системному журналу, осуществляется Администратороминформационной безопасности (по штатному расписанию Организации - инженер-системный программист).

Настройка средств из состава системы защиты информации ИСПДнОрганизации осуществляется Администратороминформационной безопасности или Системным администратором (по штатному расписанию – администратор баз данных(под контролем Администратораинформационной безопасности,в соответствии с эксплуатационной документацией на средства из состава СЗИ ИСПДн.

В обязанности Системногоадминистратора входит учет, хранение и выдача пользователям персональных идентификаторов, съемных носителей информации, паролей и ключей для средств защиты информации от НСД.

При эксплуатации ИСПДн, к настройке и конфигурированию средств защиты информации из состава СЗИ ИСПДнОрганизации должен быть допущен Администратор информационной безопасности илиСистемный администратор под контролем Администратора информационной безопасности. Какие-либо другие лица к данным работам не допускаются.

В процессе обеспечения ИБ ИСПДн должны соблюдаться требования следующих документов, предъявляемыек защищаемой информации:

- Положения по управлению доступом ООО «Санаторий ПлазаСПА»;
- Положения по использованию СКЗИ ООО «Санаторий ПлазаСПА»;
- Положенияпо обеспечению антивирусной защиты ООО «Санаторий ПлазаСПА»;
- Положенияпо использованию корпоративной ЛВС ООО «Санаторий ПлазаСПА»;
- Положенияпо использованию ресурсов сети Интернет и электронной почты ООО «Санаторий ПлазаСПА»;
- Положенияпарольной защиты ООО «Санаторий ПлазаСПА»;
- Положениярезервного копирования и восстановления данных ООО «Санаторий ПлазаСПА»;
- Требования к системе защиты персональных данныхООО «Санаторий ПлазаСПА»;
- Руководства администратора ИБ ООО «Санаторий ПлазаСПА»;
- Руководства пользователя ИСПДнООО «Санаторий ПлазаСПА».

Программно-технические средства из состава ИСПДнОрганизациидолжны быть размещены в помещениях, расположенных в пределах контролируемой зоныОрганизации.

Помещения, в которых допускается размещение программно-технических средств ИСПДнОрганизации, должны отвечать требованиям пожарной и электробезопасности, надежно охраняться и иметь:

– прочные двери, оборудованные надежными запорами или кодовыми замками, а также приспособлениями для опечатывания или СКУД;

– сигнализацию, связанную с подразделением охраны или дежурным по подразделению.

Серверные комнаты, с устанавливаемыми в них телекоммуникационным оборудованием (серверами и средствами их управления, телекоммуникационным оборудованием) также должны удовлетворять вышеперечисленным требованиям, приэтом доступ в данные помещения должен иметь Администратор информационной безопасностии Системный администратор.

Каналы связи (между компонентами ИСПДнОрганизации), расположенные в пределах контролируемой зоны, должны прокладываться в кабель-каналах, препятствующих осуществлению несанкционированного к ним подключения.

Вход в помещения, в которых производится автоматизированная обработка ИСПДн, разрешается постоянно работающим в них пользователям ИСПДнОрганизации по списку, подписанному Руководством Организации по согласованию с Ответственным за организацию обработки персональных данных.

По окончании рабочего дня все помещения, в которых размещены программно-технические средства ИСПДнОрганизации, запираются и опечатываются. Также помещения должны запираться на ключ в случае временного отсутствия в них Пользователей ИСПДнОрганизации, ответственных за данные помещения, в частности, за установленные в данных помещениях программно-технические средства обработки защищаемой информации.

Корпуса, используемых в ИСПДнОрганизации программно-технических средств, опечатываются специальными саморазрушающимися наклейками. Администратор информационной безопасности должен осуществлять периодическую проверку целостности данных наклеек.

Регламентное обслуживание или устранение неисправности программно-технических средств из состава средств автоматизации ИСПДнОрганизации, проведение которого повлечет вскрытие данных средств с нарушением целостности специальных защитных наклеек, осуществляется в присутствии Администратора информационной безопасности.

Установка программного обеспечения ИСПДнОрганизациипроводится Системным администратором, под контролем Администратораинформационной безопасности. Дистрибутивы устанавливаемого программного обеспечения должны предварительно тестироваться и проверяться на наличие вредоносного кода.

