

УТВЕРЖДЕНО
Приказом генерального директора
ООО «Санаторий «Родина»
№ 46/173 от «14» 01 2015 года.

ПОЛОЖЕНИЕ

об обработке и защите персональных данных клиентов (гостей)

ООО «Санаторий «Родина»

1. Общие положения

1.1. Настоящее Положение определяет порядок обработки персональных данных клиентов в ООО «Санаторий «Родина» (далее - Общество), в том числе все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе по передаче), обезличиванию, блокированию, уничтожению персональных данных клиентов, осуществляемых с использованием средств автоматизации и без их использования. Также настоящее Положение определяет порядок передачи персональных данных клиентов третьим лицам, случаи взимания согласий субъектов персональных данных, особенности автоматизированной и неавтоматизированной обработки персональных данных, порядок доступа к персональным данным, систему защиты персональных данных и ответственность за нарушения при обработке персональных данных и иные вопросы.

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Общества и его клиентов в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации и нормативно-методическими документами исполнительных органов государственной власти в области защиты персональных данных при их обработке на бумажных носителях и в информационных системах персональных данных.

1.4. Порядок ввода в действие и изменения Положения.

1.4.1. Настоящее Положение вступает в силу с момента его утверждения генеральным директором Общества и действует бессрочно, до замены его новым Положением.

1.4.2. Все изменения в Положение вносятся приказом генерального директора.

1.5. Сведения о персональных данных относятся к числу конфиденциальных (составляющих охраняемую законом тайну Общества). Режим конфиденциальности в отношении персональных данных снимается:

– в случае их обезличивания.

по истечении 75 лет срока их хранения.

– в других случаях, предусмотренных действующим законодательством РФ.

2. Основные понятия. Состав персональных данных клиентов

2.1. В настоящем Положении используются термины и понятия в соответствии с их определениями, указанными в действующем законодательстве, и настоящим Положением. В случае противоречия терминов, указанных в настоящем Положении и терминов, используемых в законодательстве, применяются определения, указанные в законодательстве.

2.2. Термины, определяемые в настоящем Положении:

- персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту 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;
- 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:

- автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
- распространение персональных данных – действия, направленные на раскрытие персональных данных Клиентов неопределенному кругу лиц;
- предоставление персональных данных – действия, направленные на раскрытие персональных данных Клиентов 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 работнику;
- 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;
- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- Клиент – любое физическое лицо, заключившее с Обществом договор об оказании гостиничных услуг (услуги, предоставляемые Обществом Клиенту, по размещению в гостиничных номерах, а также договор об оказании любых дополнительных услуг (услуги по проведению мероприятий, услуги СПА-комплекса и т.д.);

2.3. Сведениями, составляющими персональные данные, является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

- фамилия, имя, отчество,
- дата и место рождения,
- адрес регистрации и адрес фактического проживания,
- номера домашнего и мобильного телефонов, адрес электронной почты,
- паспортные данные,
- фотография,
- физиологические особенности,
- семейное положение: состав семьи, места работы или учебы членов семьи и родственников,
- другие сведения, необходимые ООО «Санаторий «Родина» и касающиеся субъекта персональных данных.

3. Цели и принципы обработки персональных данных Клиентов

3.1. Обработка персональных данных в Обществе осуществляется в целях оказания услуг Обществом, для разработки новых продуктов/услуг и информирования Клиента об этих продуктах/услугах (в том числе по телефону/электронной почте), а также в случаях предоставления в соответствии с законодательством РФ данных (сведений) исполнительным органам государственной, муниципальной власти, а также с целью исполнения действующего законодательства РФ.

3.2. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

3.3. Срок обработки персональных данных должен ограничиваться достижением конкретных, заранее определенных и законных целей.

3.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Сбор персональных данных, обрабатываемых в Обществе

4.1. Информация, представляемая субъектом персональных данных в Общество, должна иметь документальную форму. Общество имеет право копировать документы, содержащие персональные данные в целях исполнения договорных отношений.

