Утверждаю:

Директор ООО « Ломбард Инвест»

Жаринова Олеся Андреевна 01.09.2022 г.

Положение о защите информации и работе с персональными данными граждан в ломбарде

I. Общие положения

1.1. Положение о работе с персональными данными граждан (далее - Положение) определяет политику ООО «Ломбард Инвест» (далее - Общество), в отношении :

- обработки персональных данных;

- порядок получения, учета, обработки, комбинирования;

- использования и хранения персональных данных граждан с использованием средств автоматизации;

-порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований;

- принятие правовых, организационных и технических мер по защите информации и обеспечению безопасности персональных данных при их обработке.

1.2. Положение разработано на основании:

- Конституции Российской Федерации,

- Федерального закона "О персональных данных" от 26 июля 2006г. № 152-ФЗ,

- Федерального закона «О ломбардах» от 19 июля 2007г. № 196-ФЗ,

- Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" №115-ФЗ,

- Постановления Банка России 757-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций "

- и др. нормативно-правовых актах.

1.3. Персональные данные граждан (далее персональные данные) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе фамилия, имя, отчество, год, месяц, дата рождения, данные паспорта или иного документа удостоверяющего личность в соответствии с законодательством РФ.

1.4. Общество является оператором, организующим и осуществляющим обработку персональных данных граждан, а также определяющим цели и содержание обработки персональных данных.

1.5. Цель разработки Положения - обеспечение прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайны.

1.6. Положение о защите информации и работе с персональными данными граждан в ломбарде является основой для реализации правильного и эффективного способа минимизации возможных появлений в деятельности финансовой организации неприемлемых для нее операционных рисков, связанных с нарушением безопасности информации, и являются принятым и контролируемым руководством финансовой организации документом, определяющим:

- политику обеспечения защиты информации финансовой организации;

- область применения системы защиты информации, описанной как перечень бизнес-процессов, технологических процессов и (или) баз данных финансовой организации;

- целевые показатели величины допустимого остаточного операционного риска, связанного с нарушением безопасности информации.

- цели и задачи защиты информации;

- основные типы защищаемой информации;

- основные принципы и приоритеты выбора организационных и технических мер системы защиты информации и системы организации и управления защитой информации;

- положения о выделении необходимых и достаточных ресурсов, используемых при применении организационных и технических мер, входящих в систему защиты информации.

II. **Обработка персональных данных**

2.1. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, обезличивание, блокирование, уничтожение персональных данных.
В процессе обработки персональных данных Общество использует базы данных, находящиеся только на территории Российской Федерации.

2.2. Обществом обрабатываются персональные данные следующих категорий субъектов:
- Физические лица, находящиеся с Обществом в трудовых правоотношениях.
- Физические лица, вступающие в договорные отношения с Обществом в договорные отношения при получении краткосрочных займов, при реализации невостребованных вещей в ломбарде.
- Физические лица – представители организаций (ИП) вступающие в договорные отношения с Обществом
Обработка персональных данных несовершеннолетних Обществом не осуществляется.
Общество применяет смешанный способ обработки персональных данных с использованием средств автоматизации, включающий :
- предоставление документов удостоверяющих личность
- проверку персональных данных и документов

- внесение и использование в локальные (не облачные) автоматизированные базы данных в целях, изложенных в пункта 2.3 и 2.4

2.3. Обработка персональных данных физических лиц, находящиеся с Обществом в трудовых правоотношениях обрабатываются в целях исполнения трудового и налогового законодательства Российской федерации, смешанным способом, в том числе при помощи локального программного обеспечения необходимого для ведения налогового и бухгалтерского учета;
Сроки обработки и хранения, указанных в настоящем пункте данных определяются продолжительностью трудовых правоотношений с субъектом персональных данных;
Порядок их уничтожения определяется пунктом 5.2.6. настоящего положения.

2.4. Обработка персональных данных физических лиц, вступающие в договорные отношения с Обществом в договорные отношения по поводу получения краткосрочных займов, при реализации невостребованных вещей в ломбарде, представителей организаций (ИП) вступающие в договорные отношения с Обществом обрабатываются:
- в целях исполнения Законодательства российской Федерации о ломбардах,
- уголовно процессуального законодательства,
- а также №115-ФЗ « О ПОД/ФТ»,
смешанным способом, в том числе ,путем внесения указанных данных в локальную базу данных;
Сроки обработки и хранения, указанных в настоящем пункте данных, а также порядок их уничтожения определяются пунктом 5.2.6.-5.2.7. настоящего положения.

