

УТВЕРЖДЕНО

Протоколом Правления

«Мерседес-Бенц Банк Рус» ООО

№ 4 от «31» января 2017 года

Председатель Правления


_____ **Л.А. Зотова**

ПОЛИТИКА

**в области обработки и защиты персональных данных
в «Мерседес-Бенц Банк Рус» ООО**

2017 год

Оглавление

1. Общие положения.....	3
2. Цели обработки ПДн	4
3. Правила обработки ПДн	4
4. Установление правил и порядка обработки ПДн	5
5. Требования к конфиденциальности и обеспечению безопасности ПДн.....	6
6. Контроль	7
7. Заключительные положения.....	7

1. Общие положения

1.1. Во исполнение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Трудового кодекса РФ, требований стандарта Банка России СТО-БР-ИББС-1.0, указаний и положений Банка России, приказов ФСТЭК и ФСБ, других законодательных актов Российской Федерации в области обработки и защиты персональных данных, а также внутренних документов и Общекорпоративных правил защиты данных компании «Даймлер АГ» (далее также «Правила защиты данных») «Мерседес-Бенц Банк Рус» ООО (далее – «Банк») обеспечивает легитимность обработки и безопасность персональных данных (далее – «ПДн») в своей деятельности.

1.2. Единственным участником Банка является компания Даймлер АГ (Федеративная Республика Германия). Федеративная Республика Германия является страной-участницей Конвенции о защите физических лиц при автоматизированной обработке персональных данных ETS N 108 (Страсбург, 28 января 1981 г.).

1.3. Банк включен в Реестр операторов, осуществляющих обработку персональных данных (далее – «Реестр»). Указанный Реестр опубликован на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в сети «Интернет» по адресу: <http://rkn.gov.ru/personal-data/register/>.

1.4. Принципами обработки ПДн в Банке являются:

- обработка ПДн осуществляется на законной и справедливой основе;
- обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка ПДн, несовместимая с целями сбора ПДн;
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только ПДн, которые отвечают целям их обработки;
- содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Не допускается избыточность обрабатываемых ПДн по отношению к заявленным целям их обработки;
- при обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн, принимаются необходимые меры по удалению или уточнению неполных или неточных ПДн;
- хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем того требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, согласием на обработку ПДн, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;
- обработка ПДн не используется в целях причинения имущественного и/или морального вреда субъектам ПДн, затруднения реализации их прав и свобод;
- иные принципы, определенные в Правилах защиты данных.

2. Цели обработки ПДн

2.1. В соответствии с принципами обработки ПДн в Банке определены состав обрабатываемых ПДн и цели их обработки.

2.2. Состав и цели обработки ПДн соответствуют требованиям действующего законодательства РФ в области обработки и защиты ПДн.

2.3. Банк следует Общекорпоративным правилам защиты данных компании «Даймлер АГ» и при обработке ПДн преследует исключительно те цели, которые были определены перед началом сбора данных. Последующие изменения целей возможны только в ограниченной мере и подлежат обоснованию и информированию об этом субъекта ПДн.

3. Правила обработки ПДн

3.1. Обработка ПДн осуществляется Банком на законной основе. В случаях, предусмотренных действующим законодательством РФ, Банк осуществляет получение согласия (письменного согласия) субъекта на обработку его ПДн по установленной действующим законодательством Российской Федерации форме. Если Банк получает ПДн от третьего лица, то он в обязательном порядке требует подтверждения от этого лица, что оно имеет все необходимые основания для передачи ПДн в Банк.

3.2. Банк в ходе своей деятельности вправе поручать обработку ПДн третьему лицу, если иное не предусмотрено действующим законодательством РФ. При этом обязательным условием поручения обработки ПДн (в виде договора или доверенности) другому лицу является обязанность по соблюдению конфиденциальности и обеспечению безопасности ПДн при их обработке, а также обязательство третьего лица использовать данные исключительно в заранее определенных целях и объемах.

3.3. При поручении обработки или передаче ПДн другому лицу возможны случаи осуществления трансграничной передачи. В этом случае Банк следует требованиям законодательства РФ и осуществляет передачу только на территорию иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн. В противном случае, Банк следует требованиям части 4 статьи 12 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

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

3.5. В Банке НЕ обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни. В Банке допускается обработка следующих специальных категорий ПДн в отношении работников, их родственников и кандидатов: данные об инвалидности, данные о состоянии на учете в психоневрологическом и наркологическом диспансерах.

3.6. Обработка биометрических ПДн (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются в Банке для установления личности субъекта ПДн) в Банке осуществляется только для целей идентификации субъектов ПДн (клиентов) при их посе-

щении точек продаж, офисов и т.д. Банка. При этом для целей идентификации используется фотография в паспорте субъекта ПДн, который предоставляет сам субъект ПДн. В качестве согласия на обработку ПДн выступает конклюдентное согласие субъекта ПДн на обработку его ПДн при передаче паспорта в руки представителя Банка. Банк не использует собственные носители ПДн и ИСПДн, содержащие биометрические ПДн, для идентификации субъекта ПДн (клиента).

3.7. Банк НЕ размещает ПДн субъекта ПДн в общедоступных источниках без его письменного согласия.

3.8. Банк организывает процессы взаимодействия с субъектами ПДн таким образом, чтобы субъект мог обратиться в Банк по всем предусмотренным в законодательстве РФ вопросам, связанным с обработкой его ПДн (информация об обрабатываемых ПДн, о третьих лицах, запросы на уточнение, прекращение обработки, блокировку и уничтожение).

3.9. Предоставление ПДн органам государственной власти и местного самоуправления, в суды, правоохранительные органы, а также иным надзорным органам осуществляется Банком в случаях и в порядке, предусмотренных законодательством РФ.

4. Установление правил и порядка обработки ПДн

4.1. В соответствии с требованиями, указанными в п.1.1 настоящего документа, в Банке во внутренних документах, обязательных для исполнения всеми работниками Банка, а также партнерами, контрагентами и прочими третьими лицами в части, их касающейся, определяются:

- процедуры предоставления доступа к ПДн;
- процедуры внесения изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн;
- процедуры уничтожения, обезличивания либо блокирования ПДн в случае необходимости выполнения таких процедур;
- процедуры обработки обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (его законными представителями) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки;
- процедуры обработки запроса уполномоченного органа по защите прав субъектов ПДн;
- процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу обработки его ПДн третьим лицам;
- процедуры передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками Банка, имеющими доступ к ПДн;
- процедуры передачи ПДн третьим лицам;

- процедуры работы с материальными носителями ПДн;
- процедуры, необходимые для осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- необходимость применения типовых форм документов для осуществления обработки ПДн и процедуры работы с ними. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая Банком с целью сбора ПДн.

5. Требования к конфиденциальности и обеспечению безопасности ПДн

5.1. С целью обеспечения безопасности ПДн при их обработке в Банке реализуются требования действующего законодательства РФ в области обработки и обеспечения безопасности ПДн, требования стандарта Банка России СТО-БР-ИББС-1.0 и требования Общекорпоративных правил защиты данных компании «Даймлер АГ».

5.2. Для этих целей в Банке введена, функционирует и проходит периодический пересмотр (контроль) система защиты ПДн.

5.3. Банк применяет необходимые и достаточные организационные и технические меры, включающие в себя, в том числе:

- разработку внутренних документов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- защиту ПДн от несанкционированного доступа, неправомерной обработки или передачи, а также от утери, искажения или уничтожения (вне зависимости от того, автоматизированная или неавтоматизированная обработка ПДн осуществляется);
- определение и внедрение перед введением новых процессов обработки ПДн и новых информационных систем персональных данных (далее – «ИСПДн»), технических и организационных мер, обеспечивающих защиту ПДн, ориентированных на современный уровень техники и необходимую степень защиты данных;
- определение угроз безопасности ПДн при их обработке в ИСПДн;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- установление правил доступа к ПДн, обрабатываемых в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль и оценку эффективности применяемых мер (в том числе с привлечением аудиторских проверок);
- обнаружение фактов несанкционированного доступа к ПДн (и других инцидентов с ПДн) и принятие мер;
- восстановление ПДн.

5.4. В части обеспечения конфиденциальности обработки Банк предпринимает меры, направленные на предотвращение несанкционированного сбора, обработки или использования ПДн, в том числе:

- предоставление доступа к ПДн только в случаях и в порядке, предусмотренном законодательством РФ;
- ознакомление работников Банка, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Банка в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

5.5. В Банке назначены лица, ответственные за организацию обработки и обеспечения безопасности ПДн.

5.6. Руководство Банка заинтересовано в обеспечении безопасности ПДн, обрабатываемых в рамках выполнения основной деятельности Банка, как с точки зрения требований действующего законодательства РФ и корпоративных правил, так и с точки зрения минимизации рисков.

6. Контроль

6.1. Контроль за выполнением настоящей Политики осуществляется в рамках общей системы внутреннего контроля Банка.

7. Заключительные положения

7.1. Настоящая Политика вступает в силу с момента его утверждения и действует до момента внесения изменений и/или принятия нового документа в соответствии с внутренним порядком Банка.

7.2. В случае если какое-либо из положений настоящей Политики является или становится незаконным, недействительным, это не затрагивает действительность остальных положений настоящей Политики.

7.3. В случае изменения нормативно-правовых актов, использованных в настоящей Политике, настоящая Политика продолжает свое действие в части, не противоречащей действующему законодательству. В остальной части Банк руководствуется нормами действующего законодательства.