4.2. Клиент обязан передавать Обществу комплекс достоверных, документированных персональных данных, состав которых установлен настоящим Положением и договорными обязательствами, взятыми на себя сторонами по договору между Клиентом и Обществом. Клиент должен без неоправданной задержки сообщать Обществу об изменении своих персональных данных.

4.3. При оказании гостиничных услуг, Клиент обязуется заполнить и подписать регистрационную карту гостя, в которой указываются персональные данные Клиента, а также заполнить и подписать иные необходимые документы, в которых указываются персональные данные.

4.4. При заключении договора Клиент обязуется предоставить Обществу документы, необходимые в таком случае Обществу, в оригинале.

5. Согласие на обработку персональных данных. Случаи и порядок получения согласия

5.1. Клиенты при заполнении и подписании регистрационной карты гостя должны предоставлять согласие на обработку персональных данных, поставив свою подпись на оборотной стороне регистрационной карты гостя под фразой «Даю свое согласие на обработку (в т.ч. автоматизированную) ООО «Санаторий «Родина» моих персональных данных (любая информация, относящаяся к моей личности) в целях оказания мне услуг Обществом, а также для разработки Обществом новых продуктов/услуг и информирования меня об этих продуктах/услугах (в том числе по телефону/электронной почте). Согласие дается на 30 лет. Общество вправе раскрывать информацию обо мне третьим лицам. С Положением Общества об обработке и защите персональных данных клиентов (гостей) я ознакомлен и согласен. I give my permission for processing my private data (any information dealing with my personality) including computer-aided processing by «Grand Hotel & Spa Rodina» Limited Liability Company in order to purchase, execute services, development of new products/services and informing me about these products/services (either by telephone or e-mail). My permission is given for 30years. Company is available to divulge the information about me to the third persons. I have read and accept the Regulations of the Company on the processing and protection of personal data of customers (guests)». При этом Клиент должен поставить дату предоставления такого согласия. В случае не указания даты Клиентом, дата проставляется сотрудником Общества.

5.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

5.3. В отношении несовершеннолетних детей согласие дают их законные представители.

5.4. В случае трансграничной передачи персональных данных Клиентов Общества необходимо получать согласие субъектов персональных данных на обработку персональных данных. Трансграничная передача персональных данных — передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства. Трансграничная передача осуществляется в соответствии с действующим законодательством РФ.

5.5. **Обработка** персональных данных допускается без согласия субъекта персональных данных в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее — исполнение судебного акта);
- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с действующим законодательством;
- обработка персональных данных необходима для исполнения договора (гражданско-правового или трудового), стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

5.6. Предоставляя согласие на обработку персональных данных, Клиент также дает согласие на использование его фотографии, на уведомление его об акциях, розыгрышах, лотереях, спец. предложениях, о новых тарифах, услугах, а также об

изменении тарифов услуг Общества, а также на передачу его персональных данных исполнительным органам государственной власти в целях выполнения законодательства РФ, подзаконных актов и иных документов.

6. Права Клиентов и обязанности Общества в отношении персональных данных, обрабатываемых в Обществе

6.1. Клиент - субъект персональных данных имеет право на получение информации (далее - сведения), касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законодательством;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные федеральным законодательством.

6.2. Клиент вправе требовать от Общества 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 действующим законодательством меры по защите своих прав.

6.3. Сведения, содержащие персональные данные, должны быть предоставлены в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.4. Сведения, содержащие персональные данные, предоставляются Клиенту или его представителю оператором при обращении либо при получении запроса Клиента - 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, 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.

6.5. В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений и ознакомления с

такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.6. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан 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.

6.7. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены Обществу на основании действующего законодательства или если персональные данные являются общедоступными, Общество до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

- наименование (фамилия, имя, отчество) и адрес Общества или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные действующим законодательством права субъекта персональных данных;
- источник получения персональных данных.

6.8. Если обязанность предоставления персональных данных установлена федеральным законом, Общество обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

7. Порядок обработки, доступа, передачи и защиты персональных данных Клиентов

7.1. Общество в своей деятельности принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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.

