Положение о порядке обработки персональных данных ЗАО "Сбербанк Лизинг" (Утверждено Решением Правления ЗАО "Сбербанк Лизинг" от 31.07.2013 N 23-07/13. Зарегистрировано 07.08.2013 N 075-1)

УТВЕРЖДЕНО
Решением Правления
ЗАО "Сбербанк Лизинг"
от 31.07.2013 N 23-07/13

Зарегистрировано 07.08.2013 N 075-1

ПОЛОЖЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЗАО "СБЕРБАНК ЛИЗИНГ"

Реквизиты ВНД смотри в файле Rekviziti_075_1.doc.

1. Назначение и область действия

1.1 Настоящее Положение предназначено для организации в ЗАО "Сбербанк Лизинг" (далее - Компания) процесса обработки персональных данных (далее - ПДн) согласно требованиям действующего федерального законодательства:

- Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ "О персональных данных";

- Постановление Правительства Российской Федерации от 01.11.2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2 Действие настоящего Положения распространяется на все процессы, связанные с обработкой ПДн.

1.3 Положение обязательно для ознакомления и исполнения руководителями и работниками структурных подразделений, принимающих участие в обработке ПДн, работниками Управления информационных технологий, являющимися Администраторами информационной системы персональных данных (далее - ИСПДн), Ответственным за организацию обработки ПДн, Ответственным за обеспечение безопасности ПДн, Координатором по обращениям и запросам.

1.4 Положение должно быть опубликовано для ознакомления всеми заинтересованными лицами, обработка ПДн которых проводится в Компании.

2. Субъекты ПДн

2.1 Субъектом ПДн является любое физическое лицо.

2.2 Субъекты, ПДн которых обрабатываются в Компании, относятся к следующим категориям в зависимости от целей обработки и характера договорных отношений между Компанией и субъектом ПДн:

- работники;

- кандидаты на трудоустройство;

- контрагенты (физические лица - представители юридических лиц, индивидуальные предприниматели, с которыми заключаются договоры оказания возмездных услуг);

- клиенты (физические лица - представители юридических лиц, индивидуальные предприниматели, с которыми заключаются договоры лизинга);

- члены Совета директоров, члены Ревизионной комиссии;

- посетители.

2.3 Перечень обрабатываемых ПДн для каждой категории субъектов разрабатывается Ответственным за обеспечение безопасности ПДн, утверждается Приказом генерального директора и подлежит пересмотру и уточнению ежегодно в плановом порядке и внепланово на основании информации о необходимости внесения изменений от руководителей подразделений Компании.

3. Цели обработки ПДн

3.1 Обработка ПДн работников осуществляется в целях организации кадрового учета для обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым договорам, ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральными законами, в частности: "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", "О персональных данных", а также Уставом и внутренними нормативными документами ЗАО "Сбербанк Лизинг".

3.2 Обработка ПДн кандидатов на трудоустройство осуществляется в целях замещения вакантных должностей в ЗАО "Сбербанк Лизинг".

3.3 Обработка ПДн контрагентов осуществляется на основании Гражданского кодекса РФ, Налогового кодекса РФ, в целях заключения, исполнения гражданско-правовых договоров (договоров оказания возмездных услуг (подряда)) с юридическими и физическими лицами, индивидуальными предпринимателями и иными лицами.

3.4 Обработка ПДн клиентов (физических лиц) необходима для исполнения договора, стороной которого является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн.

3.5 Обработка ПДн членов Совета директоров и ревизоров осуществляется для осуществления

прав и законных интересов ЗАО "Сбербанк Лизинг" в соответствии с Федеральным законом от 26.12.1995 г. N 208-ФЗ "Об акционерных обществах" и Устава ЗАО "Сбербанк Лизинг".

3.6 Обработка ПДн посетителей осуществляется в целях оформления заявок на пропуск посетителей на территорию ЗАО "Сбербанк Лизинг".

4. Права и обязанности Компании

4.1 Права Компании

ЗАО "Сбербанк Лизинг" как Оператор ПДн имеет право:

- отстаивать свои интересы в суде;

- предоставлять ПДн субъектов ПДн третьим лицам, если передача предусмотрена в Трудовом кодексе и иных федеральных законах Российской Федерации;

- поручать обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку ПДн по поручению Оператора ПДн, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом о защите Пдн. В поручении Оператора ПДн должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн;

- отказывать в предоставлении ПДн в случаях, предусмотренных законодательством.

4.2 Обязанности Компании

ЗАО "Сбербанк Лизинг" в соответствии с требованиями Федерального закона N 152-ФЗ "О персональных данных" обязано:

- уведомлять уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн до начала обработки ПДн;

- предоставлять субъекту ПДн информацию, касающуюся обработки его ПДн, по его запросу или в случае получения ПДн не от субъекта ПДн, уточнять, блокировать и уничтожать ПДн за исключением случаев, предусмотренных законодательством;

- назначать Ответственного за организацию обработки ПДн;

- издавать документы, определяющие политику в отношении обработки ПДн, по вопросам обработки ПДн и устанавливающие процедуры, направленные на предотвращение и выявления нарушений законодательства, устранение таких нарушений и их последствий;

- применять правовые, организационные и технические меры по обеспечению безопасности ПДн;

- осуществлять внутренний контроль и (или) аудит соответствия обработки ПДн Федеральному закону N 152-ФЗ "О персональных данных" и принятым в соответствии с ним нормативным правовым

актам, требованиям к защите ПДн, политике Компании в отношении обработки, внутренними локальными документами регламентирующими обработку и защиту ПДн;

- оценивать вред, который может быть причинен субъектам ПДн в случае нарушения Федерального закона N 152-ФЗ "О персональных данных", соотношение указанного вреда и принимаемых Компанией мер, направленные на обеспечение выполнения обязанностей, перечисленных в данном разделе;

- ознакомлять работников Компании, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, документами, определяющими политику Компании в отношении обработки ПДн, внутренними документами по вопросам обработки ПДн (настоящее Положение, "Положение о порядке организации и обеспечения безопасности персональных данных", "Инструкция работнику при работе с персональными данными", "Инструкция Администратора ИСПДн", "Положение о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных", "Положение о порядке обработки обращений субъектов персональных данных"), проводить обучение указанных работников;

- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику Компании в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн, в том числе в информационно-телекоммуникационной сети, с использованием которой осуществляется сбор ПДн;

- представлять внутренние документы по вопросам обработки ПДн и иным способом подтверждать принятие мер, перечисленных в данном разделе, по запросу уполномоченного органа по защите прав субъектов ПДн.

5. Права субъектов ПДн

5.1 Права субъектов ПДн

В соответствии с Федеральным законом N 152-ФЗ "О персональных данных" субъект ПДн имеет право:

а) получать сведения, касающиеся обработки ПДн Компанией, а именно:

1) подтверждение факта обработки ПДн Компанией;

2) правовые основания и цели обработки ПДн Компанией;

3) цели и применяемые Компанией способы обработки ПДн;

4) наименование и место нахождения Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором ПДн или на основании федерального закона;

5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки ПДн Компанией, в том числе сроки их хранения;

7) порядок осуществления субъектом ПДн прав, предусмотренных N 152-ФЗ "О персональных данных";

8) информацию об осуществленной или предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные Федеральным законом N 152-ФЗ "О персональных данных" или другими федеральными законами;

б) потребовать от Компании уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

в) обжаловать в суде любые неправомерные действия или бездействие Компании при обработке и защите его ПДн;

г) отозвать согласие на обработку ПДн в предусмотренных законом случаях.

5.2 Порядок осуществления прав

5.2.1 Обращение субъекта ПДн к оператору ПДн в целях реализации его прав, установленных Федеральным законом N 152-ФЗ "О персональных данных", осуществляется в письменном виде по установленной форме при личном визите в Компанию субъекта ПДн или его законного представителя. (Здесь и далее по тексту под субъектами ПДн понимается как сам субъект ПДн, так и его законный представитель, полномочия которого установлены Федеральным законом N 152-ФЗ "О персональных данных" либо иным законом РФ).

5.2.2 Форма обращения заполняется субъектом ПДн с проставлением собственноручной подписи. Субъект обязан предъявить документы, удостоверяющие его личность и документы, подтверждающие основания, по которым лицо выступает в качестве законного представителя субъекта ПДн.

5.2.3 Ответ на обращение отправляется субъекту ПДн в письменном виде по почте на адрес, указанный в обращении, в срок, не превышающий тридцать дней с даты получения обращения.

5.2.4 Срок внесения необходимых изменений в ПДн, являющиеся неполными, неточными или неактуальными, не может превышать семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными.

5.2.5 Срок уничтожения ПДн, являющихся незаконно полученными или не являющихся необходимыми для заявленной цели обработки, не может превышать семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.3 Ограничения прав субъектов ПДн

5.3.1 Право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если:

- обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма;

- предоставление ПДн нарушает права и законные интересы других лиц.

5.3.2 В случае если сведения, касающиеся обработки ПДн, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе направить повторный запрос в целях получения сведений, касающихся обработки ПДн, и ознакомления с такими ПДн не ранее чем через тридцать дней после 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 ПДн.

5.3.3 Субъект ПДн вправе направить Компании повторный запрос в целях получения сведений, касающихся обработки ПДн, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте 5.3.2 в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос должен содержать обоснование повторного направления.

5.3.4 Компания вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5.3.2 и 5.3.3.

6. Принципы и условия обработки ПДн

6.1 Принципы обработки ПДн

Обработка ПДн должна осуществляться на основе следующих принципов:

а) обработка ПДн должна осуществляться на законной и справедливой основе;

б) обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

в) не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместных между собой;

г) обработке подлежат только те ПДн, которые отвечают целям их обработки;

д) содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям обработки;

е) при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки;

ж) хранение ПДн должно осуществляться в форме, позволяющей определять субъект ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным

законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.2 Условия обработки ПДн

6.2.1 Обработка ПДн должна осуществляться с соблюдением принципов и правил, установленных Федеральным законом "О персональных данных". Обработка ПДн допускается в следующих случаях:

а) обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

б) обработка ПДн 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;

в) обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

г) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

д) обработка ПДн необходима для осуществления прав и законных интересов Оператора ПДн или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

е) обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн. Исключение составляет обработка ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

ж) осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе.

6.2.2 В следующих случаях (за исключением специально обговоренных в ФЗ "О персональных данных" случаев) требуется письменное согласие субъекта на обработку его ПДн:

а) включение ПДн субъекта в общедоступные источники ПДн;

б) трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн;

в) принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

6.2.3 Шаблоны согласий субъектов на обработку ПДн приведены в приложении (Приложение А).

6.2.4 При отсутствии необходимости письменного согласия субъекта на обработку его ПДн, согласие субъекта может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме.

6.2.5 Для каждого бизнес-процесса Компании, в рамках которого производится обработка ПДн и для осуществления которого требуется письменное согласие субъекта ПДн, по приведенной форме составляется отдельный шаблон согласия на обработку с указанием целей обработки ПДн в рамках данного процесса, видов ПДн и необходимого периода их хранения.

6.2.6 Компания вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (далее - поручение Оператора). Лицо, осуществляющее обработку ПДн по поручению Компании, обязано соблюдать принципы и правила обработки ПДн, предусмотренные федеральным законом. В поручении Оператора должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона N 152-ФЗ "О персональных данных". Типовые положения поручения Оператора приведены в приложении (Приложение Б).

6.2.7 В том случае, если Компания поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Компания. Лицо, осуществляющее обработку ПДн по поручению Компании, несет ответственность перед Компанией.

6.2.8 Компания и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7. Требования к обработке ПДн

7.1 Обязанности Компании при обработке ПДн

В соответствии с требованиями Федерального закона N 152-ФЗ "О персональных данных" Компания обязана:

- предоставлять субъекту ПДн по его запросу информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставить отказ (в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя);

- по требованию субъекта ПДн уточнять обрабатываемые ПДн, блокировать или удалять, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих эти факты;

- вести Журнал учета обращений субъектов ПДн, в котором должны фиксироваться запросы субъектов ПДн на получение ПДн, а также факты предоставления ПДн по этим запросам;

- уведомлять субъекта ПДн об обработке ПДн в том случае, если ПДн были получены не от субъекта ПДн (за исключением оговоренных в п/п 3 п. 4.2.1);

- в случае достижения цели обработки ПДн незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн либо если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом N 152-ФЗ "О персональных данных" или другими федеральными законами;

- в случае отзыва субъектом ПДн согласия на обработку своих ПДн прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом ПДн. Об уничтожении ПДн Компания обязана уведомить субъекта ПДн;

- в случае поступления требования субъекта о прекращении обработки ПДн в целях продвижения товаров, работ, услуг на рынке немедленно прекратить обработку ПДн.