2.5.Обработка персональных данных должна осуществляться на законной и справедливой основе.

2.6. Обработка персональных данных осуществляется **с письменного получения согласия субъекта персональных данных**, поскольку указанное необходимо для исполнения договора, стороной которого и выгодоприобретателем является субъект персональных данных, и с целью обработки первичной бухгалтерской документации, исполнение законодательства « о ломбардах», «о потреб. займе», «ПОД/ФТ», «о бухгалтерском учете», Трудового Кодекса РФ, Налогового Кодекса РФ, « о ДМ и ДК» , Постановлений Правительства « о ГИИС».

Договор «Залоговый билет», Трудовой договор, иной документ, содержащий персональные данные, включает в себя Согласие в письменной форме субъекта персональных данных на обработку его персональных данных ,в том числе согласно требованиям п. 4 ст.9 №152-ФЗ:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, **если обработка будет поручена такому лицу;**

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

2.7. Общество вправе поручить обработку персональных данных другому лицу **с согласия субъекта персональных данных**, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение оператора).

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных №152-ФЗ «О персональных данных» (далее №152-ФЗ).

В поручении оператора должны быть определены:
- перечень персональных данных,
- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных,
- цели их обработки,
- должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 №152-ФЗ,
- обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии со статьей 6 №152-ФЗ,
- обязанность обеспечивать безопасность персональных данных при их обработке,
- а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 №152-ФЗ, в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 №152-ФЗ.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет

оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

2.8. Общество не планирует поручать , не поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу.

2.9. **Обществом не осуществляется**:

- обработка и (или) распространение персональных данные, разрешенные субъектом персональных данных для распространения.

-обработка биометрических данных, либо специальных категорий персональных данных,

- трансграничная передача персональных данных,

- исключительно автоматизированная обработка персональных данных,

- сбор персональных данных на страницах принадлежащего Обществу сайта в информационно-телекоммуникационной сети "Интернет", не используется онлайн технологии для подачу онлайн заявок на заем и связанную с этим обработку персональных данных заявителей.

- обработка персональных данных в облачных информационных системах,

- создание общедоступных источников персональных данных,

- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи (таргетирование), а также в целях политической агитации,

- получение не от субъекта персональных данных.

2.10. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

2.11. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, исключительно на территории РФ, в служебных помещениях общества.

2.12. Не допускается обработка персональных данных граждан, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

2.13. Персональные данные гражданина не могут быть использованы в целях причинения ему имущественного и морального вреда, затруднения реализации его прав как гражданина Российской Федерации.

2.14. Обществом разъясняются субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

2.14 Перечень лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных утверждается руководителем Общества.

III. Права субъекта персональных данных

3.1. Субъект персональных данных имеет право на получение персональных данных имеющихся в распоряжении Общества.

3.2. Субъект персональных данных 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 законом меры по защите своих прав.

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

1) подтверждение факта обработки персональных данных Обществом;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Обществом способы обработки персональных данных;

4) наименование и место нахождения Общества, сведения о лицах (за исключением работников Общества), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Обществом 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 законом;

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) меры, направленные на обеспечение выполнения Обществом обязанностей, предусмотренных Федеральным законом, изложенные в настоящем Положении.

Сведения настоящего пункта предоставляются субъекту персональных данных или его представителю Обществом в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя, в том числе с учетом ст. 14 N 152-ФЗ "О персональных данных".

3.4. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

3.5. Субъект персональных данных имеет право в любое время, в том числе до начала обработки персональных данных ознакомиться с документом, определяющим политику Общества в отношении обработки персональных данных.

IV Обязанности Общества в отношении обработки персональных данных.

4.1.Общество сообщает в порядке, предусмотренном ст. 14 N 152-ФЗ "О персональных данных", субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными информацию, предусмотренную частью 7 ст. 14 N 152-ФЗ "О персональных данных" в порядке пункта 3.3 Положения, при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя.
Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Предоставляемая информация не должна содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Общество обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 ст. 14 N 152-ФЗ "О персональных данных" или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Обществом в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.3. Общество в срок не превышающий семи рабочих дней со дня, предоставления субъектом персональных данных или его представителем сведений, или по запросу РКН , подтверждающих, **что персональные данные являются неполными, неточными или неактуальными**, обеспечивает внесение в них необходимых изменений, в том числе блокирование неточных персональных данных.

4.4. 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**, Общество обязано уничтожить такие персональные данные.

4.5. Общество обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах.

4.6. В случае **выявления неправомерной обработки персональных данных** при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо РКН, Общество обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки.
В случае выявления неправомерных действий с персональными данными необходимо в срок, не превышающий трех рабочих дней с даты такого выявления, устранить допущенные нарушения.

В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней от даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

В случае устранения нарушений или уничтожении персональных данных уведомляет субъекта персональных данных или его законного представителя, РКН.

4.7. **В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа)** персональных данных, повлекшей нарушение прав субъектов персональных данных, Общество обязано с момента выявления такого инцидента самостоятельно, РКН или иным заинтересованным лицом уведомить РКН:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Обществом на взаимодействие с РКН, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

4.8. В случае достижения цели обработки персональных данных или окончания срока действия согласия субъекта ПД необходимо незамедлительно прекратить их обработку и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

4.9. В случае подачи субъектом персональных данных заявления на уничтожение своих персональных данных необходимо прекратить их обработку и уничтожить персональные

данные в срок, не превышающий тридцати дней с даты поступления указанного заявления, если сохранение персональных данных более не требуется для целей обработки персональных данных, в том числе с учетом требований федеральных законов.
Об уничтожении (невозможности уничтожения) персональных данных нужно уведомить субъекта персональных данных.

4.10.В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 4.7- 4.9 Положения, Общество осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

4.11. В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), **за исключением случаев**, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 настоящего Федерального закона, в том числе применимо к деятельности Общества пунктами ч.1 ст 6 :

- 2) обработка персональных данных **необходима для достижения целей законом**, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей
- 5) обработка персональных данных **необходима для исполнения договора**, 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.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Обществом в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

4.12. Сотрудники Общества обрабатывают персональные данные в соответствии с обязанностями, установленными федеральными законами, перечисленными в п.2.3-2.4 и разъясняют субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

При сборе персональных данных Общество обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) персональных данных граждан Российской Федерации с использованием баз данных в порядке п. 2 Положения и Раздела V Применяемые меры выполнения обязанностей оператора, защиты информации, обеспечения безопасности персональных данных.

4.13. Общество обеспечивает беспрепятственный доступ к настоящему Положению, определяющему его политику в отношении обработки персональных данных и обеспечении их конфиденциальности (сохранности), реализуемые требованиях к защите персональных данных.

Доступ обеспечен в местах обслуживания клиентов, путем ознакомления работников Общества, ознакомления иных лиц по запросу.

4.14. Общество обязано принимать правовые, организационные и технические меры, необходимые и достаточные для обеспечения выполнения обязанностей возложенных на него Федеральным законом.

В случае изменения сведений, указанных в Уведомлении об обработке персональных данных ранее направленных в РКН, а также в случае прекращения обработки персональных данных Общество обязано уведомить об этом РКН в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

4.15. Общество предоставляет настоящее Положение, документы и локальные акты, подтверждающие принятие мер, направленных на обеспечение выполнения обязанностей, по запросу РКН.
Общество сообщает в РКН по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса.
Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Обществу в адрес РКН мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

V. Применяемые меры выполнения обязанностей оператора, защиты информации, обеспечения безопасности персональных данных.

5.1. Общество при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает защиту 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.

Общество обеспечивает 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, в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

5.2. В целях обеспечения выполнения обязанностей оператора,защиты информации и безопасности персональных данных Обществом принимаются следующие меры:

а) Назначается лицо ответственное за организацию обработки персональных данных.

б) Утверждение настоящего Положения определяющих :

-политику оператора в отношении обработки персональных данных,

- цели обработки персональных данных категории

- перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются,

- способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований,

- мер по обеспечению безопасности персональных данных,

- процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

- оценку уровня защиты информации и обеспечения безопасности персональных данных, с учетом потенциальных угроз защиты информации и вреда, который может быть причинен субъектам персональных данных.

б) Электронные носители персональных данных обеспечиваются антивирусной защитой.

в) Обществом обеспечивается целостность информационной системы и персональных данных, предотвращение вторжений в базы содержащие персональные данные и информацию.