7.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

7.3. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам,

программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

7.4. Методами и способами защиты информации от несанкционированного доступа являются:

- реализация разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием документам;
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
- разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей, контроль несанкционированного доступа и действий пользователей и посторонних лиц;
- учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- использование защищенных каналов связи;
- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

7.5. В Обществе применяется комплекс мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

7.5.1. 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.

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

7.5.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

7.6. К техническим средствам защиты информационных систем персональных данных в Обществе относятся серверы и программное обеспечение для хранения и обработки персональных данных Клиентов. Используется клиент-серверная архитектура с разграничением прав доступа пользователей к информации, содержащей персональные данные Клиентов.

7.7. В Обществе используется следующее основное программное обеспечение для обработки персональных данных:

- «1С: Бухгалтерия»,
- «Fidelio»,
- «Micros»,

- «Клиент-Банк»,
- «MS Office»,
- «СКАЛА»
- Серверное ПО.

Вышеуказанные технические средства информационных систем персональных данных размещаются в офисных и иных помещениях Общества, расположенных по адресу: 354008, Российская Федерация, Краснодарский край, г. Сочи, ул. Виноградная, д. 33.

Установка средств защиты информации и монтаж оборудования, используемого для обработки персональных данных Клиентов, выполнен в соответствии с требованиями технической документации.

7.8. Требования к работникам в связи с обработкой персональных данных:

- обеспечение конфиденциальности персональных данных, обрабатываемых в Обществе, является обязательным требованием для всех работников Общества, которым персональные данные стали известны.
- все лица, допущенные к работе с персональными данными, а также связанные с эксплуатацией и техническим сопровождением информационных систем персональных данных должны быть под роспись ознакомлены с требованиями настоящего Положения.

7.9. Порядок доступа и передачи персональных данных:

7.9.1. Перечень должностей и работников, имеющих доступ к персональным данным Клиентов, утверждается настоящим Положением и/или приказом Генерального директора. Указанным в перечне работникам Общества предоставляется доступ к работе с персональными данными исключительно в пределах и объемах, необходимых для выполнения ими своих должностных обязанностей.

Право доступа к персональным данным Клиентов в пределах, необходимых для выполнения своих должностных обязанностей имеют следующие категории работников Общества:

- генеральный директор,
- работники бухгалтерии,
- директор по взаимодействию с гостями
- заместитель генерального директора по защите активов,
- работники службы защиты активов,
- работники юридического отдела,
- работники отдела информационных технологий,
- работники отдела продаж и маркетинга,
- работники службы приема и обслуживания, непосредственно связанные с обработкой персональных данных,
- работники хозяйственного отдела, непосредственно связанные с обработкой персональных данных,
- работники СПА-комплекса, непосредственно связанные с обработкой персональных данных,
- работники службы ресторанов, непосредственно связанные с обработкой персональных данных.

7.9.2. Временный или разовый допуск к работе с персональными данными в связи со служебной необходимостью может быть получен сотрудником Общества по согласованию с генеральным директором.

7.9.3. Доступ лиц, не являющихся сотрудниками Общества, к персональным данным Клиентов Общества без согласия самих Клиентов, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функции и полномочий соответствующих органов государственной власти, а также в иных случаях, предусмотренных действующим законодательством. Предоставление информации по запросу или требованию органа государственной власти

осуществляется после указания генерального директора Общества о необходимости предоставления информации.

7.9.4. Доступ работников Общества к персональным данным Клиентов прекращается с даты прекращения трудовых отношений, либо даты изменения должностных обязанностей работника и/или исключения его из списка лиц, имеющих право доступа к персональным данным. В случае увольнения работника все носители, содержащие персональные данные, которые в соответствии с должностными обязанностями находились в распоряжении работника в период его работы в Обществе, должны быть переданы непосредственному руководителю.

7.9.5. Работники обязаны незамедлительно сообщать заместителю генерального директора по защите активов Общества об утрате или недостатке носителей информации, составляющей персональные данные, а также о причинах и условиях возможной утечки персональных данных. В случае попытки посторонних лиц получить от работника персональные данные, обрабатываемые в Обществе, незамедлительно известить об этом заместителя генерального директора по защите активов Общества.

