Политика обработки и защиты персональных данных

ПОЛИТИКА ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ «САНАТОРИЙ «КРЕПОСТЬ»

1. Общие положения

1.1. Настоящий документ определяет политику Филиала АО «Корпорация «Тактическое ракетное вооружение» «Санаторий «Крепость» (далее - «Санаторий «КРЕПОСТЬ» либо Организация) в отношении обработки персональных данных (далее - ПД).

1.2. Настоящая Политика в отношении обработки персональных данных (далее - Политика) составлена в соответствии с пунктом 2 статьи 18.1 Закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и является основополагающим внутренним регулятивным документом, определяющим ключевые направления его деятельности в области обработки и защиты персональных данных, оператором которых является Организация.

1.3. Настоящая Политика действует в отношении всех персональных данных, обрабатываемых в Организации, которые могут быть получены как от физического или юридического лица (контрагента), состоящего в договорных отношениях с Организацией, так и от субъекта персональных данных, состоящего с Организацией в отношениях, регулируемых трудовым законодательством (далее - работника).

1.4. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.5. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Организацией 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 ПД, полученных до ее утверждения.

Обеспечение безопасности персональных данных, законности и справедливости их обработки является одной из приоритетных задач Санатория.

1.6 Политика является общедоступным документом, декларирующим концептуальные основы деятельности Санатория при обработке

персональных данных, и подлежит опубликованию на официальном сайте Санатория в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет)

1.7. Понятия и термины, используемые в настоящей Политике, применяются в значениях, установленных Федеральным законом.

1.8. Настоящая Политика может быть дополнена либо изменена. Изменения в Политику вносятся на основании приказов директора Санатория и при изменении нормативно-правовых актов.

1.9. Обработка ПД в Организации осуществляется в связи с выполнением функций, предусмотренных учредительными документами и определяемых:

Конституция Российской Федерации;

Трудовой кодекс Российской Федерации;

Налоговый кодекс Российской Федерации

Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и принятые в соответствии с ним нормативные правовые акты Российской Федерации;

Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и принятые в соответствии с ним нормативные правовые акты Российской Федерации;

Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; постановление Госкомстата России от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;

Приказ Минздрава России от 05.05.2016 № 279н «Об утверждении Порядка организации санаторно-курортного лечения».

Законом от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

Постановлением Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

иными нормативными правовыми актами Российской Федерации.

1.10. Основные понятия.

персональные данные - 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 персональных данных, оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) 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 средств вычислительной техники;

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

пациент (гость, отдыхающий, представитель отдыхающего, работник) - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

медицинская деятельность - профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях;

лечащий врач - врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

1.8. Субъекты персональных данных имеют право:

на полную информацию о персональных данных;

доступ к своим персональным данным;

предоставление сведений о наличии персональных данных в доступной форме.

1.9. Политика распространяется на персональные данные, полученные как до, так и после утверждения настоящей Политики.

1.10. Политика обязательна для ознакомления лицами, передающими в Организацию персональные данные.

1.11. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции.

1.12. Действующая редакция хранится в месте нахождения Организации по адресу: 357700, Ставропольский край, г. Кисловодск, пр. Мира, 9, электронная версия Политики - на сайте по адресу: https://kmvfort.ru/

2. Цели сбора персональных данных.

2.1. Обработка ПД в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

2.2. Персональные данные обрабатываются Организацией в следующих целях:

2.2.1. Осуществление и выполнение возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей, в частности:

выполнение требований законодательства в сфере труда и налогообложения;

трудоустройства и оформления трудовых отношений;

получения работниками образования и продвижения по службе; контроля качества выполняемой работы;

обеспечения безопасности сотрудников и сохранности имущества;

предоставления работникам гарантий и компенсаций в соответствии с законодательством;

ведение текущего бухгалтерского и налогового учёта, формирование, изготовление и своевременная подача бухгалтерской, налоговой и статистической отчётности;

обеспечение оказания гражданам медицинской помощи, организация и проведение санаторно-курортного лечения и лечебного питания, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации»;

выполнение требований законодательства по определению порядка обработки и защиты ПД граждан, являющихся клиентами или контрагентами Организации (далее - субъекты персональных данных).

2.2.2. Осуществления прав и законных интересов Организации в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Организации, или третьих лиц либо достижения общественно значимых целей;

2.2.3. В иных законных целях.

3. Правовые основания обработки персональных данных.

3.1. Организация обрабатывает персональные данные работников и отдыхающих в соответствии с:

Трудовым кодексом Российской Федерации;

Гражданским кодексом Российской Федерации;

Налоговым кодексом Российской Федерации;

Федеральным законом от 24 июля 2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;

Федеральным законом от 15 декабря 2001 г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации»;

Федеральным законом от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств»;

Федеральным законом от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации»;

Приказом Министра внутренних дел Российской Федерации от 29 декабря 2016 г. №925 «О некоторых вопросах обработки персональных данных в МВД России»;

Уставом организации;

Положением об обработке и защите персональных данных работников Организации;

трудовыми договорами, договорами о материальной ответственности, ученическими договорами, которые Организация заключает с работниками;

согласием работников и отдыхающих на обработку персональных данных;

обязательством о неразглашении конфиденциальной информации.

4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. В Организации обрабатываются ПД следующих субъектов: физические лица, состоящие с Организацией в трудовых отношениях; физические лица, являющие близкими родственниками работников Организации;

физические лица, уволившиеся из Организации;

физические лица, являющиеся кандидатами на работу;

физические лица, состоящие с Организацией в гражданско-правовых отношениях;

физические лица, являющиеся клиентами или контрагентами Организации;

физические лица, являющиеся представителями или работниками клиентов или контрагентов юридических лиц;

физические лица, обратившиеся в Организацию за медицинской помощью или находящиеся на санаторно-курортном лечении.

4.2. Организация обрабатывает любые персональные данные работников, бывших работников, кандидатов на замещение вакантных должностей, а также родственников работников в целях трудовых отношений. Исключение составляют персональные данные специальных категорий:

о состоянии здоровья, если это не связано с выполнением работы;

расовой и национальной принадлежности;

политических взглядах;

религиозных или философских убеждениях;

интимной и частной жизни.

4.3. Организация обрабатывает любые персональные данные отдыхающих в целях организации и проведения санаторно-курортного лечения и бывших отдыхающих, закончивших санаторно-курортное лечение. Исключение составляют персональные данные специальных категорий:

расовой и национальной принадлежности;

политических взглядах;

религиозных или философских убеждениях;

судимости.

4.4. Организация обрабатывает следующие персональные данные физических лиц, являющихся клиентами или контрагентами Организации, и физических лиц, являющихся представителями или работниками клиентов или контрагентов юридических лиц:

фамилия, имя, отчество;

паспортные данные;

занимаемая должность или выполняемая работа;

сведения о юридическом лице;

сведения об индивидуальном предпринимателе;

4.5. Обрабатываемая информация о субъектах, указанных в п.п. 4.2-4.4, является конфиденциальной.

5. Порядок и условия обработки персональных данных.

5.1. В Организации создана система конфиденциального делопроизводства. Система обеспечивает создание, движение и хранение документов работников и отдыхающих и иных документов, содержащих персональные данные таким образом, чтобы исключить несанкционированное использование этих сведений.

5.2. Организация в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона 152-ФЗ «О персональных данных».

5.3. Организация не осуществляет обработку биометрических персональных данных в целях определения личности (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).

5.4. Организация не выполняет обработку специальных категорий персональных данных работников, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

5.5. Организация не выполняет обработку специальных категорий персональных данных отдыхающих, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений.

5.6. Организация не производит трансграничную (на территорию иностранного государства органу власти иностранного государства иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

5.7. Организация производит передачу персональных данных третьим лицам на основании соответствующего соглашения и только с согласия субъектов персональных данных.

5.8. Организацией созданы общедоступные источники персональных данных (справочники, адресные книги). Персональные данные, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес,

абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта персональных данных.

5.9. Доступ к персональным данным в Организации имеют только те специалисты, кому это необходимо для исполнения должностных обязанностей и в соответствии с требованиями внутренних регулятивных документов Организации.

5.10. Работники, получающие доступ к персональным данным, определены в Положении об обработке и защите персональных данных субъектов персональных данных Организации.

5.11. Допущенные к обработке ПД работники под подпись знакомятся с документами Организации, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных работников.

5.12. Права, обязанности и ответственность работников, обрабатывающих персональные данные в Организации, закрепляются в их трудовых договорах и должностных инструкциях.

5.13. За нарушение правил обработки и хранения персональных данных, ставших им известными по работе, работники Организации привлекаются к дисциплинарной ответственности.

5.14. Обработка персональных данных в Организации ведется как с использованием средств автоматизации, так и без использования средств автоматизации.

5.15. Обработка персональных данных осуществляется:

с согласия субъекта персональных данных на обработку его персональных данных;

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

в случаях, когда 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).

5.16. Все персональные данные Организация получает только у субъекта персональных данных.

5.17. В случае, когда персональные данные можно получить у третьих лиц, это делается исключительно с письменного согласия субъекта.

5.18. В случаях, предусмотренных законом, Организация обрабатывает персональные данные без специального согласия на то субъекта персональных данных.

5.19. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Организация в ходе своей деятельности предоставляет персональные данные следующим организациям:

Федеральной налоговой службе;

отделению Пенсионного фонда РФ; территориальному Фонду социального страхования;

территориальному Фонду обязательного медицинского страхования;

страховым медицинским организациям по обязательному и добровольному медицинскому страхованию;

банкам для начисления заработной платы;

судебным и правоохранительным органам в случаях, установленных законодательством;

участникам системы межведомственного электронного взаимодействия;

негосударственным пенсионным фондам;

бюро кредитных историй с (согласия субъекта);

юридическим компаниям, работающим в рамках законодательства РФ, при неисполнении обязательств по договору займа с (согласия субъекта).

5.20. Организация не поручает обработку персональных данных другим лицам на основании договора.

5.21. Организация вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.22. В остальных ситуациях Организация предлагает субъекту оформить персональное и конкретное письменное согласие на обработку персональных данных или их передачу третьим лицам.

5.23. Субъект персональных данных может в любой момент отозвать свое согласие на обработку сведений по письменному заявлению.

5.24. Организация хранит персональные данные в рамках конфиденциального делопроизводства в порядке, исключающем их утрату или неправомерное использование.

5.25. При достижении целей обработки Организация уничтожает персональные данные. Исключения составляют:

персональные данные, которые должны храниться длительное время в силу требований нормативных правовых актов;

если кандидат на работу желает остаться в кадровом резерве.

5.26. Организация передает персональные данные в порядке, установленном законодательством. Персональные данные передаются только с письменного согласия субъекта, за исключением случаев, предусмотренных законом.

5.27. В Организации соблюдаются требования конфиденциальности персональных данных. Работники, получившие доступ к персональным данным, дают обязательство не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.28. Организация обеспечивает неограниченный доступ к документу, определяющему ее политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

5.29. Организация при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.30. Хранение персональных данных в Организации осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.31. Остальные персональные данные хранятся в Организации в соответствии со сроками хранения архивных документов, указанных в приказе Министра культуры Российской Федерации от 25.08.2010 г. № 558 «Об утверждении «перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

5.32. При обработке персональных данных без использования средств автоматизации хранение документов, содержащих персональные данные, осуществляется в шкафах, запираемых на ключ.

5.33. Организация при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их

защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

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

5.35. Для обеспечения безопасности ПД организация руководствуется следующими принципами:

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

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

комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах организации и других имеющихся в организации систем и средств защиты;

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

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

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

персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПД;

минимизация прав доступа: доступ к ПД предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;

гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных организации, а также объема и состава обрабатываемых ПД;

специализация и профессионализм: реализация мер по обеспечению

безопасности ПД осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

эффективность процедур отбора кадров: кадровая политика организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;

наблюдаемость и прозрачность: меры по обеспечению безопасности ПД 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 ПД, а результаты контроля регулярно анализируются.

5.36. Доступ к персональным данным в организации имеют только те специалисты, кому это необходимо для исполнения должностных обязанностей и в соответствии с требованиями внутренних регулятивных документов организации.

5.37. Допущенные к обработке ПД работники под подпись знакомятся с документами организации, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных работников.

5.38. В организации не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся организацией ПН уничтожатся или обезличиваются.

5.39. При обработке ПД обеспечиваются их точность, достаточность, а при необходимости и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПД.

5.40. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

назначение Организацией ответственных за организацию обработки персональных данных;

издание Организацией документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Организации в отношении обработки персональных данных, локальным актам Организации;

определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

ознакомление работников Организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных

учетом машинных носителей персональных данных;

выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;

восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных;

обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются в должностных регламентах вышеуказанных лиц;

5.41. Субъект ПД вправе требовать от Организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.42. Сведения предоставляются субъекту персональных данных или его представителю Организацией при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных 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 персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.43. Организация вправе отказать субъекту персональных данных в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Организации.

5.44. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных Организацией;

правовые основания и цели обработки персональных данных;

цели и применяемые Организацией способы обработки персональных данных;

наименование и место нахождения Организации, сведения о лицах (за исключением сотрудников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Организацией или на основании федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»; информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Организации, если обработка поручена или будет поручена такому лицу.

5.45. Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в орган, уполномоченный по вопросам защиты прав субъектов персональных данных, или в судебном порядке.

6. Актуализация, исправление, удаление и уничтожение персональных данных. Ответы на запросы субъектов на доступ к персональным данным.

6.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации, а обработка должна быть прекращена.

6.2. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

Организация не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами;

иное не предусмотрено иным соглашением между Организацией и субъектом персональных данных.

6.3. Организация обязана сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

6.4. Уничтожение документов (носителей), содержащих ПД, производится путем сжигания, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

6.5. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

6.6. Уничтожение документов, содержащих ПД, производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

6.7. Субъект персональных данных вправе требовать от Организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.8. Поступившее обращение субъекта персональных данных (письменный запрос или устное обращение) подлежит обязательной регистрации в Журнале регистрации обращений граждан и рассмотрению в течение трех дней с момента поступления.

6.9. В случае запроса/обращения уполномоченных органов по поводу неточности персональных данных субъекта, уполномоченные должностные лица Организации обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.10. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица Организации на основании сведений, представленных субъектом персональных данных или его представителем, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.11. Организация обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.12. Ответы на запросы субъектов персональных данных и их законных представителей регистрируются лицом, ответственным за организацию обработки персональных данных в Администрации в Журнале учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных.

6.13. В случае запроса/обращения субъекта персональных данных или его представителя по поводу неправомерной обработки персональных данных уполномоченные должностные лица Организации обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса.

6.14. В случае получения запроса/обращения на отзыв согласия и доступа субъекта персональных данных к своим данным уполномоченные должностные лица Организации обязаны уведомить субъекта персональных данных о возможных последствиях отзыва им согласия (см. п. 1.9), прекратить обработку персональных данных в целях, выходящих за рамки трудового, гражданско-правового договора или исполнения иных договорных обязательств перед субъектом. В случае отсутствия действующего договора с данным субъектом: прекратить обработку персональных данных субъекта и уничтожить персональные данные с составлением «Акта об уничтожении персональных данных субъекта» в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено действующим законодательством; уведомить субъект об уничтожении персональных данных.

6.15. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

6.16. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Результаты служебной проверки докладываются начальнику санатория. Если при проверке выявлены факты совершения должностным лицом Организации действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы.

6.17. Запрос/обращение считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

6.18. Ответы на запросы/обращения печатаются на бланке установленной формы и регистрируются в соответствии с порядком делопроизводства, установленным в Организации.