7.2 Процессы обработки ПДн

Обработка ПДн в ИСПДн включает в себя следующие основные процессы:

- сбор ПДн;

- использование ПДн;

- хранение ПДн в ИСПДн;

- передача ПДн;

- уточнение ПДн;

- блокирование ПДн;

- уничтожение ПДн.

7.3 Сбор ПДн

При сборе ПДн необходимо руководствоваться следующими правилами:

а) ПДн следует получать лично у граждан за исключением случаев получения ПДн из общедоступных источников (в том числе справочников, адресных книг). Общедоступные ПДн - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

б) если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн следует предоставить субъекту ПДн следующую информацию: наименование и адрес Оператора ПДн или его представителя; цель обработки ПДн и ее правовое основание; предполагаемые пользователи ПДн; установленные ФЗ "О персональных данных" права субъекта ПДн; источник получения ПДн. Форма уведомления субъекта об обработке ПДн приведена в приложении (Приложение В);

в) уведомление субъекта об обработке ПДн, полученных не от него самого, не требуется в следующих случаях:

1) субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим Оператором ПДн;

2) ПДн получены Оператором ПДн на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

3) ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

4) предоставление субъекту ПДн сведений, содержащихся в Уведомлении об обработке ПДн, нарушает права и законные интересы третьих лиц;

г) при отсутствии письменного согласия запрещается получать, обрабатывать и приобщать к личному делу работника данные о его расовой, национальной принадлежности, политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах, состоянии здоровья, интимной жизни. Исключение составляют следующие случаи:

1) ПДн сделаны общедоступными субъектом ПДн;

2) обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

3) обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

4) обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;

5) обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования со страховым законодательством;

д) в Компании должны обрабатываться только те ПДн, которые удовлетворяют вышеприведенным правилам их получения.

7.3.1 Порядок сбора ПДн работников

7.3.1.1 При заключении трудового договора работник предоставляет в соответствии со ст. 65 Трудового кодекса РФ следующие сведения о себе:

- паспорт или иной документ, удостоверяющий личность;

- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые;

- страховое свидетельство государственного пенсионного страхования;

- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

7.3.1.2 В отдельных случаях Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

7.3.1.3 Работник обязан предоставлять работодателю достоверные сведения о себе и своевременно сообщать ему об изменении своих ПДн.

7.3.1.4 Компания получает письменное согласие на обработку ПДн работника в случаях передачи ПДн третьим лицам (кредитным и страховым организациям, учебным центрам, организаторам торгов).

7.3.1.5 Компания имеет право проверять достоверность сведений, предоставленных работником, сверяя данные, предоставленные работником, с имеющимися у работника документами, а также иными доступными способами.

7.3.2 Порядок сбора ПДн контрагентов (подрядных организаций)

7.3.2.1 Подрядные организации, выполняющих строительно-монтажные, ремонтные, наладочные и другие работы на объектах ЗАО "Сбербанк Лизинг", обеспечивают сбор, получение согласий субъектов ПДн для передачи их в ЗАО "Сбербанк Лизинг". Руководители организаций предоставляют ПДн субъектов (списки работников с указанием Ф.И.О., паспортных данных, профессии, должности) в целях проведения мероприятий по допуску указанных лиц на объекты ЗАО "Сбербанк Лизинг". Порядок предоставления таких сведений осуществляется в соответствии с Соглашением о конфиденциальности или иным документом, согласованным сторонами.

7.3.2.2 Типовая форма договора с организациями, выполняющими строительно-монтажные, ремонтные, наладочные и другие работы на объектах ЗАО "Сбербанк Лизинг", должна содержать обязательное условие обеспечения конфиденциальности информации, в том числе ПДн, или приложение к договору "Соглашение о конфиденциальности". Обязательным условием является обязанность обеспечения ЗАО "Сбербанк Лизинг" конфиденциальности предоставляемой информации.

7.3.3 Порядок сбора ПДн контрагентов (физических лиц, с которыми заключены гражданско-правовые договоры или планируется их заключение)

7.3.3.1 Получение ПДн контрагентов (физических лиц, индивидуальных предпринимателей, с которыми заключены гражданско-правовые договоры или планируется их заключение) осуществляется сотрудниками структурных подразделений центрального офиса и филиалов ЗАО "Сбербанк Лизинг", инициирующих/курирующих заключение договоров.

7.3.3.2 Условия получения ПДн субъектов в целях заключения, исполнения гражданско-правовых договоров определены действующим законодательством РФ.

7.3.4 Порядок сбора ПДн посетителей

7.3.4.1 Получение ПДн посетителей (представителей юридических лиц, физических лиц, индивидуальных предпринимателей, с которыми заключены гражданско-правовые договоры)) осуществляется руководителями структурных подразделений центрального офиса и филиалов ЗАО "Сбербанк Лизинг", инициирующих/курирующих исполнение договоров.

7.3.4.2 Контрагенты, направляющие представителей в центральный офис и филиалы ЗАО "Сбербанк Лизинг", предоставляют ПДн субъектов (списки работников с указанием Ф.И.О., место работы) в целях проведения мероприятий по оформлению заявок на пропуск указанных лиц на объекты ЗАО "Сбербанк Лизинг".

7.3.5 Порядок сбора ПДн членов Совета директоров, Ревизионной комиссии

Обработка ПДн членов Совета директоров, Ревизионной комиссии необходима для осуществления прав и законных интересов ЗАО "Сбербанк Лизинг" в соответствии с Федеральным законом от 26.12.1995 г. N 208-ФЗ "Об акционерных обществах". ЗАО "Сбербанк Лизинг" получает ПДн членов Совета директоров, ревизоров (членов Ревизионной комиссии) на основании письменных заявлений кандидатов на избрание. Хранение ПДн членов Совета директоров возложено на Юридическое Управление, членов Ревизионной комиссии - на Управление внутреннего аудита.

7.4 Использование ПДн

7.4.1 Использование ПДн, собранных в соответствии с разделом 7.3, в ИСПДн Компании осуществляется в соответствии с Перечнем должностей работников, допущенных к работе с ПДн, в целях принятия решений или совершения иных действий в отношении субъекта ПДн и обеспечения функционирования бизнес-процессов Компании. Шаблон указанного перечня приведен в приложении (Приложение Г). Данный перечень подлежит пересмотру и при необходимости актуализации не реже одного раза в год.

7.4.2 Список должностей работников, допущенных к работе с ПДн для каждой ИСПДн (или резервируемым информационным и аппаратным ресурсам), должен поддерживаться в актуальном состоянии. С этой целью проводятся следующие действия:

- изначально для всего комплекса ИСПДн (с указанием конкретной ИСПДн) на основании согласованных заявок на предоставление доступа Ответственным за организацию обработки ПДн формируется Перечень должностей работников, допущенных к работе с ПДн (или резервируемым информационным и аппаратным ресурсам) для выполнения своих должностных обязанностей;

- каждые полгода Перечень должностей работников, допущенных к работе с ПДн (или резервируемым информационным и аппаратным ресурсам), актуализируется Ответственным за организацию обработки ПДн путем анализа категорий работников, которым необходим доступ к ИСПДн.

7.4.3 Доступ к ПДн ограничивается в соответствии с федеральными законами РФ и настоящим Положением.

7.4.4 Работники имеют право получать только те ПДн, которые необходимы им для выполнения своих должностных обязанностей, и использовать их лишь в целях, для которых они сообщены.

7.4.5 Работники ЗАО "Сбербанк Лизинг" и третьи лица не вправе разглашать полученные ими в

результате своей профессиональной деятельности сведения о субъектах ПДн.

7.4.6 Допуск работника к ПДн может быть прекращен в следующих случаях:

- расторжение договора (независимо от причин расторжения);

- однократное нарушение взятых на себя обязательств, связанных с неразглашением и защитой ПДн;

- по инициативе ЗАО "Сбербанк Лизинг".

7.4.7 Руководители структурных подразделений ЗАО "Сбербанк Лизинг" обязаны обеспечивать контроль за допуском работников к ПДн и принимать меры по обоснованному ограничению количества лиц, имеющих доступ к соответствующим документам.

7.4.8 Доступ к ПДн органам государственной власти предоставляется в случаях, предусмотренных федеральными законами, в том числе:

- в целях предупреждения угрозы жизни и здоровья субъекта ПДн;

- в целях защиты основ конституционного строя, нравственности, прав и законных интересов других лиц;

- в целях обеспечения обороны страны и безопасности государства, в том числе при поступлении официальных запросов в соответствии с положениями Федерального закона от 12.08.1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности".

7.4.9 Доступ к ПДн на основании и во исполнение федеральных законов предоставляется:

- Федеральной инспекции труда и федеральным органам исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности;

- Федеральной налоговой службе и межрегиональным инспекциям и управлениям Федеральной налоговой службе;

- Федеральной службе государственной статистики и ее территориальным органам;

- Федеральному фонду обязательного медицинского страхования и его территориальным органам;

- Федеральной службе по финансовым рынкам;

- Военным комиссариатам;

- Фонду социального страхования РФ;

- Пенсионному фонду РФ,

- иным лицам в порядке, предусмотренном действующим законодательством.

7.4.10 В соответствии с Федеральным законом от 27.12.1991 г. N 2124-1 "О средствах массовой информации" средства массовой информации (далее - СМИ) имеют право обращаться с запросами, в ответ на которые организация обязана предоставить необходимые для СМИ сведения, если они не составляют коммерческую тайну или иную специально охраняемую законом тайну.

7.4.11 ЗАО "Сбербанк Лизинг" может предоставлять СМИ только общедоступные ПДн.

7.4.12 При получении ЗАО "Сбербанк Лизинг" запроса от СМИ в отношении сведений, составляющих ПДн, проводится экспертная оценка запрашиваемых сведений. ЗАО "Сбербанк Лизинг" готовит мотивированное заключение об отказе или предоставлении информации, касающейся ПДн в трехдневный срок со дня получения запроса.

7.4.13 Третьи лица (юридические и/или физические лица, индивидуальные предприниматели) для получения доступа к ПДн обязаны предоставить в ЗАО "Сбербанк Лизинг" в письменной форме запрос.

7.4.14 ПДн субъекта могут быть представлены третьим лицам только с письменного согласия субъекта. В письменном согласии субъекта ПДн должно быть указано третье лицо (наименование юридического лица, адрес юридического лица и/или Ф.И.О. физического лица), которому передаются ПДн, а также цель передачи и обработки ПДн.

7.4.15 В случае принятия решения о предоставлении доступа к ПДн субъекта организации и/или третьему лицу, ЗАО "Сбербанк Лизинг" направляет ответ о предоставлении информации в письменной форме.

7.4.16 Обращения (запросы) на предоставление доступа к обрабатываемым ПДн с отметкой о предоставлении информации по запросу или отказе в предоставлении информации по запросу фиксируется в соответствующем Журнале учета обращений ЗАО "Сбербанк Лизинг". Форма Журнала учета и порядок действий при обработке обращений приведены в Положении о порядке обработке обращений субъектов ПДн.

7.4.17 В случае если ЗАО "Сбербанк Лизинг" на основании договора поручает обработку ПДн другому лицу, одним из условий договора является обязанность обеспечения указанным лицом конфиденциальности данных и безопасности ПДн при их обработке.

7.4.18 Предоставление доступа к ПДн субъектов организациям, физическим лицам, которые на основании договоров осуществляют обработку ПДн, в порядке, установленном законодательством РФ, ЗАО "Сбербанк Лизинг" ограничивает эту информацию только теми ПДн, которые необходимы для выполнения указанными лицами их функций (услуг, работ).

7.5 Хранение ПДн в ИСПДн

7.5.1 Хранение ПДн в информационных системах Компании осуществляется в соответствии со следующими требованиями:

- хранение ПДн должно осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места их хранения;

- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не

дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

- запрещается несанкционированное копирование ПДн на отчуждаемые носители информации;

- при хранении ПДн в ИСПДн должны соблюдаться условия, обеспечивающие конфиденциальность и сохранность ПДн;

- несанкционированный доступ к ПДн должен быть исключен. Доступ должен быть разрешен только работникам, включенным в Перечень должностей работников, допущенных к работе с ПДн.

7.5.2 Работники Компании, обладающие правом доступа к ПДн, несут ответственность за хранение ПДн на своих автоматизированных рабочих местах.

7.6 Передача ПДн

7.6.1 Передача ПДн осуществляется в следующих случаях:

- выполнение работниками должностных обязанностей, связанных с обработкой ПДн;

- передача ПДн в рамках предприятий (банки, клиенты, контрагенты), с которыми заключены договоры, предполагающие передачу и обработку ПДн, в целях обеспечения бизнес-процессов Компании;

- передача ПДн в рамках федерального законодательства.

7.6.2 При передаче ПДн работниками Компании должны быть соблюдены следующие правила:

- несанкционированный доступ к ПДн в процессе передачи должен быть исключен;

- передача ПДн возможна только в том случае, если обеспечивается конфиденциальность передаваемой информации. Если Компания на основании договора поручает обработку ПДн третьей стороне, существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности и безопасности ПДн при их передаче;

- не сообщать ПДн субъекта ПДн третьей стороне без письменного согласия субъекта (форма согласия приведена в приложении (Приложение А) к настоящему документу), за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации и иными федеральными законами.

- не сообщать ПДн субъекта ПДн в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих ПДн субъектов ПДн, 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.

7.6.3 Передавать ПДн субъектов ПДн представителям субъектов ПДн в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми ПДн, которые необходимы для выполнения указанными представителями субъектов ПДн их функций.

7.6.4 Органам государственной власти, иным государственным органам, органам местного самоуправления, обладающим правом на получение информации, содержащей ПДн в соответствии с действующим законодательством Российской Федерации, ПДн передаются в пределах, необходимых для выполнения ими своих полномочий при мотивированном запросе.

7.6.5 Не требуется согласие работника Компании на передачу его ПДн, если передача информации или предоставление документов, содержащих ПДн, предусмотрено законодательством Российской Федерации.

7.6.6 До начала осуществления трансграничной передачи Оператор ПДн обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.

7.6.7 Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;

- предусмотренных международными договорами Российской Федерации.

7.6.8 Документы, содержащие ПДн, передаются через организации, специализирующиеся на почтовых рассылках, организацию федеральной почтовой связи (Федеральное государственное унитарное предприятие ("Почта России")), а также лично работникам сторонних организаций под подпись.

7.6.9 Электронные документы, содержащие ПДн, передаются на учтенных носителях информации и/или по телекоммуникационным каналам связи при использовании средств криптографической защиты информации.

7.7 Уточнение ПДн

7.7.1 В случае выявления работником Компании неточных ПДн или неправомерных действий с ними работник информирует о данном факте Координатора по обращениям и запросам. Координатор по обращениям и запросам инициирует выполнение действий, описанных в Положении о порядке обработки обращений субъектов ПДн.

7.7.2 В случае уточнения (изменения) ПДн необходимо известить третьих лиц, которым ранее были сообщены или переданы неверные или неполные ПДн, обо всех исключениях, исправлениях и дополнениях в них.

7.7.3 Об устранении допущенных нарушений или об уничтожении ПДн требуется уведомить субъекта ПДн или его представителя либо уполномоченный орган по защите прав субъектов ПДн в случае, если соответствующую проверку инициировал указанный орган.

7.8 Блокирование ПДн

7.8.1 В случае выявления работником Компании неправомерной обработки ПДн или выявления неточных ПДн при обращении субъекта или его представителя либо по запросу уполномоченного органа по защите прав субъектов ПДн, Координатор по обращениям и запросам инициирует блокирование ПДн, относящихся к этому субъекту ПДн, и выполнение действий, описанных в Положении о порядке обработки обращений субъектов ПДн и Положении о порядке взаимодействия с уполномоченным органом по защите прав субъектов ПДн.

7.8.2 В случаях если отсутствует возможность уничтожения ПДн, Компания осуществляет блокирование таких ПДн и обеспечивает уничтожение в срок не более чем шесть месяцев.

7.9 Уничтожение ПДн

7.9.1 ПДн подлежат уничтожению (или обезличиванию) в ИСПДн в 30-дневный срок (если иное не оговорено согласием субъекта ПДн) по достижении целей их обработки либо в случае утраты необходимости в достижении этих целей или отзыва субъектом ПДн согласия на обработку своих ПДн.

7.9.2 Об уничтожении ПДн требуется уведомить субъекта ПДн или его представителя либо уполномоченный орган по защите прав субъектов ПДн в случае, если соответствующую проверку инициировал указанный орган.

7.9.3 В случае отсутствия возможности уничтожения ПДн в течение указанного срока, ПДн должны быть заблокированы, после чего ПДн должны быть уничтожены в срок, не превышающий 6 месяцев.

7.9.4 Должен быть определен режим уничтожения ПДн после окончания периода хранения (автоматизированный, ручной).

7.9.5 ПДн, уничтожаемые в случае невозможности устранения допущенных нарушений либо в случае отзыва субъектом ПДн согласия на обработку своих ПДн, уничтожаются в ручном режиме.

7.9.6 Отбор (выделение) и уничтожение материалов, содержащих ПДн, производится Комиссией. Комиссия и ее состав назначаются приказом генерального директора ЗАО "Сбербанк Лизинг" (в центральном офисе) и приказами директоров филиалов ЗАО "Сбербанк Лизинг".

7.9.7 Отобранные к уничтожению материальные носители ПДн:

- измельчаются механическим способом на специальном оборудовании до степени, исключающей возможность прочтения текста;

- ПДн, хранящиеся на магнитных носителях, подлежат обязательному удалению путем полного форматирования носителя или уничтожения носителя на специальном оборудовании, о чем делается отметка в Журнале учета электронных носителей ПДн.

7.9.8 При необходимости обезличивания части ПДн, если это допускается материальным носителем, производится удаление (вымарывание) данных, исключающее дальнейшую обработку этих ПДн.

7.9.9 Уничтожение ПДн в ручном режиме должно оформляться Актом об уничтожении ПДн, представленным в приложении (Приложение Д).

7.10 Обеспечение конфиденциальности ПДн

7.10.1 Компания и иные лица, обладающие правом доступа к ПДн (либо в рамках выполнения должностных обязанностей или в рамках договора), обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7.10.2 Для обеспечения защиты ПДн от неправомочных действий необходимы следующие организационные меры:

- знание работниками Компании требований принятых в Компании и обязательных для ознакомления и исполнения соответствующей категорией работников нормативно-методических документов по защите информации, в том числе ПДн;

- все работники, имеющие действующие трудовые отношения, деятельность которых связана с получением, обработкой и защитой ПДн, обязаны подписать обязательство о неразглашении ПДн либо заключить дополнительное соглашение к трудовым договорам, а также быть ознакомлены под подпись с Положением о работе с ПДн;

- со всеми принимаемыми на работу работниками, деятельность которых будет связана с получением, обработкой и защитой ПДн, должны заключаться обязательства о неразглашении ПДн, в которых должны быть отражены вопросы обязанности обеспечения конфиденциальности ПДн. Положения типового договора положения о неразглашении приведен в приложении (Приложение Е)настоящего документа;

- разделение полномочий пользователей в информационных системах в зависимости от их должностных обязанностей;

- наличие формализованной процедуры по предоставлению доступа к информационным системам ПДн, а также по регулярному пересмотру (ревизии) прав доступа работников в зависимости от занимаемой ими должности.

7.10.3 Компания может передавать ПДн на обработку третьим лицам (принимающей стороне), только если это необходимо для достижения целей обработки ПДн, причем существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке.

7.10.4 В том случае, если договор был заключен до вступления в силу ФЗ "О персональных данных", либо условие конфиденциальности ПДн не было прописано по каким-либо причинам, необходимо подписывать дополнительное соглашение о неразглашении ПДн. Соглашение о неразглашении ПДн должно быть подписано до момента передачи ПДн.

7.10.5 Передача ПДн третьим лицам без заключенного соглашения и без применения мер защиты ПДн, согласно п. 3 ст. 6 Федерального закона N 152-ФЗ "О персональных данных", не допускается.

7.10.6 Положения типового договора о неразглашении ПДн приведены в приложении (Приложение Б).

8. Условия обработки ПДн, осуществляемой без использования средств автоматизации

8.1 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).

8.2 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.

8.3 Работники, осуществляющие обработку ПДн без использования средств автоматизации, до начала обработки должны быть проинформированы о факте обработке ими ПДн, о категориях ПДн, об особенностях и правилах обработки ПДн, изложенных в настоящем Положении.

8.4 В типовых формах, в которые предполагается внесение ПДн, должна содержаться следующая информация:

- цель обработки ПДн, наименование и адрес Оператора ПДн, источник получения ПДн, срок обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки;

- поле для проставления субъектом ПДн отметки о согласии на обработку ПДн без использования средств автоматизации.

8.5 Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн.

8.6 Ведение Журнала учета посетителей Компании осуществляется частным охранным предприятием, правила ведения Журнала устанавливаются организацией, ведущей Журнал.

8.7 При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- 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;

- 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.

8.8 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).

8.9 Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

8.10 Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

8.11 Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

8.12 Носители ПДн не должны оставаться без присмотра. При покидании рабочего места лица, ответственные за носители ПДн, должны убирать носители в сейф или шкаф, закрывающийся на ключ.

8.13 Хранение материальных носителей ПДн не может осуществляться в открытом доступе. Хранение материальных носителей ПДн по возможности должно осуществляться в отдельных запираемых помещениях с ограниченным доступом или в запираемых металлических или деревянных шкафах.

8.14 Доступ к архивам, хранилищам документации или специально выделенным шкафам, должен быть ограничен, и предоставляться только тем работникам, которые осуществляют работу с материальными носителями ПДн.

8.15 Ответственным за предоставление доступа к документам в структурных подразделениях является руководитель подразделения, где осуществляется хранение ПДн.

8.16 Хранение копий материальных носителей ПДн должно осуществляться в личных запираемых металлических или деревянных шкафах работников или их непосредственных руководителей.

8.17 Хранение материальных носителей ПДн в открытом доступе в рабочих помещениях подразделений Компании и на столах работников допускается только в течение рабочего дня под персональной ответственностью работника.

9. Взаимодействие с государственными органами

9.1 Отношения в области организации и осуществления государственного контроля и надзора регулируются Федеральным законом от 26.12.2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля", который является обязательным для всех без исключения органов государственного контроля (надзора), и устанавливает порядок проведения проверок, а также административными регламентами надзорных органов, которые разрабатываются на основании и в соответствии с этим законом.

9.2 Компания обязана уведомить уполномоченный орган по защите прав субъектов ПДн <1>) о

своем намерении осуществлять обработку ПДн.

- <1>) Роскомнадзор

9.3 Компания вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн:

- обрабатываемых в соответствии с трудовым законодательством;

- полученных Компанией в связи с заключением договора, стороной которого является субъект ПДн, если ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются Оператором ПДн исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

- сделанных субъектом общедоступными ПДн;

- включающих в себя только фамилии, имена и отчества субъектов ПДн;

- необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится Компания;

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн.

9.4 Компания обязана сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения запроса.

9.5 В случае получения запроса или обращения уполномоченного органа по защите прав субъектов ПДн о недостоверности ПДн или неправомерных действиях с ними, необходимо исправить выявленные нарушения и уведомить указанный орган об устранении нарушений либо об уничтожении ПДн в случае невозможности устранения нарушений в срок, не превышающий десяти рабочих дней.

9.6 В установленных федеральным законодательством случаях Компания обязана предоставлять информацию, содержащую обрабатываемые ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции.

9.7 Запросы на предоставление доступа к обрабатываемым ПДн могут быть обжалованы в судебном порядке в соответствии с законодательством Российской Федерации.

9.8 Контроль и надзор за выполнением требований по обработке ПДн в ИСПДн, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности <2>), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации <3>), в пределах их компетенции и без права ознакомления с ПДн, обрабатываемыми в комплексе ИСПДн Компании.

- <2>) ФСБ России

- <3>) ФСТЭК России

- (наименования уполномоченных органов государственной власти даются на момент написания Положения)

9.9 Порядок взаимодействия с уполномоченным органом по защите прав субъектов ПДн описан в Положении о порядке взаимодействия с уполномоченным органом по защите прав субъектов ПДн.

10. Обязанности Администраторов ИСПДн, Ответственного за организацию обработки ПДн, Ответственного за обеспечение безопасности ПДн, Координатора по обращениям и запросам

Должностные инструкции Администраторов ИСПДн, Ответственного за организацию обработки ПДн, Ответственного за обеспечение безопасности ПДн и Координатора по обращениям и запросам должны быть расширены с учетом специфики обработки и защиты ПДн. Работники, назначаемые на данные роли, должны быть ознакомлены под подпись со своими должностными инструкциями.

В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица запрещается совмещать роли Администратора ИСПДн и Ответственного за обеспечение безопасности ПДн в лице одного работника.

10.1 Обязанности Администраторов ИСПДн

В обязанности Администраторов ИСПДн входит:

- управление учетными записями пользователей комплекса ИСПДн;

- предоставление и прекращение доступа пользователей к ПДн в ИСПДн в соответствии с утвержденным Перечнем должностей работников, допущенных к работе с ПДн или с утвержденными заявками на доступ к ПДн;

- установка и конфигурирование аппаратного и программного обеспечения комплекса ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн;

- поддержание штатной работы комплекса ИСПДн;

- мониторинг работы комплекса ИСПДн, включая межсетевые экраны и сетевого оборудования;

- предоставление периодической отчетности Ответственному за обеспечение безопасности ПДн о работе ИСПДн, состоянии защиты ИСПДн на основе результатов мониторинга, нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по эксплуатации ИСПДн и защите информации;

- контроль физической сохранности средств и оборудования ИСПДн <4>;

<4>) Ответственное лицо за контроль физической сохранности средств и оборудования ИСПДн в филиале может назначаться на сотрудника филиала приказом директора филиала

- контроль процессов резервного копирования;

- контроль работы пользователей в сетях общего пользования и (или) международного обмена (обхода правил межсетевого экранирования, составление рекомендаций к изменению правил межсетевого экранирования);

- уточнение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов ПДн;

- блокирование ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов ПДн;

- уничтожение ПДн в случаях, определенных настоящим Положением и Положением о порядке обработки обращений субъектов ПДн.

10.2 Обязанности Ответственного за организацию обработки ПДн

В обязанности Ответственного за организацию обработки ПДн входит:

- осуществление внутреннего контроля за соблюдением Компанией и ее работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

- доведение до сведения работников Компании положений законодательства Российской Федерации о ПДн, внутренних документов по вопросам обработки ПДн, требований к защите ПДн;

- осуществление контроля за приемом и обработкой обращений и запросов субъектов ПДн или их представителей;

- уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн, об изменениях в реквизитах Оператора ПДн;

- уведомление уполномоченного органа по защите прав субъектов ПДн по запросу этого органа с предоставлением необходимой информации в течение тридцати дней с даты получения такого запроса.

10.3 Обязанности Ответственного за обеспечение безопасности ПДн

10.3.1 В обязанности Ответственного за обеспечение безопасности ПДн входит:

- контроль выполнения мероприятий по защите ПДн;

- фиксация нарушений установленного порядка обработки ПДн, в т.ч. в сетях общего пользования и сети Интернет;

- предоставление сведений о ПДн в рамках проведения учета защищаемых носителей и проведения инвентаризации;

- установка, конфигурирование и администрирование аппаратных и программных средств защиты информации комплекса ИСПДн;

- восстановление работы средств защиты в случае нарушения их работоспособности;

- учет защищаемых носителей ПДн;

- учет технических средств защиты информации;

- периодические проверки журналов безопасности;

- анализ защищенности ИСПДн;

- организация процесса обучения работников по направлению обеспечения безопасности ПДн;

- мониторинг порядка обработки ПДн;

- участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

10.3.2 Ответственный за обеспечение безопасности ПДн обладает следующими полномочиями:

- проведение плановых и внеплановых контрольных мероприятий в целях контроля, изучения и оценки фактического состояния защищенности ПДн;

- может запрашивать необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности ПДн.

10.4 Обязанности Координатора по обращениям и запросам

10.4.1 В обязанности Координатора по обращениям и запросам входит:

- обработка обращений субъектов ПДн;

- ведение и хранение Журнала учета обращений субъектов ПДн;

- обработка запросов уполномоченного органа по защите прав субъектов ПДн;

- ведение и хранение Журнала учета запросов уполномоченного органа по защите прав субъектов ПДн;

- ведение и хранение Журнала учета проверок уполномоченным органом по защите прав субъектов ПДн.

10.4.2 Координатор по обращениям и запросам обладает следующими полномочиями:

- может запрашивать необходимую информацию у Администраторов ИСПДн;

- может давать Администраторам ИСПДн распоряжения касательно блокирования, уточнения и

уничтожения ПДн;

- может оценивать правомерность полученных запросов уполномоченного органа по защите прав субъектов ПДн;

- может созывать комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки ПДн.

11. Организация обучения персонала в области защиты ПДн

В целях совершенствования системы защиты ПДн и общего уровня осознания проблематики информационной безопасности работниками Компании должны проводятся мероприятия, направленные на обучение и повышение квалификации персонала в области информационной безопасности. Для организации обучения работников внутри Компании и за ее пределами должен ежегодно составляться План обучения на период. План обучения разрабатывается Управлением кадровой политики. Вновь поступившие на работу работники в обязательном порядке до начала исполнения своих трудовых обязанностей проходят инструктаж по основным мерам безопасности информации при работе с конфиденциальной информацией. Данный инструктаж проводит работник Управления кадровой политики.

12. Ответственность за нарушения при обработке ПДн

12.1 Статья 24 Федерального закона от 27.07.2006 г. N 152-ФЗ "О персональных данных" определяет ответственность за нарушение федерального закона, которая выражается в виде уголовной, административной, дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

12.2 Административная ответственность за нарушение федерального закона наступает за:

- неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации (ст. 5.39 Кодекса об административных правонарушениях (далее - КоАП РФ).

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (ПДн) (ст. 13.11 КоАП РФ);

- разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность) (ст. 13.14 КоАП РФ);

- непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде (ст. 19.7. КоАП РФ).

12.3 Ответственность за выполнение обязанностей по обеспечению безопасности ПДн,

возложенную на структурные подразделения Компании, обрабатывающие ПДн, несут руководители соответствующих подразделений и работники данных подразделений.

12.4 В случае нарушения порядка обработки и обеспечения безопасности ПДн работники Компании несут ответственность, предусмотренную ст. 90 ТК РФ, а также гражданско-правовую, административную, уголовную ответственность, предусмотренную действующим законодательством РФ.

13. Перечень терминов

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Администратор информационной системы персональных данных - работник Управления информационных технологий ЗАО "Сбербанк Лизинг", осуществляющий сопровождение программных и аппаратных компонентов информационной системы персональных данных в процессах внедрения, эксплуатации и вывода из эксплуатации и техническую поддержку пользователей системы.

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное требование для операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Координатор по обращениям и запросам - работник ЗАО "Сбербанк Лизинг", отвечающий за обработку обращений и запросов субъектов персональных данных и уполномоченного органа по защите прав субъектов персональных данных, сбор сведений и составление ответов на обращения и запросы в законодательно установленные сроки.

Материальный носитель персональных данных (далее - материальный носитель) - материальный объект, используемый для закрепления и хранения информации. В целях настоящего Положения под материальным носителем понимается бумажный документ (бумажный носитель), диск, дискета, флэш-карта (электронные носители).

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

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Обработка персональных данных - любое действие (операция) или совокупность действий

(операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор - 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. В настоящем Положении под Оператором понимается ЗАО "Сбербанк Лизинг".

Ответственный за обеспечение безопасности персональных данных - работник ЗАО "Сбербанк Лизинг", осуществляющий мероприятия по организации защиты персональных данных.

Ответственный за организацию обработки персональных данных - работник ЗАО "Сбербанк Лизинг", подотчетный Правлению ЗАО "Сбербанк Лизинг" и отвечающий за соблюдение Компанией и ее работниками законодательства Российской Федерации о персональных данных.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

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

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.

Цель обработки персональных данных - конкретный конечный результат действий, совершенных с персональными данными, вытекающий из требований законодательства и направленный, в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон.

Приложение А. Формы согласия субъектов

А.1 Форма согласия представителя компании ЗАО "Сбербанк Лизинг"

Форму согласия представителя компании ЗАО "Сбербанк Лизинг" смотри в файле Приложение А.1.doc.

А.2 Форма согласия физических лиц, не являющихся работниками ЗАО "Сбербанк

Лизинг" (в т.ч. кандидаты на трудоустройство)

Форму согласия физических лиц, не являющихся работниками ЗАО "Сбербанк Лизинг" (в т.ч. кандидаты на трудоустройство) смотри в файле Приложение А.2.doc.

Приложение Б. Положения типового договора о неразглашении ПДн

ТЕРМИНЫ

В настоящем Договоре используются термины, представленные ниже, если иное не следует из контекста.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных (обработка) - 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.

Субдоговор и заключение субдоговора - процесс, когда Стороны договариваются с третьей стороной о выполнении обязательств в соответствии с настоящим Договором, а субконтрактор означает сторону, с которой заключен субдоговор.

Технические и организационные меры обеспечения безопасности - меры, предпринимаемые для защиты персональных данных от случайного или незаконного уничтожения или случайной утраты, неавторизованной модификации, неправомерного раскрытия или доступа, а также от всех иных незаконных форм обработки.

РАЗДЕЛ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

1. Цели обработки ПДн

1.1 Обработчик по поручению Оператора совершает следующие действия с персональными данными:_____.

1.2 Целями обработки ПДн являются: _____.

2. Обязанности, связанные с безопасностью

2.1 Обработчик обязан совершать какие-либо свои действия в отношении персональных данных, которые он обрабатывает от имени Оператора, исключительно в соответствии с указаниями Оператора.

2.2 Обработчик обязан принимать надлежащие технические и организационные меры по обеспечению безопасности в соответствии с требованиями ст. 19 N 152-ФЗ "О персональных данных".

3. Конфиденциальность

3.1 Обработчик соглашается с тем, что он обязан обрабатывать персональные данные от имени Оператора, соблюдая конфиденциальность обработки. В частности, Обработчик соглашается с тем, что, если он не получил письменного согласия от Оператора, он не будет раскрывать персональные данные, переданные Обработчику Оператором/для Оператора/от имени Оператора третьим лицам.

3.2 Обработчик не должен использовать персональные данные, переданные ему Оператором, кроме как в соответствии с порядком оказания услуг, оказываемых им Оператору.

4. Заключение субдоговора

4.1 Обработчик не должен заключать субдоговор по исполнению своих обязательств, налагаемых настоящим Договором без предварительного письменного согласия Оператора.

4.2 В том случае, если Обработчик с согласия Оператора заключает субдоговор, он обязан заключать этот договор в письменной форме, а сам договор должен содержать все те обязательства в отношении безопасности обработки, которые накладываются на Обработчика в соответствии с настоящим Договором.

4.3 Если субконтрактор не в состоянии выполнять свои обязательства, вытекающие из субдоговора, Обработчик несет полную ответственность перед Оператором за выполнение обязательств, накладываемых на него настоящим Договором.

5. Обязанности Обработчика по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

В случае выявления Обработчиком неточных персональных данных или неправомерных действий с ними, Обработчик информирует о данном факте Оператора. По указанию Оператора Обработчик обязан осуществить блокирование неправомерно обрабатываемых персональных данных с момента выявления неточных персональных данных или неправомерных действий с ними или с момента получения указания от Оператора в срок, не превышающий семи рабочих дней, уточнить персональные данные, а в случае, если не удалось уточнить персональные данные, в срок, не превышающий десяти рабочих дней, уничтожить персональные данные.

6. Порядок действий с персональными данными после прекращения действия Договора

В течение семи дней со дня окончания действия настоящего Договора Обработчик обязан по указанию Оператора:

- вернуть все персональные данные, переданные для обработки Обработчику Оператором, или

- по указанию Оператора уничтожить все персональные данные, если это не запрещено законодательством, или

- выполнить все дополнительные соглашения между Сторонами в части возвращения или уничтожения данных.

Приложение В. Форма уведомления субъекта об обработке ПДн

Форму уведомления субъекта об обработке ПДн смотри в файле Приложение В.doc.

Приложение Г. Перечень должностей работников, допущенных к работе с ПДн

Перечень должностей работников, допущенных к работе с ПДн смотри в файле Приложение Г.doc.

Приложение Д. Форма акта об уничтожении ПДн

Форму акта об уничтожении ПДн смотри в файле Приложение Д.doc.

Приложение Е. Дополнение в должностные инструкции

В раздел должностных инструкций персонала ИСПДн, закрепляющий должностные обязанности, необходимо включить следующий пункт:

- При работе с информационными системами персональных данных следует руководствоваться требованиями к порядку обработки и обеспечения безопасности персональных данных, документированными в Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн ЗАО "Сбербанк Лизинг".

В раздел "Ответственность" должностных инструкций работников ЗАО "Сбербанк Лизинг", допущенных к обработке ПДн для выполнения своих должностных обязанностей, необходимо включить следующие пункты:

- Работник ЗАО "Сбербанк Лизинг" несет ответственность за обеспечение конфиденциальности ПДн, ставших ему известными в связи с выполнением должностных обязанностей.

- Работник ЗАО "Сбербанк Лизинг" несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн, документированных в "Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ЗАО "Сбербанк Лизинг".

- В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения ЗАО "Сбербанк Лизинг" или ее клиентам материального или иного ущерба, виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственности.