



УТВЕРЖДАЮ
Директор
ООО «Ломбард «Сантус»
(подпись) И.А. Сидорова/
«01» февраля 2023 г.

ПОЛОЖЕНИЕ
о защите и порядке обработки персональных данных субъектов
в обществе с ограниченной ответственностью «Ломбард «Сантус»

г. Ижевск
2023г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение разработано в соответствии с законодательством Российской Федерации, в том числе Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 06.04.2011 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативно-правовыми актами (далее по тексту – законодательство) и устанавливает порядок работы с персональными данными (далее – ПДн) работников и иных физических лиц (далее - субъектов), обрабатываемыми в ООО «Ломбард «Сантус» (далее по тексту – Общество).

1.2. Принятие настоящего Положения преследует следующие цели:

- защита ПДн субъектов от несанкционированного доступа и разглашения;
- обеспечение защиты прав и свобод субъектов при обработке их ПДн в Обществе;
- предотвращение и выявление нарушений законодательства о ПДн, устранение последствий выявленных нарушений;
- установление мер ответственности работников, имеющих допуск и доступ к ПДн субъектов, за невыполнение/нарушение требований законодательства, регулирующего обработку ПДн.

Основные понятия, используемые в настоящем Положении

Персональные данные субъектов – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка персональных данных – обработка ПДн с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе ПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий, и технических средств.

Трансграничная передача персональных данных – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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 в установленных законодательством Российской Федерации случаях ее материальный носитель.

2. ПОНЯТИЕ И СОСТАВ ПДн СУБЪЕКТА

Полный состав ПДн субъектов, обрабатываемых в Обществе, указан в «Перечне персональных данных, обрабатываемых в ООО «Ломбард «Сантус» (далее по тексту - Перечень ПДн), утвержденном директором Общества.

2.1. Информация, содержащая ПДн субъектов, необходима Обществу в целях:

2.1.1. осуществления деятельности в соответствии с уставом:

- **категории субъектов, персональные данные которых обрабатываются:** клиенты; доверенные лица клиентов;

- **категории обрабатываемых персональных данных:** иные категории персональных данных;

- **перечень обрабатываемых персональных данных:** фамилия, имя, отчество, возраст, дата, месяц, год и место рождения, паспортные данные, адрес регистрации по месту жительства и адрес фактического проживания; номер телефона (домашний, мобильный), адрес электронной почты;

- **способы обработки персональных данных:** с использованием средств автоматизации и без использования средств автоматизации;

- **срок обработки (исключая хранение):** до достижения цели обработки персональных данных;

- **срок обработки (хранения):** 5 лет согласно архивному законодательству;

• **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, измельчения в сечку в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус».

2.1.2. анализа поведенческой информации на сайте «santus.org»:

• **категории субъектов, персональные данные которых обрабатываются:** пользователи сайта;

• **категории обрабатываемых персональных данных:** иные категории персональных данных;

• **перечень обрабатываемых персональных данных:** частота посещения сайта пользователями; информация об активности на сайте; посещенные страницы и сайты, на которых были пользователи до перехода на сайт Общества; файлы cookie; данные об устройстве, операционной системе и ее версии;

• **способы обработки персональных данных:** с использованием средств автоматизации;

• **срок обработки (включая хранение):** до достижения цели обработки персональных данных;

• **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус».

2.1.3. информирования клиентов о специальных предложениях Общества с помощью средств связи:

• **категории субъектов, персональные данные которых обрабатываются:** клиенты;

• **категории обрабатываемых персональных данных:** иные категории персональных данных;

• **перечень обрабатываемых персональных данных:** фамилия; имя; отчество; номер телефона; e-mail;

• **способы обработки персональных данных:** с использованием средств автоматизации;

• **срок обработки (включая хранение):** до достижения цели обработки персональных данных;

• **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус».

2.1.4. регистрации на сайте «santus.org» и создания личного кабинета:

• **категории субъектов, персональные данные которых обрабатываются:** клиенты;

• **категории обрабатываемых персональных данных:** иные категории персональных данных;

• **перечень обрабатываемых персональных данных:** имя, фамилия, отчество, дата рождения, e-mail, номер телефона;

• **способы обработки персональных данных:** с использованием средств автоматизации;

• **срок обработки (включая хранение):** до достижения цели обработки персональных данных;

• **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус».