7.9.6. В случае если сотруднику сторонней организации необходим доступ к персональным данным Клиентов Общества, то необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности персональных данных и обязанность сторонней организации и её сотрудников по соблюдению требований действующего законодательства в области защиты персональных данных. Указанное согласие не требуется, если персональные данные предоставляются в целях исполнения гражданско-правового договора, заключенного Обществом с субъектом персональных данных.

7.10. Ответственным лицом за хранение персональных данных Клиентов является Начальник службы приема и обслуживания, начальник СПА комплекса. Персональные данные Клиентов хранятся в службе приема и обслуживания, СПА комплекса, а также на серверах компьютерной системы. Носители персональных данных Клиентов в Обществе не должны оставаться без присмотра. При оставлении рабочего места, работники, осуществляющие обработку персональных данных, должны убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче персональных данных осуществляется по возможности их восстановление.

7.11. При работе с программными средствами автоматизированной системы Общества, реализующей функции просмотра и редактирования персональных данных Клиентов, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

7.12. При сборе и обработке персональных данных работником Общества, который в соответствии с должностными обязанностями получает персональные данные от Клиента или иного лица, проводится проверка достоверности документов, содержащих персональные данные. Ввод персональных данных в автоматизированную систему Общества осуществляется работниками, имеющими доступ к соответствующим персональным данным Клиентов.

7.13. Особенности обработки персональных данных, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствии с Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

7.13.2. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

7.13.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее — типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.14. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, настоящим Положением.

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

7.16. Случаи уничтожения, блокирования и уточнения персональных данных:

- в случае выявления недостоверных персональных данных или неправомерных действий с ними Общество при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных обязано осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки. Блокирование осуществляется на основании распоряжения (приказа) генерального директора Общества путем прекращения каких-либо действий с персональными данными.
- в случае подтверждения факта неточности персональных данных Общество на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные (внести изменения) и снять их блокирование. Снятие блокирования осуществляется на основании приказа генерального директора Общества.

- в случае выявления неправомерных действий с персональными данными Общество в срок, не превышающий трех рабочих дней с даты такого выявления, обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязано уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Общество обязано уведомить 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.
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Обществом и субъектом персональных данных. Об уничтожении персональных данных Общество обязано уведомить субъекта персональных данных.
- 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).
- 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.

7.17. Уничтожение носителей, содержащих персональные данные осуществляется в следующем порядке:

- персональные данные на бумажных носителях уничтожаются способом, не позволяющим восстановить документ (применение shreddеров - уничтожителей документов).
- персональные данные, размещенные в памяти ПЭВМ, уничтожаются путем удаления их из памяти ПЭВМ.
- персональные данные, размещенные на флеш-карте, CD-диске, ином носителе информации, уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

7.18. Требования к помещениям, в которых обрабатываются персональные данные.

7.18.1. Доступ в помещения, в которых располагаются средства обработки персональных данных, должен контролироваться работниками службы защиты активов.

7.18.2. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

7.18.3. Уборка помещений и обслуживание технических средств информационных систем персональных данных должны осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к персональным данным, носителям информации, программным и техническим средствам обработки, передачи и защиты информации.

7.19. Обязанности работников ИТ-отдела в части обеспечения защиты информационных систем персональных данных:

- управление учетными записями пользователей и установление разграниченных прав доступа в информационных системах персональных данных.

- поддержание бесперебойной работы и защиты информационных систем персональных данных,
- обеспечение резервного копирования данных,
- установка и конфигурирование аппаратного и программного обеспечения информационных систем персональных данных, не связанного с обеспечением безопасности персональных данных в информационных системах персональных данных.
- выполнение требований по конфиденциальности, целостности и доступности информационных систем персональных данных и общих требований по безопасности персональных данных, установленных федеральным законодательством.
- учет и хранение машинных носителей персональных данных.
- анализ защищенности информационных систем персональных данных.
- участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством.