УТВЕРЖДЕНО

Приказом
ООО «Мерседес-Бенц Файненшл Сервисес Рус»
№ 20201222-01 от «22» декабря 2020 года
Представитель по доверенности № 41/20/DAG
Финансовый директор
ООО «Мерседес-Бенц Капитал Рус»

 **С. Ландманн**

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
в ООО «Мерседес-Бенц Файненшл Сервисес Рус»

г. Москва, 2020 год

Оглавление

1. Область применения

1.1 Настоящее Положение об обработке и защите персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус» (далее – «Положение») определяет правила обработки ПДн и устанавливает требования по организации и непосредственному функционированию процессов обработки ПДн в ООО «Мерседес-Бенц Файненшл Сервисес Рус» (далее – «Компания») в соответствии с требованиями нормативных правовых актов Российской Федерации в области обработки и защиты ПДн.

1.2 В концерне «Даймлер» действует глобально для всех предприятий корпоративная политика «Общекорпоративные правила защиты данных» (далее - «Правила защиты данных», актуальная редакция размещена на сайте «Даймлер АГ»: www.daimler.com). В соответствии с разделом III «Действие законодательства» Правил защиты данных настоящее Положение расширяет и конкретизирует их требования для применения их на территории Российской Федерации в рамках процессов, в которых осуществляется обработка ПДн, при этом приоритет остается за законодательством РФ.

1.3 Настоящее Положение является нормативным документом Компании и обязательно для исполнения всеми подразделениями и отдельными работниками Компании, связанными с обработкой или защитой ПДн, а также работниками АО «Мерседес-Бенц РУС», ООО «Мерседес-Бенц Капитал Рус» и «Мерседес-Бенц Банк Рус» ООО, привлечённых Компанией для и/или оказывающих Компании услуги в области ключевых функций, в рамках которых осуществляется обработка ПДн[1].

1.4 Требования настоящего Положения распространяются на все процессы обработки ПДн в Компании, независимо от формы представления ПДн.

2. Термины, определения и сокращения

БД — база данных.
ИБ — информационная безопасность.
ИСПДн — информационная система персональных данных.
ИТ — информационные технологии.
Компания — ООО «Мерседес-Бенц Файненшл Сервисес Рус».
ПДн — персональные данные.
ПО — программное обеспечение.
РФ — Российская Федерация.
СВТ — средство вычислительной техники.
СЗИ — средство защиты информации.
СЗПДн — система защиты персональных данных.
СКУД — система контроля управления доступом.
УБПДн — угроза безопасности персональных данных.
ФСБ России — Федеральная служба безопасности России.
ФСТЭК России — Федеральная служба технического и экспортного контроля России.

[1] Учет работников указанных юридических лиц, допущенных к обработке данных, осуществляется указанными юридическими лицами самостоятельно.

Безопасность персональных данных — состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.

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

Внутренняя типовая форма — документ, состав данных и порядок обработки которого не установлен законодательством РФ, и использующийся во внутренних бизнес-процессах Компании.

Вредоносное программное обеспечение — программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации — возможность получения и использования информации.

Доступность персональных данных — возможность беспрепятственного получения санкционированного доступа к персональным данным лицами, имеющими право на такой доступ.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Инцидент безопасности персональных данных — событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию УБПДн, результатом которой являются:

- нарушение или возможное нарушение работы СЗИ в составе СЗПДн Компании;
- нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Компании в области обработки и защиты ПДн, нарушение или возможное нарушение в выполнении процессов обеспечения безопасности ПДн Компании;
- нарушение или возможное нарушение в выполнении процессов обработки ПДн Компании;
- нанесение или возможное нанесение ущерба Компании и (или) его клиентам.

Конфиденциальная информация — информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать их распространения при отсутствии согласия субъекта ПДн или иного законного основания.

Криптографическая защита — защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

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), блокирование, удаление, уничтожение персональных данных.

Объем обрабатываемых персональных данных — количество субъектов ПДн, чьи данные обрабатываются в ООО «Мерседес-Бенц Файненшл Сервисес Рус», информационной системе или базе 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.

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

Пользователь персональных данных — лицо, участвующее в процессах(е) обработки ПДн или использующее результаты такой обработки.

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

Процесс обработки персональных данных — бизнес-процесс Компании, в рамках которого осуществляется обработка персональных данных.

Средство вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных. Субъектами ПДн являются: клиенты, представители клиента, бенефициары, выгодоприобретатели, поручители, работники Компании и кандидаты на устройство, работники контрагентов Компании и прочие физические лица, чьи ПДн обрабатываются в Компании.

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

Угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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.

Целостность персональных данных — способность средства вычислительной техники или информационной системы обеспечивать неизменность персональных данных в условиях случайного и/или преднамеренного искажения (разрушения).

3. Общие положения

3.1. При работе с ПДн во всех случаях, не урегулированных нормативными документами Компании, необходимо руководствоваться требованиями документов в следующем приоритете:

- Законодательством Российской Федерации в области обработки и защиты ПДн (в том числе подзаконными актами);
- Настоящим Положением и другими внутренними нормативными документами Компании в области обработки и защиты ПДн;
- Правилами защиты данных.

3.2. Настоящее Положение доводится до всех работников Компании, АО «Мерседес-Бенц РУС», ООО «Мерседес-Бенц Капитал Рус», «Мерседес-Бенц Банк Рус» ООО, непосредственно привлечённых Компанией для целей оказания услуг и/или оказывающих Компании услуги в области ключевых функций[2], в рамках которых осуществляется обработка ПДн, под роспись. Подпись работника на листе ознакомления означает его ознакомление со всеми требованиями, указанными в настоящем Положении.

4. Обрабатываемые ПДн

4.1. В Компании разработан и утвержден «Перечень обрабатываемых персональных данных, информационных систем персональных данных и лиц, допущенных к обработке персональных данных» (далее – «Перечень ПДн»). В Перечне ПДн закреплены категории субъектов ПДн, группы и детальный состав ПДн, цели и правовые основания обработки для каждой из групп и категорий субъектов ПДн. При разработке Перечня ПДн учитывается, что обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям обработки.

4.2. В случае если правовым основанием для обработки ПДн предусматривается необходимость получения согласия субъекта на обработку его ПДн, то данное согласие получается Компанией.

[2] Доведение настоящего Положения до сведения работников указанных юридических осуществляется этими юридическими лицами самостоятельно.

Детальные процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу его ПДн третьим лицам определены в настоящем Положении и Регламенте взаимодействия ООО «Мерседес-Бенц Файненшл Сервисес Рус» с субъектами персональных данных.

4.3. Обработка ПДн, которая не соответствует целям или составу, определенным в Перечне ПДн, в Компании запрещена. Проверка данного соответствия осуществляется в рамках пересмотра Перечня ПДн , а также при изменениях процессов обработки ПДн и/или ИСПДн.

4.4. Компания относит ПДн к разряду общедоступных в случаях, когда ПДн сделаны общедоступными субъектом персональных данных или, получены из общедоступного источника. В Компании происходит обработка общедоступных ПДн только в отношении работников Компании и кандидатов на прием на работу, а также клиентов.

Порядок отнесения тех или иных ПДн к разряду общедоступных определяется в Частном положении по обработке и защите персональных данных работников, их родственников и кандидатов ООО «Мерседес-Бенц Файненшл Сервисес Рус». Требования по обеспечению безопасности ПДн не распространяются на общедоступные ПДн.

Компания самостоятельно не формирует общедоступные источники ПДн клиентов, а использует уже существующие и поддерживаемые другими организациями (например, данные с сайтов судов, реестр банкротов и т.д.) в связи с чем согласие клиентов на признание их ПДн общедоступными не требуется.

Требования по обеспечению безопасности ПДн не распространяются на общедоступные ПДн. Также на общедоступные ПДн не распространяются требования настоящего Положения в части установления целей их обработки (ограничение их обработки достижением цели обработки), сроков хранения (и их соблюдения), учета количества субъектов, получения согласия на обработку, прекращение обработки и уничтожение (блокирование), требования к материальным носителям с общедоступными ПДн и т.д.

4.5. В Компании не допускается обработка специальных категорий ПДн, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

4.6. Обработка биометрических ПДн (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются в Компании для установления личности субъекта ПДн) в Компании осуществляется только для целей идентификации субъектов ПДн при их посещении точек продаж (если применимо), офисов и т.д. Компании. 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 Компании. Компания не использует собственные носители ПДн и ИСПДн, содержащие биометрические ПДн, для идентификации субъекта ПДн (клиента).

4.7. К документам, содержащим ПДн субъектов ПДн (за исключением работников и кандидатов Компании), относятся:

- досье юридических лиц и индивидуальных предпринимателей;
- договоры, а также другие документы, предоставленные субъектом ПДн в целях оказания Компанией услуг и/или заключения и исполнения договора;
- копии удостоверяющих личность документов, а также иных документов (в том числе различных заявлений, анкет), предоставляемых субъектами ПДн в рамках ведения Компанией хозяйственной деятельности;

- различные внутренние распоряжения и служебные записки;
- иные документы и файлы, формируемые в рамках ведения Компанией хозяйственной деятельности.

5. ИСПДн

5.1. Комплексы БД, СВТ, технические средства обработки объединяются в ИСПДн Компании. При этом в ИСПДн Компании входит несколько компонентов.

5.2. К ИСПДн Компании относятся следующие информационные системы, базы данных и файловые ресурсы:

- в них осуществляется обработка ПДн, оператором или обработчиком (на основании поручения) которых является Компания;
- ИС осуществляют обработку ПДн с использованием программного обеспечения и технических средств, принадлежащих Компании или арендованных Компанией.

5.3. Запрещается объединение баз ПДн, обработка которых осуществляется в целях, несовместимых между собой. Мероприятия по определению возможности объединения баз ПДн осуществляются на этапе оценки возможности создания (модернизации) ИСПДн согласно Регламенту обеспечения безопасности персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус». При формировании отдельных файлов (отчетов, реестров и т.д.) работниками Компании, если они не будут отнесены к ИСПДн, последние должны самостоятельно на основании целей, указанных в Перечне ПДн, определять возможность объединения баз ПДн.

5.4. Для ИСПДн «МБФСР» ООО «Мерседес-Бенц Файненшл Сервисес Рус» разработаны следующие документы:

- Модель угроз безопасности ПДн при их обработке в ИСПДн «МБФСР» ООО «Мерседес-Бенц Файненшл Сервисес Рус», включающая в себя модель нарушителя в ИСПДн;
- Акт определения защищенности ПДн при их обработке в ИСПДн «МБФСР» ООО «Мерседес-Бенц Файненшл Сервисес Рус».

5.5. При моделировании угроз безопасности ПДн при их обработке в ИСПДн проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения законодательства и определение перечня актуальных угроз безопасности ПДн в конкретных условиях функционирования.

5.6. Порядок проведения необходимых в части соблюдения требований законодательства в области обработки и защиты ПДн мероприятий в рамках жизненного цикла ИСПДн Компании описан в Регламенте обеспечения безопасности персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус».

6. СЗПДн

6.1. СЗПДн Компании основана на следующих принципах:

- вовлеченности руководства Компании (Генеральный директор) – деятельность по обеспечению безопасности ПДн инициирована и контролируется руководством Компании (Генеральным директором);
- соответствия мер и средств защиты актуальным УБПДн;

- соответствия мер и средств защиты требованиям нормативных документов РФ в области обработки и обеспечения безопасности ПДн;
- комплексности – с целью обеспечения безопасности ПДн в Компании используется совокупность организационных и технических мер;
- патентной чистоты – средства защиты информации, входящие в состав СЗПДн Компании, отвечают требованиям по обеспечению патентной чистоты согласно нормативным документам РФ. Используемое общесистемное, специальное и прикладное ПО имеет соответствующие лицензии производителей;
- удобства персонала – при построении и модернизации СЗПДн в Компании учитываются и, по возможности, сводятся к минимуму возможные затруднения персонала в работе со средствами защиты и при выполнении основных процедур обеспечения безопасности ПДн;
- законности организационных и технических мер по обеспечению безопасности ПДн;
- непрерывности повышения уровня знаний работников Компании в сфере обеспечения безопасности ПДн;
- стремления к постоянному совершенствованию СЗПДн.

6.2. Основы методов и способов обеспечения безопасности ПДн заложены в настоящем Положении, а порядок их реализации описан в документах:

- Регламент обеспечения безопасности персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус»;
- Инструкция работника ООО «Мерседес-Бенц Файненшл Сервисес Рус» по правилам обработки и защиты персональных данных.

6.3. Компании, оказывающие услуги Компании в области защиты ПДн, должны иметь лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации. Компании, оказывающие услуги Компании в области шифрования информации (распространение, использование СКЗИ), должны иметь соответствующие лицензии ФСБ России.

7. Правила обработки ПДн

7.1. Опубликование документа, определяющего политику Компании в области обработки и безопасности персональных данных

7.1.1. В целях обеспечения неограниченного доступа к документу, определяющему политику Компании в отношении обработки ПДн, и к сведениям о реализуемых требованиях к защите ПДн, в Компании утвержден и введен в действие документ «Политика в области обработки и защиты персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус»» (далее – «Политика»).

7.1.2. Политика разрабатывается на основе сведений, указанных в настоящем Положении, и в частности содержит:

- информацию о включении Компании в реестр операторов, осуществляющих обработку персональных данных;
- принципы обработки ПДн;
- цели обработки ПДн;
- правила обработки ПДн;

- информацию об установленных правилах и порядках обработки ПДн;
- требования к конфиденциальности и обеспечению безопасности ПДн.

7.1.3. Политика размещена на официальном веб-сайте Компании и подлежит обязательному пересмотру при внесении изменений в настоящее Положение, а также при изменении законодательства (при необходимости).

7.1.4. При сборе ПДн с использованием сети Интернет на соответствующем ресурсе (веб-сайте) размещается ссылка на раздел официального сайта Компании, где размещена Политика. Размещение ссылки осуществляется работниками Компании или подрядных организаций, которые разрабатывают соответствующее техническое решение по сбору ПДн. Размещение должен организовать работник Компании, в зоне ответственности которого находится данный процесс сбора ПДн, включив соответствующее требование в техническое задание, в том числе подрядной организации.

7.1.5. Если субъект ПДн по какой-либо причине не может получить доступ к Политике либо указанных в ней сведений недостаточно для удовлетворения просьбы субъекта ПДн, то предоставление указанных сведений осуществляется в порядке, описанном в Регламенте взаимодействия ООО «Мерседес-Бенц Файненшл Сервисес Рус» с субъектами персональных данных.

7.2. Принципы обработки ПДн

7.2.1. Обработка ПДн в Компании осуществляется в соответствии со следующими принципами:

- 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 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.

7.2.2. В Компании проводится анализ соответствия процессов обработки ПДн заявленным принципам. Данный анализ проводится в случае:

- создания новых или внесения изменений в существующие или ликвидации процессов обработки ПДн;
- создания новых или внесения изменений в существующие или снятие с эксплуатации ИСПДн;
- изменения нормативной базы, затрагивающей принципы и/или процессы обработки ПДн в Компании;
- проведения внутренних контрольных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

7.3. Сбор ПДн

7.3.1. Компания получает ПДн из следующих источников:

- непосредственно от субъекта ПДн /представителя субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований законодательства РФ;
- от другого субъекта ПДн, в целях реализации его законных прав;
- из общедоступного источника.

7.3.2. Все ПДн субъекта ПДн необходимо получать от него лично с его письменного согласия на обработку ПДн, за исключением случаев, предусмотренных в настоящем Положении и действующем законодательстве.

7.3.3. Если предоставление ПДн является обязательным в соответствии с законодательством РФ и субъект ПДн отказывается представить его ПДн, работник Компании, осуществляющий сбор ПДн, должен разъяснить субъекту ПДн юридические последствия такого отказа. Юридические последствия отказа определяются исходя из целей, для которых субъект отказывается предоставлять свои ПДн.

7.3.4. Если правовым основанием для сбора ПДн является письменное согласие субъекта ПДн, то используются следующие места хранения такого согласия в бумажном виде:

- досье клиента (юридического лица или индивидуального предпринимателя), если иное не принято в Компании;
- личный файл работника;
- иные места, предусмотренные нормативными документами процесса, в рамках которого осуществляется сбор согласий на обработку ПДн.

7.3.5. Если при сборе ПДн не используется письменное согласие, то субъекту ПДн представляется следующая информация по его запросу:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- применяемые в Компании способы обработки ПДн;
- наименование и фактический адрес Компании, сведения о лицах (за исключением работников Компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Компанией или на основании федерального закона;

- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от № 152-ФЗ от 27.07.2006 «О персональных данных»;
- информацию об осуществляемой или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные к представлению Федеральным законом от № 152-ФЗ от 27.07.2006 «О персональных данных», внутренними документами Компании (если применимо).

7.3.6. Если ПДн субъекта ПДн возможно получить только у третьей стороны (за исключением законного представителя), то субъект ПДн должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие на получение ПДн у третьей стороны. Работник Компании, осуществляющий получение ПДн субъекта ПДн, должен осуществить информирование субъекта ПДн согласно п. 7.3.6 настоящего Положения и получить согласие Субъекта ПДн на получение ПДн у третьей стороны (если оно не было получено ранее).

7.4. Хранение и учёт ПДн

7.4.1. ПДн субъектов ПДн обрабатываются и хранятся в ИСПДн, а также на материальных носителях ПДн (бумажные, машинные).

7.4.2. В Компании обеспечивается раздельное хранение ПДн при разных целях обработки и запрещается на одном носителе фиксация ПДн, цели обработки которых заведомо несовместимы. Ответственным за исполнение данного требования является работник Компании, организующий хранение ПДн на носителе информации.

7.4.3. По возможности Компания старается обеспечивать хранение ПДн в разных базах данных, документах, шкафах, с целью избегания ознакомления с избыточным составом ПДн при выполнении процесса, требующего меньшего состава ПДн, а также для обеспечения возможности уничтожения или блокирования ПДн при достижении целей обработки.

7.4.4. Досье субъектов ПДн (клиентов юридических лиц и индивидуальных предпринимателей), с которыми у Компании действующие договоры, хранятся в Компании в шкафах, комнатах, тумбочках, запираемых на ключ. При работе с документами из досье работники Компании руководствуются внутренними нормативными документами Компании. Работники Компании также передают клиентские досье на хранение в архив с указанием сроков хранения документов. Архивные услуги может оказывать внешняя организация в соответствии с договором.

7.4.5. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установ-

лен федеральным законом, согласием на обработку ПДн, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению в следующих случаях:

- по достижении цели обработки ПДн или в случае утраты необходимости в достижении этих целей (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн, в том числе в форме согласия на обработку ПДн, действующим законодательством РФ);
- отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если хранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн, действующим законодательством РФ);
- если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки ПДн, осуществляемой Компанией или обработчиком, действующим по ее поручению, если обеспечить правомерность обработки ПДн невозможно;
- выявления неправомерной обработки ПДн без согласия субъекта ПДн.

7.4.6. Порядок учета и хранения носителей ПДн определен в Инструкции о порядке учета, хранения и уничтожения носителей персональных данных на магнитной, магнитооптической и бумажной основе в ООО «Мерседес-Бенц Файненшл Сервисес Рус».

7.4.7. В Компании приказом Генерального директора определяется перечень помещений, в которых возможна обработка ПДн (в том числе хранение ПДн). Обработка ПДн вне данных помещений (расположение элементов ИСПДн, материальных носителей ПДн) запрещена.

7.4.8. Сроки хранения ПДн определяются на основании согласий на обработку ПДн, договоров, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, законодательства РФ.

7.4.9. Использование съемных машинных носителей (внешние жесткие диски, Flash-диски, CD/DVD-диски) для хранения ПДн запрещается за исключением следующих случаев:

- использование съемного машинного носителя ПДн в рамках процедур, предусматриваемых резервным копированием;
- использование съемного машинного носителя ПДн для хранения аутентификационной, парольной или ключевой информации.

7.5. Использование ПДн

7.5.1. В Компании 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.

7.5.2. В случае если какое-либо решение формируется в рамках работы ИСПДн, то данное решение обязательно должен подтвердить работник Компании.

7.5.3. В Компании определяется перечень работников Компании и лиц, допущенных к обработке ПДн. Данный перечень фиксируется в документе Перечень ПДн (п. 4.1 настоящего

Положения). В Компании запрещается использование ПДн посторонними лицами, за исключением случаев передачи ПДн или предоставления доступа к ПДн третьим лицам (в этом случае необходимо руководствоваться требованиями п. 7.6 настоящего Положения).

7.5.4. В Компании разрешена передача ПДн только между работниками Компании, имеющими доступ к соответствующему ресурсу ПДн (набору ПДн конкретного типа субъекта ПДн). Такая передача осуществляется в рабочем порядке с учетом технологии работы с соответствующим ресурсом ПДн.

7.6. Передача ПДн третьим лицам

7.6.1. Компания вправе поручить обработку ПДн другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора (поручения) (допускается оформление договора (поручения) в форме отдельного соглашения, соглашения о конфиденциальности и/или путем включения соответствующих положений в основной договор). Лицо, осуществляющее обработку персональных данных по поручению Компании (далее – «Подрядчик»), обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Положением.

7.6.2. Компанией передаются ПДн только на основании договора (поручения) в составе и объеме, необходимом для достижения заявленных целей обработки.

7.6.3. В Компании подлежат соблюдению Правила защиты данных, вследствие чего с Подрядчиком дополнительно должен быть подписан «Договор об обработке данных по поручению / Agreement on Data Processing on Behalf».

7.6.4. В договоре (поручении) в обязательном порядке должны быть определены:

- перечень действий (операций) с ПДн, которые будут совершаться лицом (перечень действий не должен противоречить целям и действиям, заявленным перед субъектом – в договоре, согласии и т. д.);
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре, в согласии и т. д.);
- обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке;
- требования к защите ПДн (требования по защите, предъявляемые к лицу, осуществляющему обработку, не должны быть выше требований, выполняемых Компанией – в идеальном случае требования должны быть идентичны);
- порядок передачи ПДн (или предоставления доступа к ним).

7.6.5. Ответственным за подписание необходимого договора с Подрядчиками является подразделение, инициирующее заключение договора с Подрядчиком.

7.6.6. При поручении обработки ПДн должны соблюдаться нижеперечисленные критерии, за обеспечение которых отвечает подразделение Компании (ответственное лицо), инициирующее привлечение Подрядчика:

- Подрядчик выбирается на основании его пригодности для обеспечения требуемых технических и организационных защитных мер[3];

[3] Пригодность Подрядчика может быть определена на основании самооценки Подрядчика и(или) соответствующих обязательств в соглашении с Компанией.

- перед началом обработки данных Компания должна убедиться в соблюдении Подрядчиком его обязанностей (соблюдение требований по безопасности данных подрядчик может подтвердить, предъявив, в частности, надлежащую сертификацию).

7.6.7. В Компании разрешена трансграничная передача ПДн на территорию иностранных государств:

- являющихся сторонами «Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- содержащихся в «Перечне иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных», утвержденном уполномоченным органом по защите прав субъектов ПДн.

7.6.8. В случае если иностранное государство не входит в перечень, описанный в п.7.6.7 настоящего Положения, то возможность трансграничной передачи разрешается только в следующих случаях:

- субъект дал письменное согласие на трансграничную передачу ПДн;
- передача осуществляется для исполнения договора, стороной которого является субъект ПДн;
- передача осуществляется для защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

7.6.9. Головная организация (штаб-квартира) концерна «Даймлер АГ» расположена в Федеративной республике Германия, которая входит в перечень, описанный в п.7.6.7 Положения, поэтому отдельного согласия на трансграничную передачу не требуется.

7.6.10. Компания в ходе своей деятельности кроме передачи ПДн третьим лицам (Подрядчикам, аудиторам и т.д.) может также предоставлять доступ к ПДн третьим лицам, которые хранятся и обрабатываются в ИСПДн Компании, либо в помещениях Компании. В этом случае необходимо обеспечить выполнение требований п.п. 7.6.1 – 7.6.6 настоящего Положения.

7.6.11. Прекращение доступа третьих лиц к ПДн осуществляется в случаях:

- отзыва субъектом ПДн согласия на обработку (как у Компании, так и отдельно на передачу данному третьему лицу), если иное не предусмотрено законодательством РФ;
- достижение целей обработки ПДн, если иное не предусмотрено согласием на обработку ПДн, законодательством РФ;
- прекращение договорных отношений (с учётом сроков обработки, предусмотренных в договорах, согласиях на обработку ПДн, сроками исковой давности)[4].

7.6.12. В случае если происходит частичный отзыв согласия на обработку ПДн, то прекращение доступа осуществляется в отношении тех процессов обработки ПДн, которые указаны в отзыве согласия на обработку, если в соответствии с требованиями действующего законодательства РФ, обработка не может быть продолжена.

7.6.13. Управление доступом осуществляется в соответствии с внутренними нормативными документами Компании, определяющими политику предоставления доступа (в том числе Корпоративная политика «Управление доступом к корпоративной информации» и др.).

[4] В случае, если существуют несоответствия между целями обработки ПДн и прекращением договорных отношений, то прекращение обработки ПДн осуществляется согласно целям обработки ПДн.

7.7. Прекращение обработки ПДн

7.7.1. Под прекращением обработки ПДн понимается остановка процессов обработки ПДн в Компании с обязательным осуществлением их блокирования или уничтожения. Указанные действия с ПДн также относятся к обработке ПДн и их выполнение свидетельствует о прекращении процессов обработки ПДн.

7.7.2. Случаи, когда необходимо прекратить обработку и осуществить блокировку или уничтожение ПДн, а также порядок осуществления этих мероприятий описаны в п.п. 7.8 – 7.10 настоящего Положения.

7.7.3. В Компании допускаются следующие способы осуществления прекращения обработки:

- автоматический в ИСПДн (в ИСПДн автоматически осуществляется проверка выполнения критериев достижения сроков и целей обработки ПДн и выполнение соответствующих процедур прекращения обработки);
- ручной на периодической основе (периодически осуществляется проверка достижения сроков и целей обработки ПДн на бумажных носителях и в ИСПДн по различным субъектам ПДн и осуществляется выполнение процедур прекращения обработки);
- ручной по результатам проведения контрольных мероприятий, выявления неправомерной обработки, запросов субъектов ПДн и т.д.

7.8. Блокирование ПДн

7.8.1. Блокировка ПДн подразумевает:

- запрет редактирования персональных данных в ИСПДн;
- информирование обработчиков о необходимости блокировки ПДн;
- запрет передачи ПДн (если передача не требуется согласно законодательству);
- изъятие бумажных документов, относящихся к субъекту ПДн и содержащих его ПДн из внутреннего документооборота Компании и запрет их использования (если это не нарушает требования законодательства).

7.8.2. Компания блокирует обрабатываемые ПДн с последующим уничтожением ПДн при отсутствии возможности уничтожения ПДн в течение срока, установленного Федеральным законом № 152-ФЗ от 27.07.2006 «О персональных данных». При этом уничтожение ПДн производится не позднее шести месяцев со дня их блокирования.

7.8.3. Компания блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых ПДн (неполные, устаревшие, неточные) или неправомерных действий в отношении субъекта ПДн (ПДн являются незаконно полученными или не являются необходимыми для установленной цели обработки) в следующих случаях:

- по требованию субъекта ПДн или его представителя;
- по требованию уполномоченного органа по защите прав субъектов ПДн;
- по результатам внутренних контрольных мероприятий (порядок проведения внутренних контрольных мероприятий описан в разделе 9 Регламента обеспечения безопасности персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус»).

7.8.4. В случае выявления неточных ПДн блокирование ПДн может быть осуществлено, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

7.8.5. Разблокировка ПДн может быть осуществлена для уточнения ПДн, по требованиям законодательства, а также если причины, в результате которых была осуществлена блокировка, были устранены.

7.8.6. Если субъект, ПДн которого заблокированы, повторно обращается в Компания, то его повторное согласие на обработку ПДн влечет разблокирование его ПДн.

7.8.7. Компания по возможности автоматизирует процесс блокирования ПДн в ИСПДн Компании для обеспечения своевременной реакции на необходимость блокировки ПДн.

7.9. Уничтожение ПДн

7.9.1. Компания уничтожает ПДн в случае:

- по достижении цели обработки ПДн или в случае утраты необходимости в достижении этих целей (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн, в том числе в форме согласия на обработку ПДн), либо если Компания не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством РФ;
- отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн и запрос не противоречит требованиям законодательства РФ (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Компанией и субъектом ПДн, законодательством РФ);
- если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки ПДн, осуществляемой Компанией или обработчиком, действующим по его поручению, если обеспечить правомерность обработки ПДн невозможно;
- выявления неправомерной обработки ПДн без согласия субъекта ПДн.
- получения соответствующего предписания от уполномоченного органа по защите прав субъектов ПДн.

7.9.2. Порядок уничтожения материальных носителей ПДн и ПДн на машинных носителях описан в Инструкции о порядке учета, хранения и уничтожения носителей персональных данных на магнитной, магнитооптической и бумажной основе в ООО «Мерседес-Бенц Файненшл Сервисес Рус».

7.9.3. Уничтожение ПДн в ИСПДн осуществляется в порядке и по инициативе лиц, определенных в Регламенте взаимодействия с субъектами персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус»:

- с использованием функций по уничтожению, реализованных в информационных системах, входящих в ИСПДн;
- путем удаления файлов с ПДн, удаление отдельных записей в файлах.

7.9.4. Компания вправе заключать договоры с третьими лицами на оказание услуг по уничтожению материальных носителей ПДн с соблюдением требований Федерального закона от № 152-ФЗ от 27.07.2006 «О персональных данных» по обеспечению конфиденциальности уничтожаемых ПДн. При этом в договоре должны быть определены порядок уничтожения

ПДн, порядок взаимодействия третьего лица с Компанией в части обработки запросов на уничтожения и предоставления отчетной документации по уничтожению материальных носителей ПДн (актов об уничтожении). Установленный в договоре порядок уничтожения ПДн должен обеспечивать требования к процедурам и механизмам уничтожения не ниже, предусмотренных в Инструкции о порядке учета, хранения и уничтожения носителей персональных данных на магнитной, магнитооптической и бумажной основе в ООО «Мерседес-Бенц Файненшл Сервисес Рус».

7.9.5. Согласно п. 2 ст. 1 Федерального закона от № 152-ФЗ от 27.07.2006 «О персональных данных» действие закона не распространяется на случаи, если обработка ПДн осуществляется для организации хранения, комплектования, учета и использования содержащих ПДн архивных документов в соответствии с законодательством об архивном деле в Российской Федерации. В виду этого, при передаче документов с ПДн третьим лицам, осуществляющим свою деятельность в соответствии с законодательством об архивном деле, требования п. 7.9.4 настоящего Положения не применяются, а применяется соответствующее законодательство[5].

7.10. Обеспечение точности, достаточности и актуальности ПДн

7.10.1. При обработке ПДн должны быть обеспечены точность, достаточность и, в необходимых случаях, актуальность по отношению к целям обработки ПДн. Компания предполагает, что субъект ПДн представил ему точные, достаточные и актуальные данные. Точность, достаточность и актуальность в процессе обработки ПДн достигается следующими методами:

- уведомлением субъектом ПДн об изменениях;
- выявлением Компанией неточности, недостоверности и последующими мероприятиями Компании для целей уточнения данных либо подтверждения их точности, достоверности и актуальности.

7.10.2. В случае выявления в рамках текущей деятельности Компании неточных, недостаточных или неактуальных ПДн осуществляется следующая совокупность действий:

- блокирование ПДн (только, если выявленная проблема может повлиять на деятельность Компании или права субъекта за время уточнения ПДн), если данные действия не нарушают прав и законных интересов субъекта ПДн или третьих лиц;
- уточнение ПДн, в результате которых снимается блокирование ПДн.

Работник Компании, который выявил неточные, недостаточные или неактуальные ПДн должен уведомить об этом Ответственного за координацию отзывов согласий при их поступлении в Компанию, который должен определить соответствующего Ответственного за организацию обработки ПДн согласно Регламенту взаимодействия с субъектами персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус» и проинформировать его о выявленном факте. Ответственный за организацию обработки ПДн (в значении термина, определенного в Регламенте взаимодействия с субъектами персональных данных в ООО «Мерседес-Бенц Файненшл Сервисес Рус») должен обеспечить выполнение указанных выше операций.

7.10.3. Необходимость обеспечения точности, достаточности и актуальности возникает на момент выполнения Компанией действий, в результате которых могут возникнуть следующие события:

[5] Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации».

- представление неверных сведений о субъекте в органы государственной власти и местного самоуправления, во внебюджетные фонды и т.д.;
- проведение денежных или имущественных операций с субъектом (или где субъект является выгодоприобретателем), в результате которых субъект получает убытки или недополучает прибыль в результате неверных сведений;
- опубликование или предоставление неверной информации о субъекте, в результате которой могут возникнуть различные негативные последствия для субъекта (моральный ущерб, убытки, вред здоровью, необеспечение своевременной медицинской помощи, недополученная прибыль и т.д.);
- неточная или неактуальная информация о субъекте может повлечь убытки Компании;
- другие события, так или иначе негативно влияющие на деятельность субъекта ПДн и/или Компании.

В случае если на момент осуществления указанных действий не наступили события, поименованные в п. 7.11.1, ПДн признаются точными, достаточными и актуальными.

7.11. Особенности обработки ПДн, осуществляемой без использования средств автоматизации

7.11.1. В связи с тем, что в Компании происходит обработка ПДн на материальных носителях ПДн (бумажные документы), то в Компании том числе осуществляется обработка ПДн без использования средств автоматизации.

7.11.2. Обработка персональных данных, осуществляемая без использования средств автоматизации, строится на принципах, изложенных в «Положении об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденном Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687.

8. Ознакомление с нормативными актами и правилами обработки ПДн

8.1. Все работники Компании, а также работники соответствующих подразделений АО «Мерседес-Бенц РУС», ООО «Мерседес-Бенц Капитал Рус», «Мерседес-Бенц Банк Рус» ООО, непосредственно привлечённых Компанией для осуществления ключевых функций, ознакомляются под роспись с нормативными документами Компании в области обработки и безопасности ПДн, включая настоящее Положение.

8.2. Обучение по вопросам обработки и защиты ПДн осуществляется в Компании следующим способами:

- обучение правилам обработки ПДн в рамках бизнес-процессов Компании (обучение проводит непосредственный руководитель работника). Периодичность: не реже одного раза в два года;
- обучение правилам обработки и защиты ПДн в рамках тренингов по вопросам обеспечения ИБ (обучение проводит лицо, ответственное за ИБ). Периодичность: не реже одного раза в два года.

8.3. Помимо работников Компании осуществляется обучение лиц, участвующих в процессах обработки ПДн по поручению Компании (работников контрагентов). Такое обуче-

ние координируется Ответственным за безопасность ПДн. В случае, если контрагент предоставляет Компании гарантии (в тексте договора (поручения), а также свидетельства в виде программы или плана обучения), что обучение работников по вопросам обработки и защиты ПДн, осуществляется им самостоятельно, то Компания не осуществляет дополнительного обучения.

9. Управление доступом к ПДн

9.1. Управление доступом работников Компании к ПДн

9.1.1. К обработке ПДн допускаются работники Компании, включенные в Перечень ПДн («Перечень обрабатываемых персональных данных, информационных систем персональных данных и лиц, допущенных к обработке персональных данных»).

9.1.2. Работники обязаны получать доступ только к тем ПДн, доступ к которым необходим в связи с исполнением ими должностных обязанностей.

9.1.3. Работник допускается к обработке ПДн только после:

- ознакомления под подпись с требованиями настоящего Положения и иными организационно-распорядительными документами Компании по обработке и защите ПДн, выполнение требований которых обязательно для соответствующего работника;
- подписи обязательства о неразглашении информации, содержащей ПДн (примерная форма указана в Приложении № 1 к Положению) или в составе должностной инструкции.

9.1.4. Хранение подписанного обязательства о неразглашении информации, содержащей ПДн, должно осуществляться подразделением (подрядчиком), выполняющим функции по кадровому администрированию в личном файле работника.

9.1.5. Прекращение доступа работников Компании к ПДн осуществляется в случаях:

- выявления несоблюдения работником требований Компании в области обработки и защиты ПДн;
- выявления неправомерного или недобросовестного использования работником ПДн, в том числе использования в личных целях;
- прекращение трудовых отношений.

9.1.6. Решение о предоставлении доступа принимается владельцем ресурса, решение о прекращении доступа принимается владельцем ресурса на основании выявленной информации или информации о прекращении трудовых отношений[6].

9.2. Управление доступом к ПДн третьих лиц, определяется договором между Компанией и третьим лицом и/или поручением. Ответственность за управление доступом сотрудников третьих лиц несет непосредственно привлеченное третье лицо.

[6] Доступ уволившемуся работнику может быть прекращен автоматически по факту его увольнения.

10. Взаимодействие с субъектами ПДн и органами власти

10.1. Взаимодействие с субъектами ПДн

10.1.1. Порядок взаимодействия с субъектами ПДн или их законными представителями описан в Регламенте взаимодействия ООО «Мерседес-Бенц Файненшл Сервисес Рус» с субъектами персональных данных.

10.2. Взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, а также третьими лицами, включая органы государственной власти.

10.2.1. Взаимодействие с уполномоченным органом по защите прав субъектов ПДн, а также третьими лицами, включая органы государственной власти, осуществляется в соответствии с законодательством РФ.

10.2.2. В целях исполнения требований законодательства РФ Компания, до начала обработки ПДн, уведомила уполномоченный орган по защите прав субъектов персональных данных (далее - «Уполномоченный орган») о своем намерении осуществлять обработку ПДн, направив соответствующие уведомление (далее - «Уведомление»), по форме, предусмотренной действующим законодательством РФ и Уполномоченным органом.

10.2.3. Уполномоченным органом (основным регулятором в сфере обработки ПДн) является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – «Роскомнадзор»). Надзор осуществляется в соответствии с «Административным регламентом исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» (Утвержден Приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312).

10.2.4. В случае изменения сведений, указанных Уведомлении, а также в случае прекращения обработки персональных данных Компания обязана уведомить об этом Роскомнадзор в течение 10 (десяти) рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных, если иной срок не установлен законодательством РФ. За организацию формирования и предоставления соответствующего информационного письма отвечает Ответственный за организацию обработки ПДн.

10.2.5. ФСБ России и ФСТЭК России могут быть наделены решением Правительства РФ полномочиями по контролю выполнения Компанией организационных и технических мер по обеспечению безопасности ПДн, без права ознакомления с ПДн, обрабатываемыми в ИСПДн. В т. ч. это касается отдельных решений Правительства РФ о проведении контрольных мероприятий.

10.2.6. В Компании ответственность за организацию взаимодействия с регулирующими органами по вопросам обработки и обеспечения защиты ПДн, в том числе при получении запроса Роскомнадзора, проведении плановых и внеплановых проверок, а также за координацию сотрудников при проведении проверок возлагается на Ответственного за организацию обработки ПДн.

10.2.7. В случае проведения проверки Роскомнадзором для взаимодействия с регулятором привлекается компания, оказывающая услуги по юридическому сопровождению деятельности Компании (АО «Мерседес-Бенц РУС»), Ответственный за обеспечение безопасности ПДн, ОКРИБ, иные сотрудники Компании (при необходимости).

10.2.8. В случае проведения проверок ФСТЭК России или ФСБ России для взаимодействия с Регуляторами в обязательном порядке привлекается Ответственный за обеспечение безопасности ПДн и сотрудники ОКРИБ.

10.2.9. Срок проведения как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней. В случае возникновения необходимости срок проведения проверки может быть продлен, но не более чем на двадцать рабочих дней. Основанием для продления сроков проведения проверки является приказ руководителя регулятора.

10.2.10. Результаты проверки оформляются актом, который составляется должностными лицами регулятора непосредственно после завершения проверки. В акте указывается:

- дата, время и место составления акта проверки;
- наименование органа федерального государственного контроля (надзора);
- дата и номер приказа проведения проверки;
- цели, задачи и предмет проверки;
- Ф.И.О. должностных лиц, проводивших проверку;
- наименование Оператора, а также Ф.И.О. и должность лиц, присутствовавших при проведении проверки;
- дата, время, продолжительность и место проведения проверки;
- сведения о результатах проверки, в том числе о выявленных нарушениях в области ПДн, об их характере и о лицах, допустивших указанные нарушения.
- сведения об ознакомлении или отказе в ознакомлении с актом проверки руководителя, иного уполномоченного представителя Компании, присутствовавших при проведении проверки, о наличии их подписей или об отказе от совершения подписи;
- сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у Компании указанного журнала.

10.2.11. Акт закрепляется подписями должностных лиц регулятора проводивших проверку и должен содержать одно из следующих заключений:

- об отсутствии в деятельности Компании нарушений требований законодательства Российской Федерации в области ПДн;
- о выявленных в деятельности Компании нарушениях требований законодательства Российской Федерации в области ПДн, с указанием конкретных статей и (или) пунктов нормативных правовых актов.

10.2.12. В случае выявления по результатам проверки нарушения требований законодательства Российской Федерации в области ПДн, вместе с актом, выдается предписание об устранении выявленных нарушений, в котором указываются:

- наименование органа федерального государственного контроля (надзора);
- дата выдачи предписания об устранении выявленных нарушений;
- номер предписания об устранении выявленных нарушений;
- наименование Оператора;
- регистрационный номер Оператора в Реестре (при наличии);

- наименование вида деятельности;
- дата и номер акта проверки;
- содержание нарушения;
- основание выдачи предписания;
- срок устранения нарушения;
- срок информирования органа федерального государственного контроля (надзора) об устранении выявленного нарушения;
- подписи должностных лиц, проводивших проверку.

10.2.13. Уполномоченным органом, ФСТЭК России, ФСБ России могут направляться мотивированные запросы в Компанию. Срок подготовки ответа – 10 дней с даты его получения (если иное не указано в запросе).

10.2.14. Регистрация и исполнение поступивших запросов, а также ответов на них осуществляется в соответствии с правилами документооборота Компании.

10.2.15. Запросы, а также ответы на них должны храниться в Компании в течение срока, установленного в соответствии с правилами внутреннего документооборота Компании.

11. Права Компании и субъекта ПДн

11.1. Права Компании

11.1.1. Компания вправе отстаивать свои интересы в суде.

11.1.2. Компания вправе предоставлять ПДн субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы, суды и др.) или получено согласие субъекта на такую передачу (при этом должны выполняться требования п. 7.6 Положения).

11.1.3. Компания вправе осуществлять проверку достоверности сведений, предоставленных субъектом ПДн.

11.1.4. Компания вправе требовать уточнений ПДн у субъектов ПДн, в случае если ПДн являются неполными, устаревшими, недостоверными в рамках требований п. 7.11 Положения.

11.1.5. Компания вправе на законных основаниях отказать в предоставлении сведений субъекту ПДн.

11.1.6. Иные права, установленные действующим законодательством.

11.2. Права субъекта ПДн

11.2.1. Субъект ПДн имеет право осуществлять действия, предусмотренные п. 10.1 Положения в части уточнения, блокирования, уничтожения ПДн, а также ознакомления с характеристиками процесса обработки его ПДн (цели обработки, состав ПДн, источник получения ПДн, сроки обработки и хранения ПДн, характер обработки ПДн и др.).

11.2.2. Субъект ПДн имеет право извещения всех лиц, которым ранее были сообщены неверные или неполные его ПДн, обо всех изменениях его ПДн.

11.2.3. Субъект ПДн имеет право обжаловать в Роскомнадзор или в судебном порядке неправомерные действия или бездействия Компании при обработке его ПДн.

12. Организационная структура Компании в сфере обработки ПДн. Требования по защите ПДн

12.1. С целью организации и контроля обработки и обеспечения безопасности ПДн, в Компании вводятся следующее роли, которые составляют основу организационной структуры в сфере обработки ПДн:

- Ответственный за организацию обработки ПДн;
- ОКРИБ;
- Ответственный за обеспечение безопасности ПДн;
- Временная комиссия по защите ПДн (далее – «Комиссия»);
- Департамент по работе с персоналом;
- Административные ассистенты и работники Компании, которые получили запрос или обращение субъекта ПДн (если поступление запроса или обращения было осуществлено по электронным каналам связи);
- Ответственный за координацию отзывов согласий при их поступлении в Компанию;
- Ответственный за резервное копирование;
- Руководители структурных подразделений Компании.

12.2. Функции указанных в п. 12.1. настоящего Положения лиц определяются внутренними документами Компании, в том числе в области обработки и защиты ПДн.

13. Контрольные процедуры

13.1. Контроль за процессом обработки и защиты ПДн осуществляется в рамках общей системы внутреннего контроля Компании.

13.2. К числу основных контролирующих органов за соблюдением требований настоящего Положения относятся:

- Генеральный директор;
- Ответственный за организацию обработки ПДн;
- ОКРИБ;
- Ответственный за обеспечение безопасности ПДн;
- Руководители структурных подразделений Компании.

13.2.1. Генеральный директор и Ответственный за организацию обработки ПДн осуществляет:

- принятие стратегических решений в сфере обработки и защиты ПДн;
- утверждение внутренних нормативных документов, регламентирующих обработку и защиту ПДн (применительно к генеральному директору).

13.2.2. Ответственный за обеспечение безопасности ПДн и сотрудники ОКРИБ осуществляют:

- текущий контроль за обеспечением безопасности ПДн и соблюдением законодательных требований при обработке ПДн (автоматизированной и неавтоматизированной);
- иные контрольные функции согласно внутренним документам Компании в области обработки и защиты ПДн.

13.2.3. Руководители структурных подразделений Компании

- постоянный контроль выполнения работниками структурных подразделений процедур, предусмотренных Положением и иными нормативными документами в области обработки и защиты ПДн;
- принятие решения о передаче документов, содержащих ПДн, в архив с указание сроков хранения;
- выявление новых процессов обработки ПДн и информирование о них Ответственного за организацию обработки ПДн;
- иные функции согласно внутренним документам Компании.

14. Перечень используемых нормативных документов.

14.1. Настоящее Положение разработано в соответствии со следующими нормативными актами и внутренними документами:

- Конституция Российской Федерации, принята всенародным голосованием 12.12.1993 (с изменениями);
- Трудовой Кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (с изменениями);
- Гражданский кодекс Российской Федерации от 21.10.1994 N 51-ФЗ (с изменениями);
- Федеральный закон № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» (с изменениями);
- Федеральный закон от № 152-ФЗ от 27.07.2006 «О персональных данных» (с изменениями);
- Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Приказ ФСТЭК России 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»;
- Административным регламентом исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (Утвержден Приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312);
- Корпоративная политика концерна «Даймлер» «Общекорпоративные правила защиты данных» (краткое наименование – Правила защиты данных, номер правил – A 17.1);
- Иные документы.

15. Заключительные положения

15.1. Настоящее Положение вступает в силу с момента его утверждения и действует до момента внесения изменений и/или принятия нового документа в соответствии с внутренним порядком Компании.

15.2. С даты утверждения настоящего Положения прекращает свое действие Положение об обработке и защите персональных данных ООО «Мерседес-Бенц Файненшл Сервисес Рус», утвержденное Приказом № 20170131-01 от 31.01.2017 года.

Приложение №1
к Положению об обработке и защите персональных данных

Форма обязательства о неразглашении информации, содержащей персональные данные (пример)

Я,_____,
(ФИО, должность, наименование структурного подразделения, наименование организации)

предупрежден (а) о том, что на период действий договора об оказании услуг/трудового договора с ООО «Мерседес-Бенц Файненшл Сервисес Рус» и исполнения условий договора/должностных обязанностей в соответствии с должностной инструкцией с внутренними нормативными документами Компании мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

- не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением условий договора/должностных обязанностей в соответствии с должностной инструкцией с внутренними нормативными документами Компании;

- в случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать руководителям структурных подразделений Компании;

- не использовать информацию, содержащую персональные данные, с целью получения личной выгоды;

- выполнять требования нормативно-правовых актов, внутренних правил, регламентирующих работу с информацией, содержащую персональные данные;

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

Обязанность соблюдения конфиденциальности информации, содержащей персональные данные, остается в силе также и после окончания трудовых отношений.

_____ _____
(ФИО) (подпись)

«_____»_____ _____г.