2.1.5. обратной связи с пользователями сайта «santus.org»:

- **категории субъектов, персональные данные которых обрабатываются:** пользователи сайта;
- **категории обрабатываемых персональных данных:** иные категории персональных данных;
 - **перечень обрабатываемых персональных данных:** фамилия, имя, отчество; номер телефона; e-mail
- **способы обработки персональных данных:** с использованием средств автоматизации;
- **срок обработки (включая хранение):** до достижения цели обработки персональных данных;
- **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.1.6. рассмотрения обращений пользователей сайта «santus.org» и направления ответа на них:

- **категории субъектов, персональные данные которых обрабатываются:** пользователи сайта;
- **категории обрабатываемых персональных данных:** иные категории персональных данных;
 - **перечень обрабатываемых персональных данных:** фамилия, имя, отчество; номер телефона, e-mail;
- **способы обработки персональных данных:** с использованием средств автоматизации;
- **срок обработки (включая хранение):** до достижения цели обработки персональных данных;
- **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.1.7. оформления и выполнения договорных, преддоговорных отношений:

- **категории субъектов, персональные данные которых обрабатываются:** контрагенты – индивидуальные предприниматели; работники контрагентов: ИП, юр. лиц;
- **категории обрабатываемых персональных данных:** иные категории персональных данных;
 - **перечень обрабатываемых персональных данных:** фамилия; имя; отчество; возраст; дата; месяц; год и место рождения; данные паспорта; адрес регистрации по месту жительства; адрес фактического проживания; номер телефона ; адрес электронной почты; (СНИЛС); ИНН;
 - **способы обработки персональных данных:** с использованием средств автоматизации и без использования средств автоматизации;
 - **срок обработки (исключая хранение):** до достижения цели обработки персональных данных;
 - **срок обработки (хранения):** согласно архивному законодательству;
 - **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, измельчения в сечку в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.1.8. выполнения требований законодательства, возложенных на Общество как работодателя:

- **категории субъектов, персональные данные которых обрабатываются:** работники, близкие родственники работников, бывшие работники;

- **категории обрабатываемых персональных данных:** иные и специальные категории персональных данных;

- **перечень обрабатываемых персональных данных:** фамилия; имя; отчество; возраст; дата; месяц; год и место рождения; данные паспорта; адрес регистрации по месту жительства; адрес фактического проживания; номер телефона (домашний, мобильный); адрес электронной почты; данные документов об образовании; семейное положение; сведения о детях; сведения о трудовом стаже, предыдущих местах работы; сведения о доходах с предыдущих мест работы; номер страхового свидетельства государственного пенсионного страхования (СНИЛС); ИНН; сведения о разрешительной документации на работу и проживание на территории РФ; сведения о добровольном и обязательном медицинском страховании; сведения об инвалидности; сведения о состоянии здоровья, сведения о заработной плате; фото, социальное положение; сведения о ближайших родственниках; знание иностранного языка; сведения о повышении квалификации, аттестационная категория, данные документов; профессия, квалификация; данные документов воинского учета; сведения об отпусках; сведения о льготах; информация о достижениях в профессии; сведения об ученых званиях, степенях; данные об оплате труда; сведения о банковской карте, счете; гражданство; место работы, должность;

- **способы обработки персональных данных:** с использованием средств автоматизации и без использования средств автоматизации;

- **срок обработки (исключая хранение):** до достижения цели обработки персональных данных;

- **срок обработки (хранения): 75 лет** согласно архивному законодательству;

- **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, измельчения в сечку в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.1.9. выполнения требований законодательства, возложенных на Общество как юридическое лицо:

- **категории субъектов, персональные данные которых обрабатываются:** учредитель;

- **категории обрабатываемых персональных данных:** иные категории персональных данных;

- **перечень обрабатываемых персональных данных:** фамилия, имя, отчество; год, месяц, дата рождения; место рождения; гражданство; адрес регистрации и проживания, дата регистрации по месту жительства; данные паспорта; контактный телефон; ИНН физического лица; СНИЛС, адрес электронной почты;

- **способы обработки персональных данных:** с использованием средств автоматизации и без использования средств автоматизации;

- **срок обработки (исключая хранение):** до достижения цели обработки персональных данных;

- **срок обработки (хранения): 75 лет** согласно архивному законодательству;

- **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, измельчения в сечку в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.1.10. рассмотрения кандидатуры соискателя на замещение вакантной должности:

- **категории субъектов, персональные данные которых обрабатываются:** соискатели;

- **категории обрабатываемых персональных данных:** иные категории персональных данных;

- **перечень обрабатываемых персональных данных:** фамилия, имя, отчество; номер телефона; адрес электронной почты; сведения об образовании; гражданство; место работы, должность; сведения об опыте работы; знание иностранного языка; семейное положение, сведения о владении компьютерными программами;

- **способы обработки персональных данных:** с использованием и без использования средств автоматизации;

- **срок обработки (исключая хранение):** до принятия решения о заключении трудового договора или отказе;

- **срок обработки (хранения):** 1 год с момента принятия решения об отказе в заключении трудового договора;

- **порядок уничтожения персональных данных:** уничтожение персональных данных субъектов осуществляется комиссией либо уполномоченным работником на основании приказа директора путем удаления, измельчения в сечку в соответствии с «Инструкцией по уничтожению персональных данных в ООО «Ломбард «Сантус»».

2.2. Состав и объем ПДн субъектов, необходимый Обществу, устанавливается в зависимости от категории субъекта и обрабатывается в соответствии с целями обработки и положениями соответствующего законодательства.

3. ОСОБЕННОСТИ ОБРАБОТКИ ПДн РАБОТНИКОВ

3.1. Порядок обработки ПДн работников устанавливается с соблюдением требований Трудового кодекса Российской Федерации и иных федеральных законов.

3.2. В целях обеспечения прав и свобод человека и гражданина Общество и его представители, при обработке ПДн работника обязаны соблюдать следующие требования:

- 1) обработка ПДн работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- 2) при определении объема и содержания обрабатываемых ПДн работника необходимо руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

- 3) все ПДн работника следует получать у него самого. Если ПДн работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Общество должно сообщить работнику о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа работника дать письменное согласие на их получение;

- 4) Общество не имеет права получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области ПДн к специальным категориям ПДн, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами;

5) Общество не имеет права получать и обрабатывать ПДн работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, Общество не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита ПДн работника от неправомерного их использования или утраты обеспечивается Обществом за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами Общества, устанавливающими порядок обработки ПДн работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) Общество, работники и их представители должны совместно вырабатывать меры защиты ПДн работников.

Передача ПДн работника

3.3. При передаче ПДн работника необходимо соблюдать следующие требования:

- не сообщать ПДн работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, установленных Трудовым кодексом Российской Федерации или иными федеральными законами;

- предупредить лиц, получающих ПДн работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн работника, обязаны соблюдать их конфиденциальность. Данное положение не распространяется на обмен ПДн работников в порядке, установленном трудовым кодексом Российской Федерации и иными федеральными законами;

- разрешать доступ к ПДн работников только специально уполномоченным лицам, имеющим к ним допуск, при этом указанные лица должны иметь право получать только те ПДн работника, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- осуществлять передачу ПДн работника в пределах Общества в соответствии с настоящим Положением, иными локальными нормативными актами, с которыми работник должен быть ознакомлен под роспись;

- передавать ПДн работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, иными федеральными законами, и ограничивать эту информацию только теми ПДн работника, которые необходимы для выполнения указанными представителями их функций;

- не сообщать ПДн работника в коммерческих целях без его письменного согласия.

- передача ПДн работников допускается в объемах, необходимых для выполнения задач, соответствующих причине сбора этих данных.

Обязанности работника.

3.4. Работник обязан:

- предоставить Обществу или его представителю документы, содержащие ПДн, состав которых установлен Трудовым кодексом Российской Федерации и иным законодательством, регулирующим трудовые правоотношения;

- в срок, не превышающий 5 рабочих дней, лично либо через своего представителя сообщать лицу, ответственному за ведение кадрового делопроизводства, об изменении своих персональных данных и представить подтверждающие документы.

Права работника.

3.5. В целях обеспечения защиты ПДн, хранящихся у Общества, работники имеют право на:

- полную информацию об их ПДн и обработке этих данных;

- свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих ПДн;

- доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

- требование об исключении или исправлении неверных или неполных ПДн, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. При отказе Общества исключить или исправить ПДн работника он имеет право заявить в письменной форме Обществу о своем несогласии с соответствующим обоснованием такого несогласия;

- дополнение ПДн оценочного характера заявлением, выражающим собственную точку зрения;

- требование об извещении Обществом всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия Общества при обработке и защите его ПДн.

4. ПОРЯДОК ОБРАБОТКИ ПДн СУБЪЕКТОВ

4.1. Обработка ПДн субъектов должна осуществляться с соблюдением принципов и правил, предусмотренных законодательством.

4.2. Организацию и контроль за порядком обработки и защитой ПДн субъектов в структурных подразделениях Общества, работники которых обрабатывают ПДн, осуществляют их непосредственные руководители.

4.3. Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено законодательством, на основании заключаемого с этим лицом договора (контракта). Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные законодательством, соблюдать конфиденциальность ПДн, принимать необходимые меры, направленные на

обеспечение выполнения обязанностей, предусмотренных законодательством. В поручении оператора должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона «О персональных данных», обязанность по запросу Общества в течение срока действия поручения, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Общества установленных требований, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона «О персональных данных», в том числе требование об уведомлении Общества о случаях, предусмотренных частью 3.1 статьи 21 указанного федерального закона.

4.4. Уничтожение персональных данных (носителей, содержащих ПДн), производится в соответствии с локальными актами Общества.

Помещения, в которых обрабатываются ПДн субъектов

4.5. ПДн субъектов обрабатываются в структурных подразделениях Общества по направлениям деятельности. В целях выполнения своих трудовых обязанностей ПДн субъектов могут обрабатываться как на бумажных носителях, так и в электронном виде.

4.6. Помещения, в которых ведется обработка ПДн субъектов, их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в них носителей, содержащих ПДн.

4.7. Помещения, в которых обрабатываются ПДн субъектов, при отсутствии в них работников должны быть заперты.

Особенности обработки ПДн без использования средств автоматизации

4.8. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее - материальные носители), в специальных разделах или на полях форм (бланков).

4.9. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых, заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

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

а) при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное

копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

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

4.11. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). В таком случае составляется акт, утверждаемый директором Общества.

4.12. Уточнение ПДн 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 ПДн.

4.13. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн 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 Обществом.

4.14. При работе с материальными носителями, содержащими ПДн, работники Общества должны исключить несанкционированный к ним доступ, соблюдая следующие правила:

- при угрозе несанкционированного доступа к материальным носителям, содержащим ПДн, работник обязан исключить возможность визуального съема информации с них и убрать носитель(и) в запираемый шкаф (сейф и т.п.);

- покидая рабочее место, все материальные носители, содержащие ПДн, должны убираться в запираемый шкаф (сейф и т.п.);

- работник обязан принимать иные меры в соответствии со сложившейся ситуацией, исходя из обязанности исключения несанкционированного доступа к материальным носителям, содержащим ПДн.

4.15. Работники, осуществляющие обработку ПДн без использования средств автоматизации, должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Общества.

Особенности обработки ПДн в ИСПДн

4.16. Общество при обработке ПДн в ИСПДн обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

4.17. Порядок обработки ПДн в ИСПДн Общества регламентируется настоящим Положением и иными локальным нормативными актами Общества в области технической защиты ПДн.

4.18. Допуск к обработке ПДн в ИСПДн имеют работники согласно «Перечню должностей работников, доступ которым к персональным данным необходим для исполнения трудовых обязанностей в ООО «Ломбард «Сантус». Доступ работников в ИСПДн реализуется посредством технических средств и способов, не противоречащих законодательству Российской Федерации.

4.19. Использование средств вычислительной техники для обработки ПДн в ИСПДн допускается только после выполнения требований безопасности информации.

4.20. Обеспечение безопасности ПДн достигается, в частности:

- 1) определением угроз безопасности ПДн при их обработке в ИСПДн;
- 2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- 5) учетом машинных носителей ПДн;
- 6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
- 7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- 9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

4.21. При проведении технического обслуживания и ремонта техники, в которой ведется обработка ПДн, запрещается передавать ремонтным организациям блоки с элементами накопления и хранения ПДн.

4.22. Машинные носители, содержащие ПДн (несъемные диски - жесткие диски; съемные носители: гибкие магнитные диски, съемные пакеты дисков, иные магнитные, оптические или магнитно-оптические диски и т.п.) до начала работы регистрируются ответственным работником с проставлением реквизитов, идентифицирующих каждый носитель.

4.23. Доступ работников в ИСПДн реализуется посредством технических средств и способов, не противоречащих законодательству Российской Федерации.

4.24. Работники, обрабатывающие ПДн в ИСПДн, обязаны соблюдать следующие требования:

- проверять все новые данные на наличие вирусов;
- никому не сообщать (не передавать) сведения о доступе (логин, пароль);
- не оставлять без контроля включенным автоматизированное рабочее место;

- при оставлении рабочего места программное обеспечение, используемое при обработке ПДн в ИСПДн, переводится в режим работы, исключающий доступ к информации без ввода пароля или идентификатора.

4.25. Общество производит регулярное резервное копирование данных в ИСПДн. Лицо, ответственное за резервное копирование, назначается директором Общества. Порядок резервного копирования устанавливается локальными актами Общества.

4.26. Общество обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ

Права субъектов ПДн

Субъект ПДн обладает правами, предоставленными законодательством.

5.1. Субъект ПДн имеет право:

5.1.1. на получение сведений, указанных в п. 5.1.3 настоящего Положения, за исключением случаев, когда право субъекта на доступ к его ПДн ограничено в соответствии с федеральными законами;

5.1.2. требовать от Общества уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

5.1.3. при обращении или направлении запроса¹ требовать от Общества предоставления сведений о наличии его ПДн в доступной форме. При этом в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Запрос должен отвечать требованиям пункта 3 статьи 14 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных». При этом подлежит предоставлению следующая информация:

- 1) подтверждение факта обработки ПДн субъекта в Обществе;
- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые способы обработки ПДн;
- 4) наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Обществом или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;

¹ С данным запросом вправе обратиться представитель субъекта ПДн.

7) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

8) информацию об осуществляемой или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Общества, если обработка поручена или будет поручена такому лицу;

10) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;

11) иные сведения, предусмотренные Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Общество предоставляет вышеуказанные сведения субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе, в течение 10 рабочих дней с момента обращения либо получения запроса субъекта или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Обществом в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.1.4. на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.1.5. на обжалование действий или бездействия Общества в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

5.2. После предоставления необходимых сведений субъекту ПДн по его запросу, последний вправе обратиться повторно в Общество или направить ему повторный запрос о предоставлении данных, не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством, нормативно-правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

5.3. Субъект ПДн вправе обратиться повторно в Общество или направить ему повторный запрос в целях получения необходимых сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в п. 5.2 настоящего Положения в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос наряду со сведениями, предусмотренными законодательством, должен содержать обоснование его направления.

5.4. Общество вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным законодательством. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Обществе.

6. ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ И ЗАЩИТЫ ПДн

6.1. К информации, содержащей ПДн субъектов, применяется режим конфиденциальности, то есть обязательное для соблюдения получившим доступ к ПДн субъектов лицом требование

не раскрывать третьим лицам и не допускать их распространения без согласия субъекта ПДн или иного законного основания.

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

Защита ПДн направлена на предупреждение нарушения порядка доступа к ПДн, обеспечение сохранности носителей, содержащих ПДн, обеспечение достоверности ПДн и соблюдение режима конфиденциальности ПДн.

6.3. Конфиденциальность и защита ПДн обеспечиваются путем принятия Обществом следующих мер:

- определение перечня ПДн субъектов, обрабатываемых в Обществе;
- ограничение доступа к ПДн путем определения должностных лиц, допущенных к обработке ПДн;
- определение работников, ответственных за: организацию обработки ПДн; реализацию мер, необходимых для обеспечения условий для сохранности персональных данных и исключения несанкционированного к ним доступа; обеспечение безопасности ПДн в информационной системе; распределение между ними соответствующих обязанностей;
- регламентация правил обработки ПДн субъектов путем установления порядка работы с этой информацией и контроля за его соблюдением;
- учет лиц, получивших доступ к ПДн субъектов, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию ПДн субъектов в рамках договорных отношений;
- выявление возможных каналов несанкционированного доступа к ПДн субъектов, обеспечение безопасности информации при обработке ПДн субъектов с использованием средств вычислительной техники;
- исключение бесконтрольного использования средств обработки ПДн субъектов посторонними лицами;
- определение помещений, в которых ведется работа с ПДн субъектов, исключение бесконтрольного доступа посторонних лиц в эти помещения;
- определение мест обработки (хранения) материальных носителей, содержащих ПДн;
- использование необходимых средств технической защиты информации в ИСПДн;
- организация надлежащего порядка уничтожения ПДн, их материальных носителей;
- своевременное выявление нарушения требований разрешительной системы доступа работниками к определенным сведениям;
- проведение воспитательной и разъяснительной работы с работниками по предупреждению нарушения норм законодательства, регулирующего обработку ПДн, обучение;
- принятие иных мер, не противоречащих законодательству.

6.4. Право доступа к ПДн имеют работники, занимающие соответствующие должности согласно «Перечню должностей работников, доступ которым к персональным данным необходим для выполнения трудовых обязанностей в ООО «Ломбард «Сантус»».

Работники Общества обрабатывают ПДн только в том объеме, который необходим им для выполнения своих трудовых обязанностей.

6.5. При обработке ПДн работники должны обеспечивать безопасность носителей, содержащих ПДн, находящихся в их распоряжении.

6.6. Работники, обрабатывающие ПДн, обязаны обеспечивать их конфиденциальность, соблюдать требования законодательства, настоящего Положения и иных локальных актов Общества, обеспечивать защиту ПДн от несанкционированного доступа.

6.7. Работникам, осуществляющим обработку ПДн, запрещается оставлять вне контроля материальные носители и средства обработки ПДн. При оставлении рабочего места материальные носители убираются в запираемые шкафы, сейфы и т.п., а программное обеспечение, используемое при обработке ПДн в ИСПДн, переводится в режим работы, исключающий доступ к информации без ввода пароля или идентификатора.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПДн

7.1. Работник, обрабатывающий ПДн, несет ответственность за нарушение установленного порядка и правил обработки.

7.2. Руководитель подразделения осуществляет контроль за обработкой ПДн работниками в своем подразделении.

7.3. В случае нарушения норм, регулирующих обработку и защиту ПДн, работник может быть:

-привлечен к дисциплинарной и материальной ответственности в порядке, установленном трудовым кодексом Российской Федерации и иными федеральными законами;

-привлечен к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.4. По факту нарушения правил обработки ПДн, а также установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, может быть организовано служебное расследование.

8. ПРОВЕДЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ И (ИЛИ) АУДИТА СООТВЕТСТВИЯ ОБРАБОТКИ ПДн ЗАКОНОДАТЕЛЬСТВУ, ТРЕБОВАНИЯМ К ЗАЩИТЕ ПДн, ПОЛИТИКЕ ОБЩЕСТВА В ОТНОШЕНИИ ОБРАБОТКИ ПДн, ЛОКАЛЬНЫМ АКТАМ

8.1. Внутренний контроль и (или) аудит соответствия обработки ПДн законодательству о ПДн, требованиям к защите ПДн, политике Общества в отношении обработки ПДн, локальным актам, осуществляется с целью изучения и оценки фактического состояния соблюдения правил обработки ПДн, обеспечения надлежащей защиты ПДн, выявления недостатков и нарушений, выработки предложений, направленных на их устранение и предотвращение.

8.2. Контрольные мероприятия проводятся ответственным за организацию обработки ПДн в Обществе либо образуемой комиссией из числа работников, имеющих допуск к ПДн, согласно утвержденному директором Общества ежегодному плану в соответствии с «Правилами осуществления внутреннего контроля и(или) аудита соответствия обработки персональных данных законодательству, требованиям к защите персональных данных, политике ООО

«Ломбард «Сантус» в отношении обработки персональных данных, локальным актам». При необходимости, может быть проведена внеплановая проверка.

Проведение проверки не должно приводить к необоснованному ознакомлению с ПДн участвующих в ней лиц.

8.3. По результатам проверки составляется отчет с отражением в нем состояния дел в Обществе, по соблюдению требований законодательства, регламентирующего обработку ПДн, выявленных недостатков и нарушений правил обработки ПДн, предложений по их устранению.

8.4. Отчет предоставляется директору Общества. На основании представленного отчета директор определяет ответственных работников и сроки для устранения выявленных нарушений, недостатков, принимает иные необходимые решения.

8.5. После устранения всех нарушений ответственным за организацию обработки ПДн составляется об этом акт.


9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно до замены его новым.

9.2. Настоящее Положение обязательно для всех работников Общества.

9.3. Все работники Общества должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

Ответственный за организацию
обработки персональных данных



(подпись) /Е.С. Васильева/