г) Обществом обеспечивается защита среды виртуализации.

д) Обществом обеспечивается защита технических средств.

е) Обществом определяется перечень должностей осуществляющих обработку персональных данных (**Приложение 1** к положению).

ж) Обществом ведется учет материальных носителей с базами данных, содержащих персональные данные (**Приложение 2** к положению), в том числе с учетом «Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» (утв. Постановлением Правительства РФ от 6 июля 2008 г. N 512)

5.2.1. На лицо ответственное за организацию обработки персональных данных возлагаются обязанности по осуществлению внутреннего контроля соответствия обработки персональных данных настоящему Федеральному закону, требованиям к защите персональных данных, политике Общества.

Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации (Директора Общества).

5.2.2. Лицом ответственное за организацию обработки персональных данных, проводится ознакомление работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных и в том числе требованиями к защите персональных данных и информации, документами, определяющими политику Общества в отношении обработки персональных данных и защиты информации и (или) обучение указанных работников.

4. Лицо, ответственное за организацию обработки персональных данных, организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов, а также взаимодействие с РКН.

5.2.3. Обществом обеспечивается конфиденциальность обрабатываемых персональных данных в соответствии ст. 7 №152-ФЗ « О персональных данных» и ст. 3 №196-ФЗ «О ломбардах», **по которому обязано не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.**

5.2.4. Обществом в процессе обработки персональных данных используется оборудование исключающее возможность несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

5.2.5. Обществом обеспечивается техническая возможность восстановления персональных данных, модифицированных или уничтоженных в случае несанкционированного доступа к ним.

Лицом ответственным за организацию обработки персональных данных организуется еженедельное резервное копирование данных, используемых ломбардом в процессе осуществления ломбардной деятельности.

5.2.6. Бухгалтерские документы, содержащие персональные данные, по истечении предельного срока хранения бухгалтерской документации, подлежат уничтожению под контролем лица ответственное за организацию обработки персональных данных.

5.2.7. Базы данных , содержащие персональные данные хранятся, в целях исполнения Федерального закона №115-ФЗ "О ПОД/ФТ» , не менее пяти лет, после чего подлежат уничтожению под контролем лица ответственное за организацию обработки персональных данных.

5.3.Обществом применяются меры защиты, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой информации**:**

5.3.1. К защищаемой обществом информации относится:

- информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде сотрудникамиОбщества и (или) клиентами;
- информация, необходимая Обществу для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами или иным имуществом;
- информация об осуществленных Обществом и клиентами финансовых операциях;
- ключевая информация средств криптографической защиты информации, используемой Обществом и клиентами при осуществлении финансовых операций.

5.3.2. Усиленный, стандартный , минимальный уровни защиты **информации не являются обязательными** к реализации Обществом в процессе осуществления деятельности ломбарда , согласно Положению Банка России от 20 апреля 2021 г. N 757-П.

Согласно требованиям национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер" Обществом применяются **компенсирующие меры защиты информации** с учетом специфики деятельности и п. 6.4 ГОСТ Р 57580.1-2017.

При невозможности технической реализации отдельных выбранных мер защиты информации, а также **с учетом экономической целесообразности** на этапах адаптации (уточнения) базового состава мер могут разрабатываться **иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности информации**, определенных в модели угроз, и нарушителей безопасности информации финансовой организации.

В этом случае финансовой организацией должно быть проведено обоснование применения компенсирующих мер защиты информации.

Применение компенсирующих мер защиты информации **(компенсирующего уровня защиты)** направлено на обработку операционного риска, связанного с реализацией угроз безопасности информации, на нейтрализацию таких угроз и вреда.

5.3.3. Защита информации осуществляется посредством реализации Обществом следующих мер:

- ограничение доступа к аппаратным средствам и регламентации доступа пользователей к сетевым ресурсам;
- разграничение прав на уровне прикладных программ;
- ообеспечение защиты целостности и достоверности финансовой информации при работе с электронными финансовыми документами;
- обеспечение защиты при передаче финансовой информации.

5.3.3.1 Ограничение доступа к аппаратным средствам достигается путем расположения компьютерного оборудование в местах, исключающих возможность доступа посторонних лиц. Компьютеры (рабочие места в обособленных подразделениях), на которых обрабатывается финансовая информация клиентов располагаются в помещениях, в которые имеет доступ ограниченный круг сотрудников имеющих электронные ключи от охранной сигнализации, для доступа в указанные помещения, а также сотрудников автоматизации Общества.

Список таких сотрудников предоставляется в охранное предприятие, осуществляющее охрану вышеуказанных помещений.
Порядок использования Организацией сети интернет исключает несанкционированное подключение к устройствам обработки и хранения финансовой информации клиентов.

Обособленные подразделения оснащены пожарно-охранной сигнализацией, круглосуточно находятся под централизованной охраной в лицензированных предприятиях, что обеспечивает защиту от несанкционированного доступа третьих лиц к материальных носителям информации с данными клиентов и их операций.

5.3.3.2 Обществом используется следующее разграничение прав на уровне прикладных программ:

- Доступ к программному обеспечению, с использованием которого осуществляется заключение договоров с клиентами, обработка и хранение финансовой информации клиентов имеют исключительно **операционисты, менеджеры** Общества, а также сотрудники автоматизации Общества согласно должностным обязанностям, закрепленным в инструкциях.

- Прочие специалисты Общества, включая бухгалтерию Общества используют в своей работе сводную аналитическую информацию, предоставляемую им **операционистами и (или)менеджерами** Общества без персонификации указанной информации о клиентах.

- Доступ к программному обеспечению, на основе которого проводятся финансовые операции Общества без персонификации указанной информации о клиентах имеет главный бухгалтер.

- Доступ к программному обеспечению, используемому к передаче информации Банку России и Федеральной Службе по Финансовому Мониторингу имеет **ответственный сотрудник (специальное должностное лицо)**.

5.3.4. Обществом обеспечивается защита передаваемой информации с помощью СКЗИ соответствующей с технической документации на СКЗИ, ГОСТ Р 34.10-2012, а также федеральным законам и нормативным правовыми актами Российской Федерации.

Общество применяет СКЗИ российского производства, СКЗИ имеет сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

VI Перечень информационных систем персональных данных

Персональные данные обрабатываются Обществом при помощи следующих информационных систем:

1. Программное обеспечение персональных компьютеров.

2. Базы данных используемые для обслуживания клиентов и исполнения законодательства.

3. Бухгалтерское и учетное программное обеспечение.

VII Ответственность.

7.1. Лица, виновные в нарушении требований Федерального закона "О персональных данных" от 26 июля 2006г. № 152-ФЗ, несут предусмотренную законодательством Российской Федерации ответственность.

КоАП включает наказание по ст. 5.39 (отказ в предоставлении информации), 13.11 (нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)), 13.12 (нарушение правил защиты информации), 13.13 (незаконная деятельность в области защиты информации) и 13.14 (разглашение информации с ограниченным доступом)

Уголовный кодекс РФ предусматривает наказание по ст. 137, 140 и 272

7.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

УТВЕРЖДАЮ: Директор ФИО
Жаринова Олеся Андреевна

Приложение 1 к Положению о
работе с персональными данными граждан в
ООО « Ломбард Инвест»

Перечень должностей осуществляющих обработку персональных данных в ООО
« Ломбард Инвест»

В ООО «Ломбард Инвест» устанавливается следующий перечень должностей осуществляющих обработку персональных данных:
1. Главный Бухгалтер.
2. Старший кассир
3. Кассир оценщик

С Положением о работе с персональными данными граждан в ломбарде, перечнем должностей осуществляющих обработку персональных данных в ООО «Ломбард Инвест» ознакомлен, к работе принял:

_____
_____
_____

Приложение 2 к Положению о работе с персональными данными граждан в ООО ломбард « »

Журнал учета носителей баз, содержащих

персональные данные

п№	Вид (тип)носителя	Марка носителя	Заводской (инвентаризационный)№
1.	Системный блок	DNS	- - / B0009
2.	Системный блок	DNS	- - / 580001
3.	Ноутбук	Emashines E729	№ 72601 / 890007

в ООО ломбард « »

Приложение 3

Протокол

оценки уровня защиты информации

Председатель комиссии:

Члены комиссии

Рассмотрев исходные данные об информационной системе ООО ломбард « », комиссия определила:

1. Типы информации - категории общих данных в информационной системе:

2.Уровень значимости информации:

3.Актуальные угрозы для информационной системы и баз данных :

Комиссия утвердила следующее:

Председатель комиссии _____/

Члены комиссии _____/