При использовании в ИСПДн материальных носителей для организации функционирования ИСПДн должна обеспечиваться:

– защита от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы ПДн;

– возможность идентификации ИСПДн, в которую была осуществлена запись ПДн, а также Пользователя, осуществившего такую запись;

– невозможность несанкционированного доступа к ПДн, содержащимся на материальном носителе.

Ответственный работник за обработку ПДн ведет учет материальных носителей ПДн в «Журнале учета материальных носителей ИСПДн». Выдача материальных носителей ИСПДн пользователю осуществляется под роспись. Шаблон «Журнала учета материальных носителей ИСПДн» представлен в Приложении И.

Запрещается использовать материальный носитель по истечении срока эксплуатации, установленного изготовителем материального носителя.

В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к ПДн, то такая информация должна быть подписана электронной цифровой подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

Требования к уничтожению информации сматериальных носителей и самих носителейПДн определяются порядком удаления информации и уничтожения носителей «Руководства по эксплуатации СИБООО «Санаторий ПлазаСПА»».

Ответственность за уничтожение информации с носителей возлагается на пользователя ИСПДн, за уничтожение носителей информации – на Администратора информационной безопасности.

Администратор информационной безопасность должен инициировать создание Комитета по информационной безопасности. Комитет по информационной безопасности решает следующие задачи:

– решение вопросов по ИБ, в случае если для их решения необходимо привлечение структурных подразделений Организации;

– внесение изменений в организационно-распорядительную документацию, касающуюся деятельности структурных подразделений, не обеспечивающих информационную безопасность;

5 НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ВОРГАНИЗАЦИИ

В рамках бизнес-процессов ведется неавтоматизированная обработка ПДн. Неавтоматизированная обработка ПДн в Организации является вспомогательной деятельностью при организации процесса обработки ПДн в рамках ИСПДн.

Описание неавтоматизированной обработки ПДн приведено в «Отчете об информационном обследовании ООО «Санаторий ПлазаСПА», в разделе «ОписаниеИСПДнООО «Санаторий ПлазаСПА» в подразделах «Технологический процесс обработки».

Неавтоматизированная обработка ПДн в Организациизаключается в работес бумажными носителями информации, которые содержат сведения, составляющие ПДн (далее – бумажные носители ПДн), согласно «Перечню ИСПДнООО «Санаторий ПлазаСПА», подлежащих защите».

К бумажным носителям ПДнОрганизации относятся:

– Анкеты на бумажных носителях, получаемые от Клиентов и договоры(в т.ч. дополнительные соглашения к ним), заключаемые с Клиентом Организации.;

- Анкеты на бумажных носителях, получаемые от Работников и трудовые договоры(в т.ч. дополнительные соглашения к ним), заключаемые с Работником Организации.

6.1 Требования кнеавтоматизированной обработкеперсональных данных

В Организации установлены следующие требования к хранению бумажных носителей ПДн:

– срок хранения для бумажных носителей ПДн, устанавливается согласно «Перечню сведений, относящихся к защищаемой информации ООО «Санаторий ПлазаСПА», в зависимости от состава ПДн либо законодательством РФ;

– бумажные носители ПДн хранятся в специализированных шкафах или сейфах, при этом,соответствующим приказом РуководстваОрганизации, назначается Ответственный работникдля каждого Структурного подразделения Организации, в рамках которого согласно описанию технологического процесса представленного в «Отчете об информационном обследовании ООО «Санаторий ПлазаСПА», в разделе «Описаниенеавтоматизированной обработкиООО «Санаторий ПлазаСПА», происходит обработка бумажных носителей ПДн;

– запрещается хранение бумажных носителей ПДн в местах, доступных для ознакомления посторонними лицами;

– Работнику Организации выполняющему обработку ПДн с использованием бумажных носителей ПДн запрещается хранить их в месте, доступном для других лиц.

В Организации установлены следующие требования к уничтожению бумажных носителей ПДн:

– уничтожение бумажных носителей ПДн должно проводиться при помощи технических средств (уничтожителей бумаги), исключающих возможность полного или частичного восстановления данных носителей;

– ответственным за уничтожение бумажных носителей ПДн соответствующим приказом РуководстваОрганизациинаначается Работник,отвечающий за обработку персональных данных;

– уничтожение бумажных носителей ПДн должно оформляться актом.

К неавтоматизированной обработке ПДн допускаются Работники Организации:

– прошедшие инструктаж о правилах работы с бумажными носителями ПДн;

– прошедшие инструктаж о правилах обеспечения ИБ при работе с бумажными носителямиПДн;

– подписавшие «Соглашение о неразглашении персональных данных Клиента»и/или «Соглашение о неразглашении персональных данных Работника»;

– ознакомившиеся под роспись с «Руководством пользователя ИСПДнООО «Санаторий ПлазаСПА»».

Инструктаж проводит Администраторинформационной безопасности. По результатам инструктажа делается запись в «Журнале инструктажа о правилах пользованияИСПДн».

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

Для типовых форм бумажных носителей ПДн (анкет, договоров), характер информации в которых предполагает или допускает включение в них ПДн, в Организациидолжны соблюдаться следующие условия:

– типовая форма бумажного носителя ПДнили связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Организации, фамилию, имя, отчество и адрес Субъекта ПДн или РаботникаОрганизации, предоставляющих ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Организацией способов обработки ПДн;

– типовая форма бумажного носителя ПДндолжна предусматривать поле, в котором Субъект ПДн или РаботникОрганизации,предоставляющий ПДн, может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;

– типовая форма бумажного носителя ПДндолжна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

Уточнение персональных данных при осуществлении их неавтоматизированной обработки в Организациипроизводится путем обновления или изменения данных на бумажном носителеПДн, либо путем изготовления нового бумажного носителяПДн с уточненнымиПДн.

Неавтоматизированная обработка ПДн в Организациидолжна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения персональных данных (бумажных носителейПДн) и установить Работников Организации, осуществляющих неавтоматизированную обработку ПДн, либо имеющих к ним доступ.

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

6 ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Данное Положение вступает в силу с момента ееутверждения Учредителем либо лицом им уполномоченным, действует до выпуска новой версии или полностью аннулируется после выпуска соответствующего приказа.

Порядок внесения изменений в Положение:

– предложения по внесению изменений рассматриваются Комитетом по ИБ Организации и утверждаются Руководством Организации. Руководство Организации также имеет право единоличного внесения изменений, без рассмотрения их Комитетом по ИБ;

– все изменения являются обязательными для исполнения, и распространяются на Организацию после утверждения Руководством Организации целиком;

– устаревшие версии Положенияпередаются в архив Организации со сроком хранения не менее 5 лет.

7 ОТВЕТСТВЕННОСТЬ

Требования настоящегоПоложенияобязательны для выполнения всеми Работниками Организации согласно назначенным ролям и должностным обязанностям.

Работники Организации, нарушившие положения настоящего документа, привлекаются к дисциплинарной, гражданско-правовой и другой ответственности, установленной Законодательством Российской Федерации и/или условиями трудового соглашения (контракта).

Неправомерность деятельности Организации по сбору и использованию ПДн субъекта ПДн может быть установлена в судебном порядке.

Положение, в том числе предупреждение об ответственности, доводится до всех Работников Организации под роспись.

ПРИЛОЖЕНИЕ А. ШАБЛОН СОГЛАШЕНИЯ О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТА

Соглашение о неразглашении персональных данных Клиента

Я, _____, паспорт серии _____, номер _____, выданный _____ «____» _____ _____ года, подтверждаю, что, являясь Работником ООО «Санаторий ПлазаСПА», получаю доступ к персональным данным КлиентаОрганизации. Я также понимаю, что во время исполнения своих должностных обязанностей мне приходится заниматься обработкой персональных данных субъекта персональных данных.

Я понимаю, что разглашение информации, содержащей сведения, составляющие персональные данные Субъекта персональных данных, может нанести ущерб Субъекту персональных данных как прямой, так и косвенный.

В связи с этим даю обязательство при обработке персональных данных Субъекта персональных данных соблюдать все требования «Положения по обработке и защите персональных данных ООО «Санаторий ПлазаСПА».

Я подтверждаю, что не имею права разглашать сведения содержащие информацию, составляющую персональные данные Субъекта персональных данных, в частности:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета(при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном(персонифицированном) учете в системе обязательного пенсионного страхования;
- сведения о месте работы;
- занимаемая должность;
- телефон;
- № email;
- Сведения о расчетных счетах;
- номер полиса медицинского страхования лица(при наличии);
- анамнез;
- диагноз;

– сведения об организации, оказавшей медицинские услуги;

– вид оказанной медицинской помощи;

– условия оказания медицинской помощи;

– сроки оказания медицинской помощи;

– объем оказанной медицинской помощи;

– результат обращения за медицинской помощью;

– сведения об оказанных медицинских услугах;

– примененные стандарты медицинской помощи;

– сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу

- иные сведения, подпадающие под категорию персональных. Я предупрежден(-а) о том, что в случае разглашения мной сведений, касающихся персональных данных Субъекта персональных данных или их утраты, я несу ответственность в соответствии с действующим Законодательством.

С «Положением по обработке и защите персональных данных ООО «Санаторий ПлазаСПА»» ознакомлен(-а).

«____» _____ 201__ г. _____

ПРИЛОЖЕНИЕ Б. ШАБЛОН СОГЛАШЕНИЯ О НЕРЗГЛАШЕНИИПЕРСОНАЛЬНЫХ ДАННЫХРАБОТНИКА

Соглашение о неразглашении персональных данных Работника

Я, _____, паспорт серии _____, номер _____, выданный _____ «____» _____ _____ года, подтверждаю, что, являясь Работником ООО «Санаторий ПлазаСПА», получаю доступ к персональным данным Работников Организации. Я также понимаю, что во время исполнения своих должностных обязанностей мне приходится заниматься обработкой персональных данных Работников Организации.

Я понимаю, что разглашение информации, содержащей сведения, составляющие персональные данные Работников Организации, может нанести ущерб Работникам Организации как прямой, так и косвенный.

В связи с этим даю обязательство при обработке персональных данных Работника соблюдать все требования «Положения по обработке и защите персональных данных ООО «Санаторий ПлазаСПА».

Я подтверждаю, что не имею права разглашать сведения содержащие информацию, составляющую персональные данные Работника, в частности:

– фамилия, имя, отчество, в том числе прежние (дата, место и причина изменения);
– дата рождения (число, месяц, год);
– место рождения;
– пол;
– гражданство;
– адрес и дата регистрации;
– адрес проживания;
– паспортные данные (серия, номер паспорта, кем и когда выдан);
– семейное положение и состав семьи (степень родства, фамилия, имя, отчество и дата рождения близких родственников);
– сведения о заработной плате и иных доходах;
– подразделение;
– должность;
– номер телефона (мобильный, домашний);
– адрес электронной почты;
– ИНН;
– номер страхового свидетельства Пенсионного Фонда;
– информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
– информация о приеме на работу (наименования предприятия, подразделение, должность, перемещения по должности, увольнения);

– результаты обязательных предварительных(при поступлении на работу) и периодических медицинских осмотров(обследований);

– наличие (отсутствие) судимости;

– информация о трудовом стаже (место работы, должность, период работы);

– данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, изменения к трудовому договору);

– информация об отпусках;

– сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета).

– имущественное положение;

– информация о доходах;

– реквизиты банковского счета;

– медицинское заключение о тяжести повреждения здоровья;

– сведения об инвалидности;

– сведения, содержащиеся в листке временной нетрудоспособности;

– государственные награды, иные награды и знаки отличия(кем награжден и когда);

– биометрические данные;

– место работы или учебы членов семьи и родственников;

– характер взаимоотношений в семье;

– содержание трудового договора;

– подлинники и копии приказов по личному составу;

– личные дела и трудовые книжки сотрудников;

– основания к приказам по личному составу;

– дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

– копии отчетов, направляемые в контролирующие органы.

Я предупрежден(-а) о том, что в случае разглашения мной сведений, касающихся персональных данных Работника Организации или их утраты, я несу ответственность в соответствии с действующим Законодательством.

С «Положением по обработке и защите персональных данных ООО «Санаторий ПлазаСПА» ознакомлен(-а).

«____» _____ 201__ г. _____

ПРИЛОЖЕНИЕ В. ШАБЛОН СОГЛАСИЯ СУБЪЕКТА ПДн (Клиента) НА ОБРАБОТКУ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласие Субъекта ПДнна обработку персональных данных

Я, _____, проживающий(-ая) по адресу _____паспорт серии _____, номер _____, выданный _____ «____» _____ _____ года, подтверждаю, что даю согласие ООО «Санаторий ПлазаСПА», на автоматизированную и неавтоматизированную обработку (сбор, систематизацию, хранение, накопление, уточнение (обновление, изменение), использование, блокирование, обезличивание, уничтожение, распространение (в том числе передачу, трансграничную передачу) с передачей как по внутренней сети ООО «Санаторий ПлазаСПА», так и с передачей по сетям связи общего пользования (Интернет), а также на совершение иных действий, в соответствии с законодательством Российской Федерации моих персональных данных:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета(при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном(персонифицированном) учете в системе обязательного пенсионного страхования;
- сведения о месте работы;
- занимаемая должность;
- телефон;
- № email;
- Сведения о расчетных счетах;
- номер полиса медицинского страхования лица(при наличии);
- анамнез;
- диагноз;
- сведения об организации, оказавшей медицинские услуги;
- вид оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объем оказанной медицинской помощи;

– результат обращения за медицинской помощью;

– сведения об оказанных медицинских услугах;

– примененные стандарты медицинской помощи;

– сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу;

ООО «Санаторий ПлазаСПА» также предоставлено право на получение информации и документов от третьих лиц для осуществления проверки достоверности и полноты информации обо мне.

Обработка персональных данных осуществляется с применением следующих основных способов: фиксирование, составление перечней на бумажном и электронном носителе, запись на электронные носители, хранение бумажных и электронных носителей, содержащих персональные данные, а также иные способы обработки

Персональные данные хранятся ООО «Санаторий ПлазаСПА» в течение сроков хранения, установленных законодательством Российской Федерации. Обработка персональных данных (за исключением хранения) прекращается по достижении цели обработки и прекращения обязательств по заключенным договорам и соглашениям.

Настоящее согласие может быть отозвано мною путем направления соответствующего уведомления вООО «Санаторий ПлазаСПА».

Настоящее согласие дается до истечения сроков хранения персональных данных либо до момента его отзыва мной в письменной форме, в этом случае ООО «Санаторий ПлазаСПА» прекращает обработку персональных данных, а персональные данные подлежат уничтожению не позднее срока договора, заключенного с ООО «Санаторий ПлазаСПА», а по его истечении – в течение срока, определяемого действующим Законодательством Российской Федерации и внутренними документами ООО «Санаторий ПлазаСПА».

«____» _____ 201__ г. _____

ПРИЛОЖЕНИЕ Г. ШАБЛОН СОГЛАСИЯ СУБЪЕКТА ПДн (Работника) НА ОБРАБОТКУ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласие Субъекта ПДн на обработку персональных данных

Я, _____
(фамилия, имя, отчество)
проживающий по адресу: _____
(адрес места жительства)

Документ, удостоверяющий личность _____ _____, выданный _____
(тип документа) (серия номер) (дата выдачи)

_____
(сведения о выдавшем органе)
даю согласие Оператору персональных данных – ООО «Санаторий ПлазаСПА», находящемуся по адресу: Ставропольский край, г. Железноводск, ул. Калинина,12-14;

а) на обработку моих персональных данных в целях:

– формирования общедоступных справочников ООО «Санаторий ПлазаСПА»;

– б) на передачу моих персональных данных организациям - третьим лицам в целях:

– для представления информации в различные контролирующие органы в соответствии с требованиями законов и нормативных актов РФ.

– Перечень моих персональных данных, в отношении которых оформлено данное согласие:

– фамилия, имя, отчество, в том числе прежние (дата, место и причина изменения);

– дата рождения (число, месяц, год);

– место рождения;

– пол;

– гражданство;

– адрес и дата регистрации;

– адрес проживания;

– паспортные данные (серия, номер паспорта, кем и когда выдан);

– семейное положение и состав семьи (степень родства,фамилия, имя, отчество и дата рождения близких родственников);

– сведения о заработной плате и иных доходах;

– подразделение;

– должность;

– номер телефона (мобильный, домашний);

– адрес электронной почты;

– ИНН;

– номер страхового свидетельства Пенсионного Фонда;

– информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

– информация о приеме на работу (наименования предприятия, подразделение, должность, перемещения по должности, увольнения);

– результаты обязательных предварительных(при поступлении на работу) и периодических медицинских осмотров(обследований);

– наличие (отсутствие) судимости;

– информация о трудовом стаже (место работы, должность, период работы);

– данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, изменения к трудовому договору);

– информация об отпусках;

– сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета).

– имущественное положение;

– информация о доходах;

– реквизиты банковского счета;

– медицинское заключение о тяжести повреждения здоровья;

– сведения об инвалидности;

– сведения, содержащиеся в листке временной нетрудоспособности;

– государственные награды, иные награды и знаки отличия(кем награжден и когда);

– биометрические данные;

К моим персональным данным имеют доступ:

– работникиООО «Санаторий ПлазаСПА», имеющие доступ к персональным данным согласно Положения по обработке и защите персональных данных ООО « Санаторий ПлазаСПА»;

– сотрудники Федеральной Налоговой Службы России, Пенсионного Фонда РФ, Фонда социального страхования РФ, страховых компаний;

Действия с моими персональными данными в процессе их обработки включают в себя:

– сбор;

– запись;

– систематизацию;

– накопление;

– хранение;

– уточнение (обновление, изменение);

– извлечение;

– использование;

– передачу (предоставление, доступ);

– блокирование;

– удаление;

– уничтожение.

– Мои персональные данные обрабатываются:

– с использованием средств автоматизации и без использования таких средств;

– с передачей по сетям связи общего доступа.

Персональные данные обрабатываются и хранятся в ООО «Санаторий ПлазаСПА» в течение сроков хранения, установленных законодательством Российской Федерации.). Настоящее согласие действует до истечения сроков хранения персональных данных либо до момента его отзыва мной в письменной форме.

Отзыв моего согласия осуществляется посредством направления Оператору письменного запроса. В случае отзыва моего согласия Оператор вправе продолжить обработку моих персональных данных при наличии следующих оснований:

– обработка персональных данных необходима для достижения целей, предусмотренных законом Российской Федерации или, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

С Положением по обработке и защите персональных данных ООО « Санаторий ПлазаСПА» ознакомлен(а)

_____ _____

(дата подписания) (подпись)

ПРИЛОЖЕНИЕ Д. ШАБЛОН ЗАЯВЛЕНИЕ НА ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ, СВЯЗАННОЙ С ОБРАБОТКОЙПЕРСОНАЛЬНЫХ ДАННЫХ

Заявление на предоставление информации, связанной с обработкой персональных данных ООО «Санаторий ПлазаСПА»

Я, _____, паспорт серии _____, номер _____, выданный _____ «____» _____ _____ года, являясь КлиентомООО «Санаторий ПлазаСПА», прошу предоставить следующую информацию, связанную с обработкой моих ПДн вООО «Санаторий ПлазаСПА»:
_____
_____
_____
_____
_____
_____

Обоснованиезапроса _____
_____
_____
_____

«____» _____ 201__ г. _____

ПРИЛОЖЕНИЕ Е. ШАБЛОН ПЕРЕЧНЯ ДОЛЖНОСТНЫХ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

УТВЕРЖДАЮ:

Генеральный директор

ООО «Санаторий ПлазаСПА»

_____ В.Н. Григорьян

«» 2014 г

Перечень должностных лиц, допущенных к обработке персональных данных

ФИО	Должность

ПРИЛОЖЕНИЕ Ж. ШАБЛОН ЖУРНАЛА ИНСТРУКТАЖА О ПРАВИЛАХ ПОЛЬЗОВАНИЯ ИСПДн

Журнал инструктажа о правилах пользования ИСПДн

ФИОинструктируемого	Должностьинструктируемого	Дата проведения инструктажа	Подпись инструктируемого	ФИОинструктирующего	Должностьинструктирующего	Подпись инструктирующего

ПРИЛОЖЕНИЕ 3. ШАБЛОН ЖУРНАЛА ИНСТРУКТАЖА О ПРАВИЛАХ ОБЕСПЕЧЕНИЯ ИБ ИСПДн

Журнал инструктажа о правилах обеспечения ИБ ИСПДн

ФИОинструктируемого	Должностьинструктируемого	Дата проведения инструктажа	Подпись инструктируемого	ФИОинструктирующего	Должностьинструктирующего	Подпись инструктирующего

ПРИЛОЖЕНИЕ И. ШАБЛОН ЖУРНАЛА УЧЕТА МАТЕРИАЛЬНЫХ НОСИТЕЛЕЙ ИСПДн

Журнал учета материальных носителей ПДн

№ п/п	Учетный номер носителя	Тип носителя	Дата выдачи носителя	Ф.И.О. и подпись Администратора информационной безопасности	Ф.И.О. и подпись лица получившего носитель	Примечание