Приложение № 1 к приказу №09-1-П от « 16 » января 2025

Утверждено
приказом Генерального директора
АО «Санаторий «Зеленая роща»
№ 09-1-П от 16.01.2025

Положение о защите персональных данных
в АО «Санаторий «Зеленая роща»

1.1.Настоящее Положение разработано в соответствии с:

• Конституцией РФ;

• Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

• Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

• Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ;

• постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

• постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

• иными нормативными правовыми актами, регулирующими вопросы обработки и защиты персональных данных.

1.2.Положение определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных.

1.3.В настоящем положении используются следующие основные понятия:

— **Оператор**: АО «Санаторий «Зеленая роща»;

— **субъект персональных данных**: физическое лицо, состоящее в трудовых отношениях с Оператором, соискатель, физическое лицо-получатель услуг, вступившее в договорные отношения с Оператором (потребитель), физическое лицо-исполнитель, вступившее в договорные отношения с Оператором, физические лица - представители перечисленных лиц;

— **уполномоченный на работу с персональными данными**: сотрудник АО, который в соответствии приказом генерального директора Оператора занимается обработкой персональных данных;

— **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;

— **согласие на обработку персональных данных**: документ, оформленный в соответствии с разделом 2 настоящего Положения;

— **конфиденциальность персональных данных**: обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

— **автоматизированная обработка персональных данных**: обработка персональных данных с помощью средств вычислительной техники;

— **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;

— **доступ к персональным данным**: предоставление возможности ознакомления с персональными данными 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;

— **информационная система персональных данных (ИСПДн)**: совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

— **использование персональных данных**: действия (операции) с персональными данными, совершаемые уполномоченным должностным лицом Оператора в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

— **общедоступные персональные данные**: персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

— **информация:** сведения (сообщения, данные) независимо от формы их представления;

— **документированная информация**: зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

1.4.Цель настоящего положения - регламентировать порядок обработки персональных данных в АО «Санаторий «Зеленая роща» и обеспечить соблюдение законных прав и свобод человека и гражданина при обработке его персональных данных, в т. ч. защита прав на неприкосновенность частной жизни, личную и семейную тайну.

1.5.Состав персональных данных, подлежащих обработке, каждой из категорий субъектов персональных данных и документы (их копии, выписки из них и т.п.), в которых содержатся персональные данные, определяются Приложением № 1 к Политике в отношении обработки персональных данных и закрепляются приказом генерального директора Оператора.

2. Согласие на обработку персональных данных

2.1.Обработка персональных данных должна осуществляться исключительно в целях обеспечения соблюдения законов или иных правовых актов, содействия субъекту персональных данных в трудоустройстве, обучении и профессиональном продвижении, обеспечения личной безопасности, контроля количества и качества выполняемой работы, обеспечения сохранности имущества, выполнения договорных обязательств.

2.2.Обработка персональных данных должна осуществляться с согласия субъекта персональных данных на обработку его персональных данных. Субъект персональных данных 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, и оформленным в соответствии с требованиями федерального законодательства.

2.3.Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, предусмотренных федеральным законодательством.

2.4.Согласие в письменной форме в виде самостоятельного документа

2.4.1. **требуется** в случаях:

— при получении персональных данных работника у третьей стороны (п. 3 ст. 86 ТК РФ);

— при передаче персональных данных работника третьим лицам, кроме тех случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в иных предусмотренных федеральными законами случаях (абз. 2 ст. 88 ТК РФ);

— для обработки сведений о расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни);

— на обработку персональных данных, разрешенных для распространения.

2.4.2 **не требуется** в тех случаях, когда:

— обработка необходима в целях исполнения заключенного с работником договора или возложенных на работодателя обязанностей, функций и полномочий,

т.е. обработка персональных данных связана с выполнением работником своих трудовых обязанностей (п. п. 2, 5 ч. 1 ст. 6 Закона о персональных данных, п. 3 Разъяснений Роскомнадзора);

— это предусмотрено коллективным договором, соглашением, а также локальными актами работодателя, принятыми в установленном ст. 372 ТК РФ порядке (абз. 2 Разъяснений Роскомнадзора);

— обязанность по обработке предусмотрена законодательством, в том числе для опубликования и размещения персональных данных работников в Интернете (абз. 1 п. 1 Разъяснений Роскомнадзора);

— обработка сведений о состоянии здоровья работника касается возможности выполнения им трудовой функции (п. 2.3 ч. 2 ст. 10 Закона о персональных данных);

— обработка персональных данных специальных категорий проводится органами прокуратуры при условии, что такие данные были получены в установленных законодательством РФ случаях (п. 7.1 ч. 2 ст. 10 Закона о персональных данных);

— проводится обработка персональных данных близких родственников работника в объеме, предусмотренном личной карточкой (форма N Т-2, утвержденная Постановлением Госкомстата России от 05.01.2004 N 1), а также при получении алиментов, оформлении социальных выплат, допуска к государственной тайне и др. (абз. 1 п. 2 Разъяснений Роскомнадзора);

— обработка персональных данных проводится в целях организации работодателем пропускного режима на территорию его служебных зданий и помещений (абз. 1 п. 5 Разъяснений Роскомнадзора);

— персональные данные работника передаются третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных федеральными законами (абз. 2 ст. 88 ТК РФ);

— обработка персональных данных осуществляется в отношении уволенных работников, например, в рамках бухгалтерского и налогового учета (пп. 5 п. 3 ст. 24 НК РФ, ст. 29 Федерального закона от 06.12.2011 N 402-ФЗ, абз. 6 - 10 п. 5 Разъяснений Роскомнадзора).

3. Меры по обеспечению безопасности персональных данных при обработке

3.1. Организационные меры по обеспечению безопасности персональных данных при обработке:

3.1.1. Для обеспечения внутренней защиты персональных данных Оператор предпринимает следующие меры:

— разрабатывает, утверждает и доводит до сведения субъектов персональных данных **Политику в области обработки персональных данных**;

— определяет цели обработки персональных данных, категории и перечень персональных данных; порядок обработки персональных данных;

— избирательно и обоснованно распределяет документы и информацию, содержащую персональные данные, между лицами, уполномоченными на работу с такими данными;

— ограничивает и регламентирует состав работников, функциональные обязанности которых требуют доступа к персональным данным других работников, назначает ответственных за обработку персональных данных;

— определяет порядок допуска к персональным данным работников и иных лиц;

— регулярно проверяет знание работниками, имеющими отношение к работе с персональными данными, требований нормативно-методических документов по защите таких данных;

— определяет порядок хранения, использования и уничтожения персональных данных.

— своевременно выявляет и устраняет нарушения установленных требований по защите персональных данных работников;

— проводит профилактическую работу с должностными лицами, имеющими доступ к персональным данным работников, по предупреждению разглашения таких сведений.

3.1.2. Для обеспечения внешней защиты персональных данных Оператор принимает следующие меры:

— устанавливает пропускной режим и особый порядок приема, учета и контроля деятельности посетителей;

— устанавливает особый порядок выдачи пропусков на территорию

санатория;

— использует технические средства охраны;

— использует программно-технические комплексы защиты информации на электронных носителях и пр.

3.2. **Технические меры по обеспечению безопасности персональных данных при обработке:**

Оператор:

— обеспечивает защиту персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 N 1119 (далее - Требования) (п. 3 Требований, п. 2 ст. 3 Закона о персональных данных).

— определяет тип угроз, которые создают актуальную опасность несанкционированного доступа к персональным данным при их обработке в информационной системе (п. 6 Требований).

— применяется один из четырех уровней защиты персональных данных (п. п. 8 - 16 Требований). Определяет состав и содержание мер по обеспечению их безопасности для каждого уровня защиты определены в соответствии с приказом ФСТЭК России от 18.02.2013 N 21. и приказом ФСТЭК России от 29.04.2021 N 77.

— не допускает проникновения в помещения, в которых размещена информационная система;

— обеспечивает сохранность носителей персональных данных;

— защищает информацию с помощью средств, прошедших процедуру оценки соответствия;

— издает приказ с перечнем работников, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе.

4. Регламент осуществления операций с персональными данными работников

4.1. *Сбор персональных данных.*

4.1.1. Операции с персональными данными работников осуществляют работники службы управления персоналом. Работник, уполномоченный на работу с персональными данными других работников санатория назначается приказом директора Оператора и принимает на себя обязательство о неразглашении

персональных данных.

4.1.2. Уполномоченный на работу с персональными данными – работник службы управления персоналом получает данные непосредственно от субъекта персональных данных и проверяет достоверность сведений, сверяя предоставленные данные с имеющимися у работника документами. При запросе персональных данных (поступлении на работу, учебу и в других случаях) субъект персональных данных должен быть предупрежден о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и юридических последствиях отказа дать письменное согласие на их получение.

4.1.3. Перечень предоставляемых и заполняемых документов, их образцы устанавливаются действующими нормативными актами и утверждаются приказом директора Оператора.

Запрещается требовать от субъектов персональных данных документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

4.1.4. При изменении персональных данных субъект персональных данных письменно уведомляет Оператора в лице уполномоченного работника о таких изменениях в срок, не превышающий 14 дней.

По мере необходимости Оператор в лице уполномоченного работника истребует у субъекта персональных данных дополнительные сведения. Субъект персональных данных предоставляет необходимые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

Оператор не вправе требовать от субъекта персональных данных предоставления информации о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, о частной и интимной жизни, его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

4.2. Получение персональных данных у третьих лиц.

4.2.1. Если персональные данные работника могут быть получены только у третьей стороны, Работник, уполномоченный на работу с персональными данными обязан уведомить об этом заранее и получить письменное согласие работника (п. 3 ст. 86 ТК РФ).

В уведомлении необходимо указать (п. 3 ст. 86 ТК РФ):

- цели получения персональных данных работника у третьего лица;

- предполагаемые источники информации (лица, у которых будут запрашиваться данные);

- способы получения данных, их характер;

- возможные последствия отказа работодателю в получении персональных данных работника у третьего лица. При отказе работника ознакомиться с уведомлением о предполагаемом получении его персональных данных у другого лица Работник, уполномоченный на работу с персональными данными составляет акт.

Информацию, не имеющую отношения к перечисленным в п. 1 ст. 86 ТК РФ целям, Работник, уполномоченный на работу с персональными данными не вправе запрашивать у третьих лиц даже с согласия работника.

Запросы и согласия на предоставления, а также факт передачи персональных данных третьим лицам фиксируются в Журналах.

4.2.2. Работник, уполномоченный на работу с персональными данными обязан вести журналы и оформлять уведомления, перечисленные в п. 3.1.3. настоящего Положения.

В журнале учета внутреннего доступа к персональным данным (доступа работников организации к персональным данным других работников) указываются дата выдачи и возврата документов (личных дел), срок пользования, цели выдачи, наименование выдаваемых документов (личных дел).

Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

В Журнале учета выдачи персональных данных работников организациям и государственным органам регистрируются поступающие запросы, а также сведения о лице, направившем запрос, дату передачи персональных данных или уведомления об отказе в их предоставлении и отмечается, какая именно информация была передана.

4.3. Обработка персональных данных

4.3.1. Обработка персональных данных осуществляется как без использования средств автоматизации, так и с использованием средств

автоматизации (информационных системах персональных данных 1С-кадры).

Персональные данные при обработке без использования средств автоматизации должны быть обособлены от иной информации путем фиксации их на отдельных материальных носителях.

Работник, уполномоченный на работу с персональными данными, осуществляющий обработку персональных данных руководствуется правилами такой обработки, установленными действующим законодательством.

4.4. Хранение и использование персональных данных работников.

4.4.1. Персональные данные являются сведениями, составляющими конфиденциальную информацию. Режим конфиденциальности в отношении персональных данных снимается:

— в случае их обезличивания;

— по истечении 75 лет срока их хранения;

— в других случаях, предусмотренных федеральным законодательством.

4.4.2. Документы, содержащие персональные данные работников, хранятся в личных делах, а также в других делах и в информационных системах персональных данных.

Запрещается хранение в личных делах копии страниц паспорта, военного билета и других документов, которые содержат персональные данные работника.

4.4.3. Персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде с соблюдением установленных правил.

4.4.4. Уполномоченный на работу с персональными данными при организации хранения руководствуется Инструкцией по организации хранения кадровых документов.

Документы воинского учета, содержащие персональные данные работников, должны храниться в железных шкафах в специально оборудованных помещениях (п. 21 Методических рекомендаций по ведению воинского учета в организациях (утв. Минобороны России 11.07.2017)).

4.5. Передача персональных данных

4.5.1. Уполномоченный на работу с персональными данными вправе:

а) осуществлять их передачу только в пределах организации и с письменного согласия субъекта персональных данных на передачу;

б) передавать персональные данные работников по мотивированному

запросу только специально уполномоченным лицам, а также представителям работников в том объеме, который необходим им для выполнения конкретных функций.

Требования к содержанию согласия на обработку персональных данных, разрешенных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 N 18.

4.5.2. Уполномоченный на работу с персональными данными вправе передавать персональные данные без согласия:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника (абз. 2 ст. 88 ТК РФ, абз. 1 п. 4 Разъяснений Роскомнадзора);

- в СФР в объеме, предусмотренном законом (абз. 15 ч. 2 ст. 22 ТК РФ, п. 2 ст. 12 Федерального закона от 16.07.1999 N 165-ФЗ, ч. 2 ст. 15 Федерального закона от 01.04.1996 N 27-ФЗ, п. 2 ст. 14 Федерального закона от 15.12.2001 N 167-ФЗ, абз. 3 п. 4 Разъяснений Роскомнадзора);

- в налоговые органы (пп. 1, 2, 4 п. 3 ст. 24 НК РФ, п. 2 ст. 12 Закона об основах обязательного соцстрахования, абз. 5 п. 4 Разъяснений Роскомнадзора);

- в военные комиссариаты (абз. 4 п. 1 ст. 4 Федерального закона от 28.03.1998 N 53-ФЗ, пп. "г" п. 30, пп. "а" - "в", "д", "е" п. 32 Положения о воинском учете, утвержденного Постановлением Правительства РФ от 27.11.2006 N 719, абз. 5 п. 4 Разъяснений Роскомнадзора);

- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем (абз. 5 ч. 6 ст. 370 ТК РФ, п. 1 ст. 17, п. 1 ст. 19 Федерального закона от 12.01.1996 N 10-ФЗ, абз. 5 п. 4 Разъяснений Роскомнадзора);

- по мотивированному запросу органов прокуратуры (п. 1 ст. 22 Федерального закона от 17.01.1992 N 2202-1, абз. 7 п. 4 Разъяснений Роскомнадзора);

- по мотивированному требованию правоохранительных органов и органов безопасности (ст. 6 Федерального закона от 29.07.2004 N 98-ФЗ, п. 4 ч. 1 ст. 13 Федерального закона от 07.02.2011 N 3-ФЗ, п. "м" ч. 1 ст. 13 Федерального закона от 03.04.1995 N 40-ФЗ, абз. 7 п. 4 Разъяснений Роскомнадзора);

- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности (абз. 3 ч. 1 ст. 357 ТК РФ, абз. 7 п. 4 Разъяснений Роскомнадзора);

- по запросу суда (ч. 4 - 7 ст. 66 АПК РФ, ч. 1, 2 ст. 57 ГПК РФ);

- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом (абз. 5 ст. 228 , 228,1 ТК РФ);

- в случаях, связанных с исполнением работником должностных обязанностей (например, при направлении в командировку). (ч. 5 - 5.2 ст. 11 Федерального закона от 09.02.2007 N 16-ФЗ, п. 13 Правил предоставления гостиничных услуг, утвержденных Постановлением Правительства РФ от 18.11.2020 N 1853, абз. 4 п. 4 Разъяснений);

- для предоставления сведений в кредитную организацию, обслуживающую платежные карты работников, если в договоре о выпуске карт (коллективном договоре, локальном нормативном акте организации) предусмотрено право работодателя передавать персональные данные работников либо работодатель действует на основании доверенности на представление интересов работников (абз. 10 п. 4 Разъяснений).

5. Регламент осуществления операций с персональными данными третьих лиц

5.1. *Сбор персональных данных.*

5.1.1.Операции с персональными данными третьих лиц – потребителей, представителей контрагентов осуществляют:

персональных данных пациентов, проживающих - менеджеры по работе с клиентами и медицинские работники;

персональных данных всех субъектов персональных данных – сотрудники бухгалтерии, планово-экономического отдела, системный администратор, администратор баз данных.

Работники, уполномоченные на работу с персональными данными третьих лиц, назначаются приказом генерального директора и принимают на себя обязательство соблюдать режим конфиденциальности полученных данных.

5.1.2. Уполномоченные на работу с персональными данными получают данные непосредственно от субъекта персональных данных и проверяют достоверность сведений, сверяя предоставленные данные с имеющимися у работника документами.

5.1.3. Запрещается требовать от субъектов персональных данных документы

помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

5.2. *Обработка персональных данных*

5.2.1. Обработка персональных данных осуществляется с использованием средств автоматизации (информационных системах ЛОГУС и САНАТОРИУМ).

5.3. *Хранение и использование персональных данных третьих лиц.*

5.3.1. Персональные данные являются сведениями, составляющими конфиденциальную информацию. Режим конфиденциальности в отношении персональных данных снимается:

— в случае их обезличивания;

— по истечении 5 лет срока их хранения.

5.3.2. Запрещается хранение копий страниц паспорта, военного билета и других документов, которые содержат персональные данные работника.

5.3.3. Уполномоченный на работу с персональными данными при организации хранения руководствуется Инструкцией по организации хранения документов. Документы, содержащие персональные данные пациентов, проживающих и других категорий субъектов персональных данных, хранятся вместе с договором на оказание санаторно-курортных услуг, договором на оказание платных медицинских услуг, договором на оказание иных видов услуг, если в ходе исполнения этих договоров происходила обработка персональных данных, а также в информационных системах ЛОГУС и САНАТОРИУМ.

5.4. Передача персональных данных.

5.4.1. Порядок работы с врачебной тайной и предоставление персональных данных потребителей – пациентов санатория осуществляется согласно Приложения № 2 к «Кодексу этики и служебного поведения работников АО «Санаторий «Зеленая роща», утвержденному приказом Генерального директора.

5.4.2. Уполномоченный на работу с персональными данными лиц, не относящихся к потребителям-пациентам вправе:

а) осуществлять их передачу только в пределах организации и с письменного согласия субъекта персональных данных;

б) передавать персональные данные работников по мотивированному запросу только специально уполномоченным лицам, а также представителям работников в том объеме, который необходим им для выполнения конкретных функций.

Требования к содержанию согласия на обработку персональных данных, разрешенных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 N 18.

5.4.3. Уполномоченный на работу с персональными данными вправе передавать персональные данные без согласия в случаях, предусмотренных п. 4.5.2. настоящего Положения.

6. Регламент взаимодействия подразделений при работе с документами, содержащими персональные данные

Работа с документами, содержащими персональные данные, должна быть организована таким образом, чтобы исключить их просмотр посторонними лицами (посетителями).

Безопасность персональных данных при их обработке в информационной системе, содержащей персональные данные обеспечивается с помощью системы защиты информации, которая должна соответствовать требованиям, предъявляемым к ИСПДн соответствующими нормативными правовыми документами.

По истечении срока хранения персональных данных, документы, содержащие персональные данные, по которым делопроизводство завершено, проходят подготовку к последующему хранению, после чего передаются на хранение в архив.

6.1. *Получение - Передача персональных данных*

6.1.1. В целях информационного обеспечения Оператор может создавать общедоступные источники (сайты, служебные справочники, другие документы, в том числе электронные), содержащие персональные данные, которые включаются в эти источники с согласия субъектов персональных данных или на основании федерального закона.

6.1.2. Распространение персональных данных допускается только с письменного согласия субъекта персональных данных.

6.1.3. При необходимости предоставления персональных данных работников санатория в составе заявки на участие в закупочных процедурах, проведения рекламных акций, осуществления публикаций и т.п работники отдела продаж и отдела маркетинга, уполномоченные на работу с персональными данными обязаны письменно обратиться в службу управления персоналом к ответственному

работнику не позднее 10 рабочих дней до даты предполагаемой передачи персональных данных.

6.1.4. Основанием для рассмотрения возможности и целесообразности передачи персональных данных третьей стороне является письменный запрос на имя генерального директора, в котором должно быть указано:

— состав испрашиваемых сведений;

— обоснование необходимости работы с этими сведениями;

— ссылка на федеральный закон (с указанием конкретных статей), на основании которого запрашиваются персональные данные;

— форма передачи сведений: доступ (ознакомление, выписки или копирование) или предоставление (в каком виде: электронном или бумажном);

— представитель, уполномоченный на получение персональных данных (фамилия, имя, отчество, серия и номер паспорта или служебного удостоверения, когда и кем они выданы);

— обязательство соблюдать режим конфиденциальности полученных данных.

6.1.5. Сотрудник службы управления персоналом, уполномоченный на работу с персональными данными работников обязан письменно уведомить субъектов персональных данных и получить его письменное согласие на передачу персональных данных. Не поступление письменного согласия означает отказ работника на передачу персональных данных.

6.1.6. Работник отдела продаж и отдела маркетинга при наличии согласия работника вправе передать персональные данные при условии предупреждения лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требует от этих лиц подтверждения того, что это правило соблюдено. Копии документов, подтверждающих исполнение данного требования передаются в службу управления персоналом для хранения.

6.1.7. Право внутреннего доступа (доступ внутри АО) к персональным данным работников имеют:

— Генеральный директор - ко всем персональным данным, обрабатываемым организацией;

— работники службы управления персоналом, бухгалтерии;

— субъект персональных данных - к своим персональным данным;

Право внутреннего доступа (доступ внутри санатория) **к персональным данным о состоянии здоровья пациентов** имеют:

— медицинские работники санатория;

— менеджеры Курортной поликлиники;

— менеджеры СПиРГ (при заселении);

— специалисты службы бронирования;

— системный администратор, администратор баз данных;

—другие работники организации при выполнении ими своих служебных обязанностей - при наличии письменного разрешения (распоряжения) руководителя организации. Перечень лиц определяется приказом генерального директора оператора. Лица, указанные в приказе подписывают Обязательство о неразглашении персональных данных. Обязательство хранится в личном деле работника.

6.1.8. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения руководителя организации по мотивированному заявлению.

6.1.9. Лица, получающие персональные данные, имеют право получать только те персональные данные, которые необходимы для выполнения конкретной функции. Они обязаны соблюдать режим конфиденциальности полученных данных.

6.1.10. Субъекту персональных данных или его представителю Оператор передает его персональные данные 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.

6.1.11. Запрещается передавать кому-либо персональные данные по телефону, факсу, электронной почте.

6.1.12. Работники, уполномоченные на работу с персональными данными

независимо от категории субъектов персональных данных в случае:

— адресного размещения на носителях и серверах, доступ к которым имеют они ибо третьи лица;

— при размещении персональных данных в источниках внутрикорпоративного документооборота;

— при опубликовании в интересах предприятия персональных данных о работнике в СМИ или на серверах интернета в соответствии с нормами законодательства **обязаны соблюдать конфиденциальность и немедленно**

— блокировать персональные данные либо изъять соответствующие данные из информационных систем при обращении субъекта персональных данных или его законного представителя либо получения запроса уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора на период проверки;

— устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными;

— уничтожить персональные данные в случае невозможности устранения допущенных нарушений в указанный срок, уведомить об устранении допущенных нарушений или об уничтожении персональных данных субъекта персональных данных или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных - также указанный орган;

— прекратить обработку персональных данных и уничтожить их в случае отзыва субъектом персональных данных согласия на их обработку или по достижению цели обработки в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва или с даты достижения цели обработки, если иное не предусмотрено федеральными законами или соглашением между оператором и субъектом персональных данных, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае поступления обращения или запроса от уполномоченного органа по защите прав субъектов персональных данных - также указанный орган;

6.1.13. Работники, уполномоченные на работу с персональными данными независимо от категории субъектов персональных данных при использовании цифровой ИС обязаны исключить передачу данных по незащищенным каналам

связи. В случае, если используется цифровая ИС, блокирование данных осуществлять посредством закрытия доступа к файлам.

6.1.14. Ликвидация персональных данных осуществляется с учетом специфики информационной системы посредством их удаления с ПК, а также серверов. Ликвидация данных на бумажных носителях осуществляется посредством уничтожения соответствующих носителей с помощью специальных технических средств в соответствии с Порядком уничтожения персональных данных, утвержденных приказом Оператора.

6.1.15. Сотрудники, имеющие доступ к персональным данным, обязаны немедленно информировать своего непосредственного руководителя и директора о нештатных ситуациях, связанных с операциями с персональными данными.

7. Права и обязанности субъекта персональных данных

7.1. В целях защиты персональных данных, обрабатываемых Оператором, субъект персональных данных имеет право:

— на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

— требовать уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для организации персональных данных;

— персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

— определять своих представителей для защиты своих персональных данных;

— на сохранение и защиту своей личной и семейной тайны;

— требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

— обжаловать неправомерные действия или бездействие Оператора при обработке и защите персональных данных.

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

— подтверждение факта обработки персональных данных Оператором;

— правовые основания и цели обработки персональных данных;

— цели и применяемые Оператором способы обработки персональных данных;

— 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;

— иные сведения, предусмотренные федеральным законодательством.

7.3. Субъект персональных данных обязан:

— передавать Оператору комплект достоверных документированных персональных данных, состав которых установлен действующим законодательством РФ;

— своевременно сообщать организации об изменении своих персональных данных.

8. Заключительные положения

Настоящее положение и изменения к нему утверждаются, вводятся в действие приказом по организации и вступают в силу с момента их утверждения приказом по организации.

Все работники организации должны быть ознакомлены под подпись с данным положением и изменениями к нему.

Настоящее положение размещается на официальном сайте организации с целью ознакомления с ним субъектов персональных данных и их представителей.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

Приложение № 1.

Меры ответственности

1. Ответственность работодателя за нарушение норм, регулирующих защиту персональных данных

За нарушение законодательства в области персональных данных работодатель может быть привлечен к административной ответственности по ст. 13.11 КоАП РФ.

В частности, обработка персональных данных без письменного согласия работника (когда оно необходимо), если эти действия не содержат уголовно наказуемых деяний, влечет наложение штрафа (ч. 2 ст. 13.11 КоАП РФ):

- на граждан - от 10 000 до 15 000 руб.;

- должностных лиц - от 50 000 до 100 000 руб.;

- юридических лиц - от 150 000 до 300 000 руб.

Такие же меры предусмотрены ч. 2 ст. 13.11 КоАП РФ за обработку персональных данных с нарушением требований к составу сведений, включаемых в письменное согласие.

За повторное допущение правонарушения, указанного в ч. 2 ст. 13.11 КоАП РФ, грозит штраф (ч. 2.1 ст. 13.11 КоАП РФ):

- для граждан - от 15 000 до 30 000 руб.;

- должностных лиц - от 100 000 до 200 000 руб.;

- юридических лиц - от 300 000 до 500 000 руб.

2. Ответственность работника, имеющего доступ к персональным данным других работников, за их разглашение

Исходя из смысла ст. 90 ТК РФ работник, по вине которого было допущено нарушение норм, регулирующих обработку и защиту персональных данных других работников, может быть привлечен к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности.

2.1. Административная ответственность работника, имеющего доступ к персональным данным других работников

На основании ст. ст. 2, 3, 5, 6 Закона о персональных данных персональные данные относятся к информации, доступ к которой ограничен. В соответствии со

ст. 13.14 КоАП РФ разглашение подобной информации (за исключением случаев, если такое разглашение влечет уголовную ответственность) лицом, получившим доступ к ней в связи с исполнением служебных или профессиональных обязанностей, влечет наложение административного штрафа:

- на граждан - от 500 до 1 000 руб.;

- на должностных лиц - от 4 000 до 5 000 руб.

Следовательно, если будет установлено, что разглашение персональных данных произошло по вине работника, ответственного за хранение, обработку и использование персональных данных других работников, то его могут привлечь к административной ответственности в виде штрафа.

2.2. Дисциплинарная ответственность работника, имеющего доступ к персональным данным других работников

Персональные данные относятся к сведениям, которые охраняются федеральным законом. Неправомерное разглашение персональных данных лицом, в чьи обязанности входит соблюдение правил хранения, обработки и использования такой информации, также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТК РФ). Согласно пп. "в" п. 6 ч. 1 ст. 81 ТК РФ трудовой договор с работником может быть расторгнут по причине разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе по причине разглашения персональных данных другого работника. Поскольку такое увольнение относится к увольнениям за нарушение трудовой дисциплины, то работника, разгласившего персональные данные, необходимо уволить с соблюдением процедуры, предусмотренной ст. 193 ТК РФ.

Помимо разглашения, к неправомерным действиям работника, имеющим доступ к персональным данным, также будет относиться отсутствие необходимых действий по полной обработке персональный данных, ее систематизации и внесении в необходимые базы данных и реестры, что также является основанием для привлечения этого лица к дисциплинарной ответственности (ст. 90 ТК РФ).

2.3. Уголовная ответственность работника, имеющего доступ к персональным данным других работников

В соответствии с ч. 1 ст. 137 УК РФ незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или

семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации наказываются, в частности, штрафом в сумме до 200 тыс. руб. или в размере заработной платы либо иного дохода осужденного за период до 18 месяцев, либо обязательными работами на срок до 360 часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. Возможно также наказание в виде ареста на срок до четырех месяцев либо лишения свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Если же лицо совершило те же деяния, используя служебное положение, то ему грозит одно из следующих наказаний (ч. 2 ст. 137 УК РФ):

- штраф в сумме от 100 тыс. до 300 тыс. руб. или в размере зарплаты либо иного дохода осужденного за период от одного года до двух лет;

- лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет;

- принудительные работы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового;

- арест на срок до шести месяцев;

- лишение свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Следовательно, если работник, ответственный за хранение, обработку и использование персональных данных других работников, злоупотреблял своими служебными полномочиями, распространял сведения о частной жизни других работников без их согласия, то он может быть привлечен к уголовной ответственности.

2.4. Материальная ответственность работника, имеющего доступ к персональным данным других работников

Статьей 90 ТК РФ предусмотрена материальная ответственность за виновное нарушение норм, регулирующих обработку и защиту персональных

данных работников. Так, в результате незаконного распространения информации о персональных данных работника последнему может быть причинен моральный вред, подлежащий возмещению работодателем. В соответствии со ст. 238 ТК РФ работник обязан возместить работодателю причиненный последнему прямой действительный ущерб. Согласно ч. 2 указанной статьи под прямым действительным ущербом также понимается необходимость возмещения ущерба третьим лицам. Следовательно, если вред работнику был причинен по вине лица, которое было ответственно за неразглашение персональных данных, то работодатель может привлечь последнее к материальной ответственности за ущерб, который был нанесен работнику такими действиями. В соответствии с п. 7 ч. 1 ст. 243 ТК РФ материальная ответственность в полном размере причиненного ущерба возлагается на работника в случае разглашения сведений, составляющих охраняемую законом тайну.

2.5. Гражданско-правовая ответственность работника, имеющего доступ к персональным данным других работников

В соответствии со ст. 151 ГК РФ, если гражданину причинен моральный вред (физические или нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. Согласно ч. 2 ст. 1099 ГК РФ моральный вред, причиненный действиями (бездействием), нарушающими имущественные права гражданина, подлежит компенсации в случаях, предусмотренных законом. На основании ст. 152 ГК РФ гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности. Следовательно, если в результате нарушения норм, регулирующих хранение, обработку и использование персональных данных работника, допущенного лицом, ответственным за осуществление вышеперечисленных действий с персональными данными, работнику причинен имущественный ущерб или моральный вред, то он подлежит возмещению в денежной форме в соответствии со статьями Гражданского кодекса РФ.

ЛИСТ СОГЛАСОВАНИЕ К положению „О защите персональных данных"

1. Главный Бухгалтер

_____ А.З. Тимергалиева

4. Начальник ПЭО

_____ З.Р. Низамова

5. Начальник кадровой службы

_____ Г.К. Сайфутдинова

6. Руководитель отдела продаж

_____ Е.Р. Пишняк

7. Руководитель МТО

_____ Е.Н. Асмеева

8. Руководитель ЮС

_____ И.К. Мазур