УТВЕРЖДЕНА
приказом АО ВТБ Лизинг
от 19 июня 2017 г. № 413-П

ПОЛИТИКА
обработки персональных данных
в АО ВТБ Лизинг

г. Москва

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Настоящая Политика обработки персональных данных в АО ВТБ Лизинг (далее – Политика) разработана в соответствии со следующими документами:

1) Конституцией Российской Федерации;

2) Гражданским кодексом Российской Федерации;

3) Трудовым кодексом Российской Федерации;

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

5) Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

6) Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;

7) постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

8) постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

9) приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

10) приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

11) иными нормативными правовыми актами Российской Федерации в области обработки и обеспечения безопасности персональных данных.

1.2. Требования Политики распространяются на все процессы обработки персональных данных в АО ВТБ Лизинг (далее – Общество), осуществляемые как с использованием средств автоматизации, так и без использования таких средств, и обязательны для исполнения всеми работниками Общества.

1.3. Положения Политики служат основой для разработки организационно-распорядительных документов Общества, регламентирующих отдельные процессы обработки персональных данных, а также содержат нормы и правила обеспечения безопасности персональных данных при их обработке в Обществе.

1.4. В Политике используются следующие основные понятия:

1) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) 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;

3) 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;

4) автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) 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;

9) обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Обработка персональных данных

2.1. Общество в соответствии с Федеральным законом «О персональных данных» признается оператором, осуществляющим обработку персональных данных.

2.2. Обработка персональных данных в Обществе осуществляется на основе следующих принципов:

1) обработка персональных данных должна осуществляться на законной и справедливой основе;

2) обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

3) не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

4) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

5) обработке подлежат только персональные данные, которые отвечают целям их обработки;

6) содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;

7) обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

8) 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;

9) должны быть приняты необходимые меры либо обеспечено их принятие по удалению или уточнению неполных или неточных данных;

10) хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

11) обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

2.3. Обработка персональных данных в Обществе допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) 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;

3) обработка персональных данных необходима для осуществления прав и законных интересов Общества или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Общество функций, полномочий и обязанностей;

5) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

6) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

7) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

8) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

9) обработка осуществляется в иных, предусмотренных Федеральным законом «О персональных данных» случаях.

2.4. Общество обеспечивает конфиденциальность обрабатываемых персональных данных, не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.5. 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 (поручения).

2.6. Лицо, осуществляющее обработку персональных данных по поручению Общества, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

2.7. Лицо, получившее доступ к персональным данным по поручению Общества, обязано не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.8. К обрабатываемым персональным данным допускаются работники Общества, которые в соответствии с их должностными обязанностями наделены такими полномочиями. Доступ предоставляется на основании приказа Общества, в котором указывается перечень наименований должностей, замещение которых представляет право доступа к персональным данным, цели обработки

персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.9. Трудовые договоры с работниками Общества, допущенными к обработке персональных данных, должны содержать обязательства о необходимости соблюдения конфиденциальности обрабатываемых персональных данных и исполнении требований организационно-распорядительных документов Общества в области обработки и обеспечения безопасности персональных данных.

2.10. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Обществе не допускается, за исключение случаев, предусмотренных Федеральным законом «О персональных данных».

2.11. Обработка персональных данных о судимости может осуществляться Обществом только в случаях и порядке, которые определяются в соответствии с федеральными законами.

2.12. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), и которые используются Обществом для установления личности субъекта персональных данных, могут обрабатываться Обществом только при наличии согласия в письменной форме субъекта персональных данных.

2.13. Трансграничная передача персональных данных на территории иностранных государств может осуществляться Обществом при наличии согласия субъекта персональных данных в письменной форме на трансграничную передачу его персональных данных или в иных случаях, предусмотренных Федеральным законом «О персональных данных».

До начала осуществления трансграничной передачи персональных данных Общество обязано убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

2.14. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Общество осуществляет запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

2.15. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято Обществом на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

2.16. В Обществе назначается лицо, ответственное за организацию обработки персональных данных, которое получает указания непосредственно от генерального директора Общества и подотчетно ему.

2.17. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) организовывать определение политики Общества в отношении обработки и защиты персональных данных.

2) организовывать разработку мер, направленных на предотвращение, выявление и устранение нарушений законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных.

3) осуществлять внутренний контроль за соблюдением Обществом и работниками Общества законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

4) доводить до сведения работников Общества положений законодательства Российской Федерации о персональных данных, локальных актов Общества по вопросам обработки персональных данных, требований к защите персональных данных;

5) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Обеспечение безопасности персональных данных

3.1. В Обществе для обеспечения выполнения обязанностей, предусмотренных законодательством Российской Федерации, при обработке персональных данных должны приниматься необходимые правовые, организационные и технические меры или обеспечиваться их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Обеспечение безопасности персональных данных в Общества достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

4) учетом машинных носителей персональных данных;

5) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

6) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

8) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

9) осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям организационно-распорядительных документов Общества и законодательства Российской Федерации в области персональных данных;

10) оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения требований законодательства Российской Федерации в области обработки персональных данных, соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации;

11) ознакомлением работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, организационно-распорядительными документами Общества, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

12) созданием структурного подразделения, ответственного за обеспечение безопасности персональных данных в Обществе, либо возложением на одно из структурных подразделений Общества функций по обеспечению такой безопасности.

3.3. Структурное подразделение, ответственное за обеспечение безопасности персональных данных в Обществе, в частности, осуществляет следующие функции:

1) организовывает и проводит работы в Обществе по созданию системы защиты персональных данных, обрабатываемых в информационных системах персональных данных, в соответствии с законодательством Российской Федерации;

2) организовывает и проводит оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

3) разрабатывает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также требования к регистрации и учету всех действий, совершаемых с персональными данными в информационной системе персональных данных;

4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям организационно-распорядительных документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных;

5) осуществляет мониторинг законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных;

6) информирует лицо, ответственное за организацию обработки персональных данных о случаях нарушения требований безопасности персональных данных (об инцидентах информационной безопасности при обработке персональных данных, в том числе о несанкционированном или случайном доступе к таким данным);

7) участвует в расследовании случаев нарушения требований безопасности персональных данных;

8) вносит лицу, ответственному за организацию обработки персональных данных в Обществе, предложения, направленные на улучшение организации обработки и обеспечения безопасности персональных данных в Обществе, в том числе с целью исключения нарушений при обработке персональных данных;

9) разрабатывает мероприятия по совершенствованию безопасности персональных данных;

10) участвует в обработке обращений и запросов субъектов персональных данных или их представителей;

11) участвует в разработке организационно-распорядительных документов Общества, регламентирующих отдельные процессы обработки персональных данных;

12) разрабатывает нормы и правила обеспечения безопасности персональных данных при их обработке в Обществе;

13) осуществляет взаимодействие с государственными органами по вопросам обработки и обеспечения безопасности персональных данных.

3.4. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, а также контроль и (или) аудит соответствия обработки персональных данных требованиям организационно-распорядительных документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных проводится Обществом самостоятельно и (или) с привлечением на договорной основе третьих лиц, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанные мероприятия проводятся не реже одного раза в три года.

4. Права субъектов персональных данных

4.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку Обществом свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Общество, в случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, проверяет полномочия данного представителя на дачу согласия от имени субъекта персональных данных.

4.2. 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 законодательством Российской Федерации меры по защите своих прав.

4.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных Общество вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, предусмотренных законодательством Российской Федерации.

4.4. Субъект персональных данных имеет право на получение следующей информации, касающейся обработки его персональных данных в Обществе, за исключением случаев ограничения указанного права, предусмотренных Федеральным законом «О персональных данных»:

1) подтверждение факта обработки персональных данных Обществом;

2) правовые основания и цели обработки персональных данных Обществом;

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 Обществом 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 Федеральным законом «О персональных данных»;

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

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

10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

4.5. Указанные сведения, предоставляются субъекту персональных данных или его представителю Обществом при обращении либо при получении запроса субъекта персональных данных или его представителя.

4.6. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Обществом, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4.7. Если субъект персональных данных считает, что Общество осуществляет обработку его персональных данных с нарушением требований законодательства

Российской Федерации 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.

5. Ответственность

5.1. Работники Общества, допущенные к обработке персональных данных, обязаны:

1) соблюдать требования настоящей Политики и других организационно-распорядительных документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных;

2) выполнять требования по обеспечению безопасности обрабатываемых персональных данных;

3) осуществлять немедленное информирование непосредственного руководителя и руководителя подразделения, ответственного за обеспечение безопасности персональных данных в Обществе, о случаях нарушения требований безопасности персональных данных (об инцидентах информационной безопасности при обработке персональных данных, в том числе о несанкционированном или случайном доступе к таким данным);

4) обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;

5) не раскрывать третьим лицам и не распространять персональные данные, обрабатываемые в Обществе.

5.2. Руководители структурных подразделений Общества обязаны организовывать работу подчиненных работников с учетом требований настоящей Политики и других организационно-распорядительных документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных.

5.3. Работники Общества, нарушающие требования настоящей Политики и других организационно-распорядительных документов Общества и законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую и (или) уголовную ответственность в соответствии с законодательством Российской Федерации.

6. Порядок пересмотра

Пересмотр и корректировка Политики производится по необходимости или в случае изменения законодательства Российской Федерации в области обработки персональных данных.