Правила защиты данных (ЕС)

Mercedes-Benz

Содержание

1 Цель Правил

Mercedes-Benz Group рассматривает обеспечение прав на защиту данных как часть своей социальной ответственности.

В некоторых странах и регионах, таких как страны Европейского Союза, законодательством установлены стандарты защиты данных физических лиц («персональных данных»), включая требование о том, что такие данные разрешается передавать в другие страны, только если в месте назначения обеспечивается надлежащий уровень защиты данных.

Настоящие Правила защиты данных (ЕС) устанавливают единые и подходящие стандарты защиты данных в рамках концерна как для:
- (а) обработки персональных данных в таких регионах, как ЕС / Европейская экономическая зона (ЕЭЗ) (далее совместно именуемые **«ЕС/ЕЭЗ»**), так и для
- (б) трансграничной передачи персональных данных компаниям концерна за пределами ЕС/ЕЭЗ (включая их последующую обработку там).

С этой целью настоящие Правила устанавливают обязательные регламенты обработки персональных данных из стран ЕС/ЕЭЗ в рамках Mercedes-Benz Group. Эти регламенты обеспечивают надлежащие гарантии защиты персональных данных за пределами ЕС/ЕЭЗ и рассматриваются как «Обязательные корпоративные правила» («Binding Corporate Rules – BCR») для Mercedes-Benz Group.

2 Сфера применения

Настоящие Правила защиты данных ЕС применяются для концерна Mercedes-Benz Group AG, подконтрольных концерну компаний (ниже именуемых **Компании концерна**), а также их сотрудников и членов руководящих органов. «Подконтрольные» в настоящем смысле означает, что Mercedes-Benz Group AG прямо или косвенно на основе обладания большинством прав голоса, большинства представительства в управлении компании или на основе соглашения вправе требовать принятия настоящих Правил.

Действие Правил распространяется на полностью или частично автоматизированную обработку персональных данных , а также на неавтоматизированную обработку в файловых системах, если только национальное законодательство не расширяет сферу их действия. В Германии настоящие Правила также действительны для всех данных о сотрудниках[1] в бумажной форме.
Действие Правил распространяется на обработку персональных данных:
- (а) компаний концерна и их филиалов с местонахождением в ЕС/ЕЭЗ или другой стране, на которые может распространяться действие настоящих Правил («компании из ЕС/ЕЭЗ»),
- (б) компаний концерна с местонахождением за пределами ЕС/ЕЭЗ, если они предлагают товары или услуги физическим лицам на территории ЕС/ЕЭЗ и/или осуществляют мониторинг поведения физических лиц на территории ЕС/ЕЭЗ («компании из третьих стран с предложениями для ЕС/ЕЭЗ») или
- (в) компаний концерна с местонахождением за пределами ЕС/ЕЭЗ, если они прямо или косвенно получили персональные данные от компаний, подпадающих под действие Правил в соответствии с пунктами а) или б), или если такие данные были им раскрыты («компании в третьих странах, получающие данные из ЕС/ЕЭЗ»).

[1] В настоящих Правилах в отношении физических лиц в целях упрощения используется только мужская форма. При этом подразумеваются представители всех гендерных идентичностей.

Обработка за пределами ЕС/ЕЭЗ далее рассматривается в настоящих Правилах как обработка в третьей стране.

Компании концерна, которые участвуют в обработке данных компаниями в третьих странах или подлежат такой обработке, приведены в параллельно действующем регламенте «Список компаний концерна, связанных Правилами защиты данных (ЕС)».

Действие настоящих Правил может распространяться на страны за пределами ЕС/ЕЭЗ. В странах, в которых данные юридических лиц защищаются в равной мере с персональными данными , настоящие Правила действуют в той же степени и для данных юридических лиц.

3 Правовая обязательность в пределах Mercedes-Benz Group

Положения настоящих Правил являются обязательными для всех компаний концерна, действующих в рамках сферы действия Правил. Поэтому в дополнение к действующему законодательству ЕС и национальным законам о защите данных компании концерна, а также их руководство и сотрудники несут ответственность за соблюдение настоящих Правил.

Если иное не предусмотрено законодательством, компании концерна не вправе принимать регламенты, отклоняющиеся от настоящих Правил.

4 Отношение к требованиям законодательства

Настоящие Правила не заменяют собой предписания ЕС и национальные законы. Они дополняют национальные законы о защите данных. Эти предписания и законы имеют приоритет, если соблюдение настоящих Правил может привести к нарушению национального законодательства. Содержание настоящих Правил также должно соблюдаться при отсутствии соответствующих национальных законов.

Если соблюдение настоящих Правил может привести к нарушению норм национального законодательства или если согласно нормам национального законодательства требуются регламенты, отличающиеся от настоящих Правил, об этом в рамках мониторинга законодательства о защите данных необходимо сообщить Уполномоченному концерна по вопросам защиты данных и центральной организации нормативно-правового регулирования. В случае противоречий между нормами национального законодательства и настоящими Правилами Уполномоченный концерна по вопросам защиты данных и центральная организация по вопросам нормативно-правового регулирования совместно с ответственной компанией концерна будут работать над поиском практического решения, отвечающего целям настоящих Правил.

5 Общие принципы обработки персональных данных

5.1 Правомерность

Персональные данные должны обрабатываться законным и добросовестным образом. Обработка данных может производиться лишь в том случае и в той мере, в какой существует достаточное правовое основание для осуществления обработки. Это также относится к обработке данных, осуществляемой между компаниями концерна. Сам факт того, что и передающая, и принимающая компании входят в состав концерна Mercedes-Benz Group, не является таким явным правовым основанием.

Обработка персональных данных допускается при наличии одного из приведенных в Разделах 5.2 и 5.3 оснований для разрешения. Наличие таких оснований для разрешения также необходимо, если цель обработки персональных данных должна быть изменена относительно первоначальной цели.

5.2 Правовое основание для данных клиентов и партнеров

5.2.1 Обработка данных в рамках договорных отношений

Персональные данные потенциального заказчика, клиента или партнера могут обрабатываться в рамках заключения, выполнения и расторжения договора. Сюда также относится обслуживание клиента или партнера, если такое обслуживание связано с целями договора.

До заключения договора персональные данные могут обрабатываться для подготовки предложений или заказов на поставку, а также для выполнения других запросов потенциального заказчика, связанных с заключением договора. Во время подготовки договора разрешается установление контакта с заинтересованными лицами, используя предоставленные ими данные. Необходимо соблюдать возможные ограничения, высказанные заинтересованным лицом.

5.2.2 Обработка данных в рекламных целях

Если субъект данных обращается в компанию концерна с запросом информации (например, с запросом на получение информационных материалов о продукте), то обработка данных для удовлетворения этого запроса разрешена. Меры по укреплению связей с клиентами и рекламные мероприятия требуют дальнейших правовых предпосылок. Персональные данные могут обрабатываться в рекламных целях или в целях изучения рынка и общественного мнения при условии, что такая обработка соответствует цели, для которой данные были первоначально собраны. Субъект данных должен быть заранее проинформирован об использовании его личных данных в рекламных целях. Если данные собираются исключительно в рекламных целях, то их указание затронутым лицом производится на добровольной основе. Субъект данных должен быть проинформирован о том, что предоставление данных для этой цели является добровольным. В рамках процесса коммуникации от субъекта данных должно быть получено согласие. Выражая свое согласие, субъект данных должен иметь возможность выбора между доступными каналами связи, такими как электронная почта и телефон (согласие см. в Разделе 5.2.3). Если субъект данных возражает против использования его данных в рекламных целях, они больше не могут использоваться для этих целей и должны быть ограничены или заблокированы для использования в этих целях. Необходимо соблюдать выходящие за рамки данного положения ограничения, которые действуют в некоторых странах в отношении использования данных в рекламных целях.

5.2.3 Согласие на обработку данных

Обработка данных может производиться на основе согласия затронутого лица. Прежде чем дать согласие, субъект данных должен быть проинформирован в соответствии с настоящими Правилами защиты данных (ЕС). В доказательных целях заявление о согласии должно принципиально предоставляться в письменной или электронной форме. При определенных обстоятельствах (например, при консультировании по телефону) согласие может быть выражено в устной форме, что должно быть задокументировано.

5.2.4 Обработка данных на основе законного разрешения или обязанности

Обработка персональных данных допускается также и в случае, если законодательные нормы требуют, предполагают или разрешают обработку данных. Вид и объем обработки данных должны соответствовать требованиям допустимой на законных основаниях обработки данных и определяются этими законодательными нормами.

5.2.5 Обработка данных на основе законного интереса

Персональные данные также могут обрабатываться, если это необходимо в законных интересах. Законные интересы, как правило, имеют правовой характер (например, взыскание непогашенной дебиторской задолженности) или коммерческий характер (например, недопущение нарушений договора). Обработка не может осуществляться на основании законного интереса, если в конкретном случае заслуживающие защиты интересы субъекта данных преобладают над законными интересами, связанными с обработкой. Достойные защиты интересы подлежат проверке при любой обработке.

5.3 Правовое основание для данных сотрудников

5.3.1 Обработка данных в рамках трудовых отношений

В рамках трудовых отношений персональные данные могут обрабатываться в случае необходимости установления, осуществления и прекращения трудовых отношений. В целях принятия решения о заключении трудовых отношений могут обрабатываться персональные данные кандидатов на должности. После отказа в занятии должности данные кандидата должны быть удалены при соблюдении доказательных сроков, если при этом кандидат не дал своего согласия на дальнейшее сохранение своих данных для более поздней процедуры отбора. Получение согласия также необходимо для использования данных для дальнейших процедур по подаче заявления на вакантную должность или перед их передачей в другие компании концерна. В существующих трудовых отношениях обработка данных всегда должна быть связана с целью трудовых отношений, за исключением случаев, когда применяется одно из следующих оснований для разрешения обработки данных.

Если в рамках установления трудовых отношений или действующих трудовых отношений необходим сбор дополнительной информации о кандидате у третьих лиц, то подлежат соблюдению соответствующие требования национального законодательства. В случае сомнения, если это допустимо, необходимо получить согласие субъекта данных .

Для обработки персональных данных, связанных с трудовыми отношениями, но не служивших изначально для установления или прекращения трудовых отношений (данные сотрудников), должно иметься одно из нижеприведенных правовых оснований.

5.3.2 Обработка данных на основе законного разрешения или обязанности

Обработка данных сотрудника допускается также и в том случае, если законодательные нормы требуют, предполагают или разрешают такую обработку данных. Вид и объем обработки данных должны соответствовать требованиям допустимой на законных основаниях обработки данных и определяются этими законодательными нормами. Если законодательством предусматривается свобода действия, то должны учитываться достойные защиты интересы сотрудника.

5.3.3 Коллективное соглашение об обработке данных

Если обработка данных выходит за рамки целей выполнения договора, она все равно может быть законной, если это разрешено коллективным соглашением. Регламенты должны охватывать конкретную цель требуемой обработки данных и составляться в соответствии с предписаниями ЕС и нормами национального законодательства.

5.3.4 Согласие на обработку данных

Обработка данных сотрудника может производиться на основе согласия затронутого сотрудника. Подача заявлений о согласии осуществляется в добровольном порядке. За отказ в согласии не могут налагаться какие-либо санкции. Заявления о согласии, предоставленные не в добровольном порядке, недействительны. В доказательных целях заявление о согласии должно принципиально предоставляться в письменной или электронной форме. Если в исключительных случаях обстоятельства этому препятствуют, то согласие может быть выражено в устной форме. В любом случае, предоставление согласия должно быть надлежащим образом документировано. Прежде чем дать согласие, субъект данных должен быть проинформирован в соответствии с настоящими Правилами защиты данных (ЕС).

5.3.5 Обработка данных на основе законного интереса

Данные сотрудников также могут обрабатываться, если это необходимо в законных интересах компании концерна. Законные интересы, как правило, имеют правовой характер (например, подача, исполнение или защита от судебных исков) или коммерческий характер (например, ускорение бизнес-процессов, оценка компаний). Прежде чем приступить к обработке данных, должно быть определено, имеются ли заслуживающие защиты интересы. Персональные данные сотрудников могут обрабатываться на основе законного интереса, если заслуживающие защиты интересы сотрудника не преобладают над интересами, связанными с обработкой.

Меры контроля, требующие обработки данных сотрудников вне рамок трудовых отношений (например, проверка результативности), не могут быть приняты, если только для этого нет юридических обязательств или обоснованных причин. Даже при наличии обоснованных причин необходимо рассмотреть вопрос о соразмерности мер контроля. С этой целью правомерные интересы компании концерна в осуществлении меры контроля (например, соблюдение требований законодательства и внутренних правил компании) должны быть сопоставлены с возможными правомерными интересами соответствующего сотрудника в исключении этой меры. Эти меры могут быть приняты только, если они уместны в конкретном случае. Перед принятием каких-либо мер должны быть определены и задокументированы законные интересы компании концерна и возможные правомерные интересы сотрудника. Кроме того, должны учитываться другие требования действующего законодательства (например, право рабочих и служащих участвовать в управлении производством и право субъектов данных на получение информации).

5.4 Обработка особо конфиденциальных данных

Обработка особо конфиденциальных персональных данных может производиться только в том случае, если это разрешено или предписано законодательством. Обработка таких данных компанией концерна допускается, в частности, если субъект данных дал на нее свое явное согласие, если обработка необходима для предъявления, осуществления или защиты юридических претензий в отношении субъекта данных или если обработка необходима для осуществления прав и обязанностей в области трудового или социального права.

В случае если планируется обработка особо конфиденциальных персональных данных, об этом необходимо заранее уведомить Уполномоченного концерна по вопросам защиты данных.

5.5 Автоматизированное принятие индивидуальных решений (по возможности, включая профилирование)

В отношении субъекта данных может быть принято полностью автоматизированное решение, которое может иметь для него правовые или аналогичные негативные последствия, только если это необходимо для заключения или выполнения договора или если субъект данных дал свое согласие на это. В некоторых случаях такое автоматизированное решение может включать в себя профилирование, т. е. обработку персональных данных, в рамках которой производится оценка индивидуальных характеристик лица (например, кредитоспособности). В этом случае субъект данных должен быть уведомлен о факте и результате автоматизированного индивидуального решения, и ему должна быть предоставлена возможность индивидуального рассмотрения дела ответственным лицом.

5.6 Обязанность информирования/прозрачность

Ответственное структурное подразделение должно информировать субъектов данных о целях и обстоятельствах обработки их персональных данных в соответствии со статьями 13 и 14 GDPR. Если данные не попадают в сферу действия Общего регламента по защите данных (GDPR), информация предоставляется в соответствии с применимым национальным законодательством. Информация должна быть предоставлена в точной, прозрачной, понятной и легкодоступной форме, а также ясным и простым языком. Должны соблюдаться требования Уполномоченного концерна по вопросам защиты данных и Подразделения нормативно-правового соответствия данных (Data Compliance). Эта информация должна всегда предоставляться при первом сборе персональных данных. Если компания концерна получает персональные данные от третьей стороны, она обязана предоставить информацию об этом субъекту данных в течение разумного срока после получения данных, за исключением случаев, когда:

- субъект данных уже имеет эту информацию или
- было бы невозможно или
- чрезвычайно трудно предоставить эту информацию.

5.7 Предназначение

Персональные данные могут обрабатываться только в законных целях, определенных до сбора данных. Последующие изменения цели обработки допускаются только при условии совместимости обработки с целями, для которых изначально были собраны персональные данные.

5.8 Минимизация данных

Любая обработка персональных данных должна, как количественно, так и качественно, ограничиваться тем, что необходимо для достижения целей, для которых эти данные обрабатываются на законных основаниях. Это необходимо учитывать уже при определении объема собираемых данных. Если это позволяет цель, а усилия соразмерны преследуемой цели, должны использоваться анонимизированные или статистические данные.

5.9 Точность данных

Сохраненные персональные данные должны быть объективно точными и, при необходимости, актуальными. Ответственные структурные подразделения должны принимать соответствующие меры для обеспечения удаления, исправления, дополнения или обновления неверных или неполных данных.

5.10 Проектируемая конфиденциальность и конфиденциальность по умолчанию

«Принцип проектируемой конфиденциальности» направлен на обеспечение того, чтобы структурные подразделения определяли внутренние стратегии в соответствии с современными техническими требованиями и принимали меры по интеграции принципов защиты данных в спецификацию и архитектуру бизнес-моделей/процессов и ИТ-систем для обработки данных с самого начала на этапе разработки концепции и технического проектирования. В соответствии с «Принципом проектируемой конфиденциальности» процедуры и системы обработки персональных данных должны быть разработаны таким образом, чтобы их первоначальные настройки ограничивались обработкой данных, необходимой для достижения цели (принцип «Конфиденциальность по умолчанию»). Сюда относятся объем обработки, срок хранения и доступность. Дальнейшие меры могут включать в себя:

- псевдонимизацию персональных данных в максимально кратчайшие сроки,
- обеспечение прозрачности в отношении функций и обработки персональных данных,
- предоставление субъектам данных возможности принимать решения об обработке их персональных данных,
- предоставление операторам процедур или систем возможности разрабатывать и совершенствовать функции безопасности.

В целях обеспечения неукоснительного соблюдения вышеуказанных принципов каждая компания концерна должна внедрять и поддерживать соответствующие технические и организационные меры на протяжении всего жизненного цикла процессов обработки данных.

5.11 Удаление и анонимизация

Персональные данные могут храниться только до тех пор, пока это необходимо для целей, для которых они обрабатываются. Это означает, что персональные данные должны быть удалены или анонимизированы , как только цель, с которой они обрабатывались, была достигнута или необходимость в ее достижении отпала по какой-то причине, за исключением тех случаев, когда продолжают действовать требования по хранению или доказательству. Ответственные за отдельные процедуры должны обеспечить выполнение процедур удаления и анонимизации в рамках своих процедур. Каждая система должна иметь процедуру ручного или автоматизированного удаления. Запросы субъектов данных на удаление или устранение персональных идентификаторов должны быть технически осуществимы в системах. Должны соблюдаться требования, предъявляемые Mercedes-Benz Group к выполнению процедур удаления (например, программные инструменты, руководство по реализации концепции удаления, требования к документации).

5.12 Безопасность обработки

Персональные данные должны быть защищены от несанкционированного доступа и незаконной обработки или передачи, а также от случайной потери, изменения или уничтожения. Перед внедрением новые методов обработки данных, в частности новых ИТ-систем, должны быть определены и внедрены технические и организационные меры по защите персональных данных. Эти меры должны основываться на современном уровне техники, рисках обработки и необходимости защиты данных.

Относящиеся к защите данных технические и организационные меры должны документироваться ответственным лицом в рамках оценки воздействия на защиту данных и Регистра обработки данных.

В частности, ответственное структурное подразделение должно проконсультироваться со своими Уполномоченным по защите бизнес-информации (BISO) и Уполномоченным по информационной безопасности (ISO), а также со своей Сетью защиты данных. Требования к техническим и организационным мерам по защите персональных данных являются частью Управления корпоративной информационной безопасностью и должны постоянно корректироваться в соответствии с техническими разработками и организационными изменениями.

5.13 (Дальнейшая) передача за пределы Mercedes-Benz Group AG

Передача персональных данных получателям за пределами или внутри компаний концерна осуществляется при условии соблюдения требований к допустимости обработки персональных данных в соответствии с настоящим разделом 5. Получатель данных обязан использовать их только для определенных целей.

В случае трансграничной передачи персональных данных (включая предоставление доступа из другой страны) должны быть выполнены соответствующие национальные требования по передаче персональных данных за границу. В частности, персональные данные из стран ЕС/ЕЭЗ могут обрабатываться вне компаний концерна в третьей стране только в том случае, если получатель может доказать, что он обладает уровнем защиты данных, соответствующим настоящим Правилам. Подходящими инструментами могут быть:

- соглашение о стандартных договорных условиях ЕС,
- участие получателя в аккредитованной ЕС системе сертификации для обеспечения надлежащего уровня защиты данных или
- признание обязательных корпоративных правил получателя для создания адекватного уровня защиты данных ответственными надзорными органами.

Передача персональных данных какому-либо государственному органу допускается только в том случае, если она не являются массовой, несоразмерной или неизбирательной и в этом контексте не выходит за пределы того, что считается необходимым в демократическом обществе. В случае возникновения противоречий между этими требованиями и требованиями государственных органов Mercedes-Benz Group будет совместно с ответственной компанией концерна работать над поиском практического решения, отвечающего целям настоящих Правил (разделом 14.3).

Все обязательства, перечисленные в настоящем разделе 5, являются бенефициарными правами третьей стороны для субъекта данных.

6 Оценка воздействия на защиту данных

При внедрении новых процессов обработки или в случае значительных изменений в существующем процессе обработки, в частности за счет использования новых технологий, компании концерна должны оценить, представляет ли эта обработка высокий риск для конфиденциальности субъектов данных. При этом должны учитываться характер, объем, контекст и цель обработки данных. В рамках анализа рисков ответственное структурное подразделение проводит оценку воздействия планируемой обработки на защиту персональных данных (оценка воздействия на защиту данных). Если после проведения оценки воздействия на защиту данных и принятия соответствующих мер по снижению риска существует высокий риск для прав и свобод субъектов данных, необходимо проинформировать Уполномоченного концерна по вопросам защиты данных, чтобы он мог проконсультироваться с ответственным органом надзора за защитой данных. Необходимо соблюдать положения, установленные Mercedes-Benz Group для проведения оценки воздействия на защиту данных (например, программные инструменты, предписания по проведению оценки).

7 Документация процедур обработки данных

Каждая компания концерна обязана документировать процедуры обработки персональных данных в регистре обработки данных. Регистр обработки данных необходимо вести в письменной форме (в том числе в электронной) и по запросу предоставлять в надзорный орган по защите данных. Необходимо соблюдать положения, установленные Mercedes-Benz Group для ведения документации (например, программные инструменты, предписания по документации).

8 Обработка по поручению

8.1 Общее

При обработке по поручению подрядчик обрабатывает персональные данные как поставщик услуг от имени заказчика и в соответствии с его предписаниями. В этих случаях соглашение об обработке по поручению должно быть заключено как с внешними подрядчиками, так и между компаниями внутри Mercedes-Benz Group согласно соответствующим требованиям законодательства (например, в соответствии со стандартом «Соглашение об обработке по поручению»). При этом заказчик несет полную ответственность за правильное осуществление обработки данных.

Положения Раздела 8.3. распространяются также на внешних заказчиков, не являющихся компаниями концерна.

8.2 Положения для заказчиков

При размещении заказа должны соблюдаться следующие требования, выполнение которых обеспечивается структурным подразделением, размещающим заказ:

- Подрядчик выбирается на основании его пригодности для обеспечения требуемых технических и организационных защитных мер.
- Подлежат соблюдению предоставленные уполномоченным концерна по вопросам защиты данных стандарты составления договоров.
- Заказ должен быть выдан в письменной или электронной форме. При этом должны быть задокументированы указания по обработке данных и сферы ответственности заказчика и подрядчика.

Перед началом обработки данных заказчик в рамках соответствующей проверки должен убедиться в соблюдении подрядчиком перечисленных выше требований. Необходимо соблюдать соответствующие положения, установленные Mercedes-Benz Group (например, программные инструменты, предписания по проведению оценки, образцы договоров). Подрядчик может документально подтвердить свое соответствие требованиям защиты данных, в частности, представив соответствующую сертификацию. В зависимости от степени риска обработки данных необходимо регулярно повторять проверки в течение срока действия договора.

8.3 Положения для внутренних подрядчиков

Подрядчику разрешается обрабатывать персональные данные исключительно в рамках указаний заказчика.

Подрядчики могут привлекать другие компании концерна или третьи стороны («субподрядчиков») для обработки персональных данных в рамках их собственного (субподрядного) договора только с предварительного согласия заказчика. Данное согласие предоставляется только в том случае, если подрядчик возлагает на субподрядчика – договорным или иным сопоставимым юридически обязательным способом – те же обязательства по защите данных, которые возложены и на подрядчика в соответствии с настоящими Правилами по отношению к компании концерна и на субъектов данных. Он также должен обязать субподрядчика принять соответствующие технические и организационные меры по защите данных. Форма согласия, а также обязательства по предоставлению информации в случае изменения субподрядных отношений должны быть указаны в договоре на оказание услуг.

Подрядчики обязаны оказывать надлежащую поддержку заказчику в соблюдении действующих в отношении него положений о защите данных, в частности, предоставляя всю необходимую для доказательства информацию. Это касается, в частности, соблюдения:

- общих принципов обработки в соответствии с Разделом 5,
- прав субъектов данных в соответствии с Разделом 10,
- обязанность заказчика сообщать об инцидентах защиты данных в соответствии с Разделом 12,
- положений для заказчиков и подрядчиков в соответствии с Разделом 8,
- и порядка обработки запросов и расследований надзорными органами.

Если применимые стандарты или правовые нормы требуют, чтобы подрядчик осуществлял обработку вопреки предписаниям заказчика, или если эти нормы препятствуют выполнению подрядчиком своих обязательств, вытекающих из настоящих Правил или соглашения об обработке по поручению, то подрядчик должен немедленно уведомить об этом своего заказчика, за исключением случаев когда соответствующая правовая норма запрещает такое уведомление. Данное положение соответственно применяется в случае, если подрядчик не может выполнить предписания своего заказчика по другим причинам. В подобном случае заказчик имеет право приостановить передачу данных и/или расторгнуть соглашение об обработке по поручению.

Подрядчики обязаны уведомлять своих заказчиков о любых юридически обязывающих запросах со стороны государственных органов на раскрытие персональных данных, если это не запрещено по другим причинам.

По усмотрению заказчика подрядчик должен удалить или вернуть все предоставленные заказчиком персональные данные после завершения предоставления услуги.

Подрядчики обязаны незамедлительно информировать своего заказчика и (при наличии) клиента заказчика о любых заявленных претензиях, запросах или жалобах от субъектов данных.

Внутренние заказчики также должны обязать внешних подрядчиков соблюдать вышеуказанные положения.

Конкретные обязательства подрядчика перед заказчиком являются бенефициарными правами третьей стороны для субъекта данных.

9 Совместная ответственность

В случае, если несколько компаний концерна совместно определяют средства и цели обработки персональных данных(при наличии, с одной или несколькими третьими сторонами) (совместно ответственные инстанции/Joint Controller), эти компании должны заключить соглашение, в котором оговариваются их обязанности и сферы ответственности в отношении субъектов данных, чьи данные они обрабатывают. При этом должны соблюдаться типовые формы договоров, предоставленные Уполномоченным концерна по вопросам защиты данных.

10 Права, имеющие исковую силу для субъектов данных

Все перечисленные в настоящем Разделе 10 права субъектов данных и обязательства компаний концерна являются бенефициарными правами третьей стороны для субъекта данных.

На запросы и жалобы, поданные в соответствии с настоящим Разделом 10, необходимо ответить в течение одного месяца. Принимая во внимание сложность и количество заявок, этот период в один месяц может быть продлен максимум еще на два месяца, о чем соответствующим образом должен быть проинформирован субъект данных.

10.1 Права субъекта данных

Субъект данных в ЕС/ЕЭЗ имеет следующие права по отношению к ответственной компании концерна или – если компания концерна является подрядчиком – по отношению к заказчику, как это более подробно изложено в законодательстве ЕС:

- право на получение информации об обстоятельствах обработки его персональных данных. Необходимо соблюдать требования Уполномоченного концерна по вопросам защиты данных в отношении такой информации.
- Право на получение информации о том, как обрабатываются его данные и какими правами в этом отношении он обладает. Если в рамках трудовых отношений согласно нормам соответствующего трудового законодательства предусмотрены другие права на ознакомление с документами работодателя (например, с личным делом сотрудника), они сохраняют свою силу. По запросу субъект данных может получить копию своих персональных данных (возможно, за разумную плату), если это не запрещают заслуживающие защиты интересы третьих лиц.
- Право на исправление или дополнение персональных данных, если они неверны или неполны.
- Право на удаление своих данных, если он отзывает свое согласие или если отсутствует или перестало действовать правовое основание для обработки данных. Это относится и к тем случаям, если вследствие истечения срока или в силу других причин отпадает надобность в обработке данных. Должны учитываться действующие обязанности по хранению, а также препятствующие удалению достойные защиты интересы.
- Право на ограничение обработки данных, если субъект данных оспаривает их точность или если компания концерна больше не нуждается в данных, в то время как субъект данных нуждается в них для удовлетворения своих юридических претензий. Субъект данных может также потребовать, чтобы компания концерна ограничила обработку его данных, если в противном случае ей пришлось бы удалить данные или если она проверяет возражение со стороны субъекта данных.
- Право на получение касающихся субъекта данных персональных данных, которые он предоставил на основании согласия или в рамках договора, заключенного или инициированного с ним, в общеупотребительном цифровом формате. Он также имеет право передавать эти данные третьей стороне, если обработка осуществляется автоматизированным способом и это технически осуществимо.

- Право в любое время возражать против прямого маркетинга. Должна быть обеспечена адекватная система управления согласиями и возражениями.
- Право на возражение против обработки персональных данных, которые обрабатываются на правовом основании, исходя из преобладающих интересов компании концерна или третьей стороны, по причинам, связанным с его конкретной личной ситуацией. Однако это право на возражение не применяется, если компания концерна имеет веские основания для обработки или если данные обрабатываются в целях предъявления, осуществления или защиты юридических претензий. В случае юридически обоснованного возражения данные должны быть удалены.

Кроме того, субъект данных имеет право отстаивать свои права против компании концерна, импортирующей данные, в третьей стране.

10.2 Процедура рассмотрения жалоб

Субъекты данных имеют право на подачу жалобы Уполномоченному концерна по вопросам защиты данных, если они считают, что были нарушены положения настоящих Правил. Жалобы такого рода могут подаваться по электронной почте.

Находящаяся в ЕС/ЕЭЗ компания концерна, которая экспортирует данные, оказывает поддержку субъектам данных, чьи персональные данные были собраны в ЕС/ЕЭЗ, в установлении фактов и отстаивании их прав в соответствии с положениями настоящих Правил против компании концерна, импортирующей данные.

В случае, если субъект данных не согласен с решением компании концерна о соблюдении предписаний (или иным образом не удовлетворен их применением), он вправе оспорить это решение или поведение путем реализации своих прав. С этой целью он может обратиться в компетентный надзорный орган, в частности, в стране его обычного места пребывания, места работы или места предполагаемого нарушения, или подать иск в суд (Раздел 11.2). Дальнейшие юридические права и обязанности остаются незатронутыми.

11 Ответственность и место судопроизводства

11.1 Положения об ответственности

Находящаяся в ЕС/ЕЭЗ компания концерна («экспортер данных»), которая первоначально передала персональные данные компании концерна, находящейся в третьей стране, будет нести ответственность за каждое нарушение настоящих Правил компанией концерна из третьей страны, которая получает данные из ЕС/ЕЭЗ для их обработки в третьей стране. Данная ответственность включает в себя обязательство по устранению противоправных ситуаций, а также по возмещению материального и нематериального ущерба, причиненного в результате нарушения настоящих Правил компаниями концерна из третьих стран .

Экспортер данных частично или полностью освобождается от этой ответственности только в том случае, если он может доказать, что компания концерна из третьей страны, получившая данные из ЕС/ЕЭЗ, не несет ответственности за действия, приведшие к ущербу.

11.2 Место судопроизводства

Субъект данных может подать иск в суд по месту нахождения ответственной организации или подрядчика или по своему обычному месту пребывания.

Субъект данных, который заявляет о нарушении настоящих Правил в рамках обработки данных в третьей стране, может предъявить свои юридические претензии как к импортирующей, так и к экспортирующей данные компании в ЕС/ЕЭЗ. Таким образом, субъект данных может обратиться в компетентные суды и надзорные органы по месту нахождения ответственной инстанции или по своему обычному месту пребывания с жалобой на предполагаемое нарушение и вытекающими из этого юридическими претензиями.

Положения об ответственности и месте судопроизводства в этом Разделе являются бенефициарными правами третьей стороны для субъекта данных.

12 Сообщение об инцидентах защиты данных

В случае потенциального нарушения требований безопасности данных («инцидент защиты данных») соответствующие компании концерна исполняют обязательства по расследованию, предоставлению информации и снижению ущерба. Инцидент защиты данных является нарушением защиты персональных данных, если имеет место нарушение безопасности данных, которое ведет к незаконному уничтожению, изменению, несанкционированному раскрытию или использованию персональных данных. В случае, если это может привести к возникновению риска для прав и свобод физических лиц, о соответствующих событиях необходимо сообщить в компетентный надзорный орган, по возможности в течение 72 часов с момента, когда компании концерна стало известно о нарушении. Кроме того, субъекты данных должны быть уведомлены о любом нарушении защиты персональных данных, которое может привести к высокому риску для их прав и свобод. Подрядчики, как определено в Разделе 8.2, обязаны немедленно сообщать своему заказчику об инцидентах защиты данных.

Если в сфере ответственности компании концерна установлен или предполагается инцидент защиты данных, все сотрудники обязаны немедленно сообщить об этом в рамках Процесса менеджмента инцидентов информационной безопасности (Information Security Incident Management Process). Необходимо соблюдать соответствующие положения, установленные Mercedes-Benz Group (например, программные инструменты, предписания по уведомлению).

Любое нарушение защиты данных должно быть задокументировано, и документация должна быть предоставлена надзорному органу по запросу.

13 Организация защиты данных и санкции

13.1 Ответственность

Члены органов управления компаний концерна несут ответственность за обработку данных в своей сфере ответственности. Поэтому они должны обеспечить соблюдение требований законодательства, а также требований, содержащихся в настоящих Правилах защиты данных (ЕС), в отношении защиты данных (например, предписанные нормами национального законодательства обязанности уведомления). В рамках своей сферы ответственности руководство несет ответственность за обеспечение принятия организационных, кадровых и технических мер для надлежащей обработки данных в соответствии с требованиями защиты данных. Ответственность за соблюдение этих предписаний лежит на соответствующих сотрудниках. О проверках мер по защите данных, проводимых надзорными органами, необходимо незамедлительно сообщать уполномоченному концерна по вопросам защиты данных.

13.2 Повышение осведомленности и обучение

Руководители должны обеспечить, чтобы их сотрудники получали и проходили необходимое обучение по вопросам защиты данных (включая содержание настоящих Правил и обращение с ними), если они имеют постоянный или регулярный доступ к персональным данным, участвуют в сборе данных или в разработке инструментов для обработки персональных данных. Должны соблюдаться требования Уполномоченного концерна по вопросам защиты данных и Подразделения нормативно-правового соответствия данных (Data Compliance).

13.3 Организация

Уполномоченный концерна по вопросам защиты данных не зависит от внутренних указаний, касающихся выполнения возложенных на него задач. Он должен обеспечивать соблюдение национальных и международных положений о защите данных. Он отвечает за настоящие Правила и следит за их соблюдением. Если компании концерна намерены принять участие в международной системе сертификации обязательных корпоративных правил по защите данных, они должны согласовать это участие с Уполномоченным концерна по вопросам защиты данных.

Правление Mercedes-Benz Group назначает Уполномоченного концерна по вопросам защиты данных и предоставляет ему поддержку в выполнении его обязанностей. Как правило, компании концерна, которые по закону обязаны назначить ответственного за защиту данных сотрудника, назначают Уполномоченного концерна по вопросам защиты данных. Уполномоченный концерна по вопросам защиты данных отчитывается непосредственно перед Правлением Mercedes-Benz Group и соответствующим руководством всех компаний концерна, для которых был назначен Уполномоченный концерна по вопросам защиты данных. Индивидуальные исключения подлежат согласованию с уполномоченным концерна по вопросам защиты данных.

В рамках существующих обязательств по отчетности Наблюдательный совет Mercedes-Benz Group должен быть проинформирован о годовом отчете Уполномоченного концерна по вопросам защиты данных.

Все субъекты данных могут в любое время связаться с Уполномоченным концерна по вопросам защиты данных, чтобы выразить свою обеспокоенность, задать вопросы, запросить информацию или подать жалобу в отношении защиты или безопасности данных. По запросу вопросы и жалобы рассматриваются конфиденциально.

Контактные данные Уполномоченного концерна по вопросам защиты данных:

Mercedes-Benz Group AG, Уполномоченный концерна по вопросам защиты данных, HPC E600,
70546 Штутгарт, Германия
Адрес электронной почты: data.protection@mercedes-benz.com
Интранет: https://social.intra.corpintra.net/docs/DOC-71499

Концерном Mercedes-Benz Group также создана организация корпоративного регулирования, которая более подробно описана в отдельных внутренних регламентах. Организация корпоративного регулирования поддерживает и контролирует компании концерна в отношении соблюдения предписаний по защите данных. Она определяет содержание тренингов по защите данных и критерии для участников.

13.4 Санкции

Незаконная обработка персональных данных или другие нарушения законов о защите данных могут преследоваться в соответствии с регулятивным и уголовным правом во многих странах, а также привести к искам о компенсации ущерба. Нарушения, за которые несут ответственность отдельные сотрудники, могут повлечь за собой дисциплинарные взыскания в соответствии с трудовым законодательством. Нарушения настоящих Правил влекут за собой наказание в соответствии с внутренними регламентами.

13.5 Аудит и контроль

Соблюдение положений настоящих Правил и действующего законодательства о защите данных регулярно контролируется на уровне концерна не реже одного раза в год, в зависимости от степени риска. Это делается посредством внутренней оценки рисков нормативно-правового соответствия, аудитов, включая конкретные вопросы защиты данных, и других проверок. Уполномоченный концерна по вопросам защиты данных имеет право потребовать дополнительных проверок. Результаты этих проверок должны быть доведены до сведения Уполномоченного концерна по вопросам защиты данных, ответственной компании концерна и ее ответственного за защиту данных сотрудника, если таковой был назначен.

В рамках существующих обязательств по отчетности о результатах проверок должно быть проинформировано Правление Mercedes-Benz Group. По запросу результаты проверок предоставляются компетентному органу надзора за защитой данных. Компетентный орган по надзору за защитой данных может в рамках предоставленных ему государственным законодательством полномочий подвергнуть каждую компанию концерна аудиторской проверке защиты данных на предмет соблюдения предписаний настоящих Правил.

14 Поправки к настоящим Правилам и сотрудничество с органами власти

14.1 Ответственность в случае внесения поправок

Изменение настоящих Правил возможно при согласовании с Уполномоченным концерна по вопросам защиты данных в соответствии с установленным порядком внесения поправок в Правила (Руководство по менеджменту правил, A 1). Поправки, которые оказывают существенное влияние на настоящие Правила защиты данных (ЕС), A 17 или которые могут повлиять на уровень предоставляемой Правилами защиты (т. е. изменения в отношении обязательного характера), должны незамедлительно доводиться до сведения компетентных органов по надзору за защитой данных, которые утверждают настоящие Правила в качестве обязывающих корпоративных правил.

Уполномоченный концерна по вопросам защиты данных несет ответственность за ведение актуального списка всех компаний концерна, на которые распространяется действие настоящих Правил (параллельно действующий регламент «Список компаний концерна, связанных Правилами защиты данных (ЕС)»). На основании настоящих Правил передача персональных данных новой компании концерна не производится до тех пор, пока новая компания концерна не будет эффективно связана настоящими Правилами и не примет соответствующие меры корпоративного регулирования по соблюдению Правил.

Субъект данных имеет право на легкий доступ к настоящим Правилам. Поэтому последняя редакция настоящих Правил доступна в на веб-сайте https://www.group.mercedes-benz.com в разделе «Защита данных». Это требование является бенефициарным правом третьей стороны для субъекта данных.

В случае внесения поправок в настоящие Правила или в список аффилированных компаний концерна, надзорный орган головного офиса Mercedes-Benz Group извещается об этом раз в год Уполномоченным концерна по вопросам защиты данных с обязательным кратким изложением причин обновления.

14.2 Сотрудничество с органами власти

Компании концерна, которые осуществляют обработку или участвуют в обработке данных в третьих странах, обязаны сотрудничать с компетентными надзорными органами в вопросах, касающихся проблем, запросов или других процедур, связанных с обработкой персональных данных в вышеупомянутом контексте. Такое сотрудничество включает в себя обязательство принимать законные аудиторские проверки со стороны надзорных органов. Кроме того, должны соблюдаться все законные указания компетентных надзорных органов на основе процедур обработки в третьих странах или положений настоящих Правил.

Положения Раздела 14.2 о сотрудничестве с органами власти являются бенефициарными правами третьей стороны для субъекта данных.

14.3 Мониторинг и отчетность о регламентах третьих стран

Ответственные лица в компаниях третьих стран должны незамедлительно проинформировать Уполномоченного по вопросам защиты данных, если их компания имеет оправданные основания полагать, что законы или другие нормативные акты, принятые страной или учреждением, отличным от ЕС и его государств-членов, представляют собой следующие риски:

- законы или нормативные акты препятствуют выполнению соответствующими компаниями третьих стран или другими компаниями концерна их вытекающих из настоящих Правил обязательств при обработке данных в третьих странах, или
- законы или нормативные акты могут оказать серьезное негативное воздействие на права субъектов данных, предоставляемые настоящими Правилами для обработки в третьих странах. В особенности, если местные органы власти требуют массовой, несоразмерной и неизбирательной передачи персональных данных, выходящей за рамки того, что считается необходимым в демократическом обществе.

Уполномоченный концерна по вопросам защиты данных оценивает последствия и уведомляет компетентный надзорный орган по защите данных (при наличии такового), если ожидается, что соответствующее юридическое требование в значительной степени повлияет на гарантии, предусмотренные настоящими Правилами. Это положение является бенефициарным правом третьей стороны для субъекта данных.

Если орган власти требует, чтобы компания в третьей стране воздержалась от раскрытия персональных данных надзорному органу по защите данных, эта компания должна принять все надлежащие меры для максимального смягчения этого запрета или его отмены, а также в рамках свободы действий в предусмотренных пределах ежегодно предоставлять надзорному органу по защите данных общую информацию о полученных запросах (например, количество заявок на раскрытие, тип запрашиваемых данных, по возможности, запрашивающая сторона).

Mercedes-Benz Group AG, Mercedesstraße 120, 70327 Stuttgart, