«УТВЕРЖДЕНО»
Приказом № 81 от 25.10.2017 года
Генерального директора
ООО «Санаторий «Изумрудный»
Староверовой Н.Ю.

ПОЛОЖЕНИЕ
о защите персональных данных
ООО «Санаторий «Изумрудный»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение о защите персональных данных в ООО «Санаторий «Изумрудный» устанавливает единый порядок обработки персональных данных в санатории «Изумрудный» (далее — санаторий).

2. Обработка персональных данных в санатории осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), настоящим Положением и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящем Положении, применяются в том же значении, что и в Федеральном законе № 152-ФЗ.

4. Целью настоящего Положения является обеспечение защиты персональных данных граждан от несанкционированного доступа, неправомерного их использования или утраты.

5. Настоящее Положение устанавливает и определяет:

1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;

2) цели обработки персональных данных;

3) содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) сроки обработки и хранения обрабатываемых персональных данных;

6) порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

6. Основные условия обработки персональных данных:

6.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных, а именно:

1) после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных пунктами 2-7, 9-11 части 1 статьи 6 Федерального закона № 152-ФЗ;

2) после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Краснодарскому

краю, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона № 152-ФЗ.

6.2. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации.

II. ПРОЦЕДУРЫ, НАПРАВЛЕННЫЕ НА ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации:

1.1. Информационные ресурсы, содержащие персональные данные, созданные, приобретенные, накопленные в санатории, а также полученные путем иных установленных законом способов, являются собственностью санатория и не могут быть использованы иначе, как с разрешения директора или в установленных законом случаях.

1.2. К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

1) назначение ответственных за организацию обработки персональных данных в санатории;

2) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона № 152-ФЗ;

3) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

4) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и настоящим Положением;

запрет на обработку персональных данных лицами, не допущенными к их обработке;

запрет на обработку персональных данных под диктовку.

1.3. Документы, определяющие политику оператора в отношении обработки персональных данных, подлежат обязательному опубликованию.

1.4. За разглашение информации, содержащей персональные данные, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима зашиты, обработки и порядка использования этой информации, работник может быть привлечен к дисциплинарной или иной ответственности, предусмотренной действующим законодательством.

2. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации:

2.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации санатория осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

2.2. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

к работе допускаются только лица, назначенные соответствующим приказом санатория;

на персональных электронных вычислительных машинах (далее - ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы).

2.3. Руководители подразделений санатория, работники санатория (пользователи информации) обязаны контролировать и выполнять предусмотренные в санатории меры по защите информации, содержащей персональные данные.

2.4. Руководители подразделений санатория обязаны:

участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ подразделения;

готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе санатория;

контролировать целевое использование работниками ресурсов информационно-телекоммуникационной сети «Интернет»;

контролировать выполнение пользователями общих правил работы на ПЭВМ и в локальной вычислительной сети санатория (далее - ЛВС);

выборочно контролировать характер исходящей информации, направляемой пользователями по электронной почте другим адресатам и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;

при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить директору и поставить в известность специалиста по кадрам;

инициировать служебные расследования по фактам разглашения информации, содержащей персональные данные, или утери документов, содержащих такую информацию, по фактам нарушений пользователями правил, установленных для работы с персональными данными в ЛВС, а также нарушений требований по защите информации;

обеспечивать условия для работы специалистов по защите информации при проверке в подразделении эффективности предусмотренных мер защиты информации.

2.5. При приеме на работу работник предупреждается об ответственности за разглашение сведений, содержащих персональные данные, которые станут ему известными в связи с предстоящим выполнением своих служебных обязанностей.

2.6. Пользователь обязан:

знать правила работы в ЛВС и принятые меры по защите ресурсов ЛВС (в части, его касающейся);

при работе на своей рабочей станции (ПЭВМ) и в ЛВС выполнять только служебные задания;

перед началом работы на ПЭВМ проверить свои рабочие папки на жестком диске, а также на внешних носителях информации с помощью штатных средств антивирусной защиты, убедиться в исправности;

при сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить программисту и своему непосредственному начальнику;

при необходимости использования внешних носителей информации, поступивших из других подразделений, учреждений, предприятий и организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов;

выполнять предписания программиста;

представлять для контроля свою рабочую станцию (ПЭВМ) руководителю подразделения и программисту;

сохранять в тайне свой индивидуальный пароль, периодически изменять его и не сообщать другим лицам;

вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить программисту и поставить в известность руководителя подразделения.

Пользователю при работе запрещается:

играть в компьютерные игры;

приносить различные компьютерные программы и пытаться установить их на локальный диск компьютера без уведомления программиста;

перенастраивать программное обеспечение компьютера;

самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);

запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме установленных программистом;

оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), внешние носители информации и распечатки, содержащие персональные данные;

допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;

работать на рабочей станции сети с информацией, содержащей персональные данные, при обнаружении неисправностей станции;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;

отсылать по электронной почте информацию личного или коммерческого характера для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с руководителем подразделения;

запрашивать и получать из информационно-телекоммуникационной сети «Интернет» материалы развлекательного характера (игры, клипы и т.д.);

запрашивать и получать из информационно-телекоммуникационной сети «Интернет» программные продукты, кроме случаев, связанных со служебной необходимостью. При этом необходимо согласование с руководителем своего подразделения и программистом;

входить в другие компьютерные системы через сеть без разрешения программиста.

2.7. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения служебных обязанностей.

3. Порядок обработки персональных данных без использования средств автоматизации:

3.1.Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых, заведомо несовместимы;

персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

3.4. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

3.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться

способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных - осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

при необходимости уничтожения или блокирования части персональных данных - уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3.8. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

3.9. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

III. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Целью обработки персональных данных является:

1) Осуществление возложенных на санаторий федеральным законодательством, Уставом ООО «Санаторий «Изумрудный» и нормативно-правовыми актами Министерства здравоохранения Российской Федерации полномочий и обязанностей по оказанию санаторно-курортной медицинской помощи;

2) организация деятельности санатория для обеспечения соблюдения законов и иных нормативных правовых актов, реализации права на труд, права на пенсионное обеспечение и медицинское страхование работников санатория.

IV. СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. К персональным данным, обрабатываемым для достижения целей, указанных в подпункте 1 пункта 1 Раздела III настоящего Положения (осуществление функций, полномочий и обязанностей по решению вопросов установленной сферы деятельности) относятся:

1) фамилия, имя, отчество (последнее – при наличии);
2) пол;
3) дата рождения;
4) место рождения;
5) гражданство;
6) данные документа, удостоверяющего личность;
7) место жительства;
8) место регистрации;
9) дата регистрации;
10) страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
11) номер полиса обязательного медицинского страхования застрахованного лица (при наличии);
12) анамнез;
13) диагноз;
14) сведения об организации, оказавшей медицинские услуги;
15) вид оказанной медицинской помощи;
16) условия оказания медицинской помощи;
17) сроки оказания медицинской помощи;
18) объем оказанной медицинской помощи;
19) результат обращения за медицинской помощью;
20) серия, номер выданного листка нетрудоспособности (при наличии);
21) сведения об оказанных медицинских услугах;
22) примененные стандарты медицинской помощи;
23) сведения о состоянии здоровья;
24) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу;
25) степень родства, фамилия, имя, отчество (при наличии), дата и место рождения несовершеннолетнего или недееспособного лица, в отношении которого субъект персональных данных является представителем (законным представителем);
26) номер сотового, домашнего и рабочего телефонов;
27) адрес электронной почты;
28) идентификационный номер налогоплательщика (ИНН);

29) другие сведения, относящиеся к субъекту персональных данных, необходимые оператору в целях оказания санаторно-курортной медицинской помощи.

2. К персональным данным, обрабатываемым для достижения целей, указанные в подпункте 2 пункта 1 Раздела III настоящего Положения (организация деятельности санатория для обеспечения соблюдения законов и иных нормативных правовых актов, реализации права на труд, права на пенсионное обеспечение и медицинское страхование работников санатория) относятся:

1) анкетные и биографические данные гражданина, включая адрес места жительства и проживания, контактный (сотовый) телефон;

2) паспортные данные или данные иного документа, удостоверяющего личность и гражданство (включая серию, номер, дату выдачи, наименование органа, выдавшего документ);

3) сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (включая серию, номер, дату выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, дату начала и завершения обучения);

4) сведения о трудовой деятельности, опыте работы, занимаемой должности, трудовом стаже, повышении квалификации и переподготовках;

5) сведения о номере, серии, дате выдачи трудовой книжки (вкладыша в неё) и записях в ней, содержание и реквизиты трудового договора (контракта);

6) сведения о составе семьи и наличии иждивенцев, их месте работы или учебы;

7) сведения и заключения о состоянии здоровья установленной формы;

8) сведения об отношении к воинской обязанности;

9) сведения о доходах и обязательствах имущественного характера, в том числе супруги (супруга) и несовершеннолетних детей;

10) сведения об идентификационном номере налогоплательщика;

11) сведения о социальных льготах и о социальном статусе;

12) сведения о страховом полисе обязательного (добровольного) медицинского страхования;

13) сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

14) реквизиты банковского счета;

15) другие сведения, относящиеся к субъекту персональных данных, необходимые оператору в целях соблюдения трудового законодательства.

V. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ

1. К субъектам, персональные данные которых обрабатываются, относятся:

1) сотрудники санатория;

2) пациенты санатория;

3) лица, подавшие заявку на бронирование установленной формы.

VI. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Сроки обработки и хранения персональных данных определяются:

1) Приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;

2) сроком исковой давности;

3) иными требованиями законодательства Российской Федерации, нормативными правовыми актами санатория.

2. Особенности хранения персональных данных:

Если срок хранения персональных данных не установлен законодательством Российской Федерации, нормативными правовыми актами санатория, то хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

VII. ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных, или в результате которых уничтожаются материальные носители персональных данных.

2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3. Порядок уничтожения обработанных персональных данных:

Уничтожению подлежат утратившие практическое значение и не имеющие исторической или иной ценности носители информации, содержащие персональные данные. При уничтожении таких носителей должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

Уничтожение производится путем сожжения, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение документов путем измельчения в бумажную сечку. Внешние носители информации и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность их восстановления.

Уничтожение обработанных персональных данных производится комиссией, с составлением соответствующего акта. Состав комиссии назначается приказом директора. В комиссию назначаются лица, допущенные к

работе с персональными данными и являющиеся экспертами в различных областях деятельности санатория, имеющие непосредственное отношение к уничтожаемым материалам.

На документальные материалы, отобранные комиссией для уничтожения, составляется акт об уничтожении документов, который подписывается членами комиссии и утверждается директором.

Отобранные и включенные в акт об уничтожении документальные материалы после их сверки членами комиссии хранятся отдельно от других материалов.

Уничтожение документальных материалов, до утверждения акта об уничтожении документов директором, запрещается.

Уничтожение должно производиться в возможно короткий срок после утверждения директором акта об уничтожении документов.

Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики, проекты документов и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта входит проведение следующих мероприятий:

разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя и руководителя подразделения, допущенных к обработке персональных данных;

накапливание остатков носителей в опечатываемом ящике (урне);

физическое уничтожение остатков носителей несколькими сотрудниками подразделения, допущенными к работе с персональными данными;

внесение отметок об уничтожении в учетные формы документов и носителей.
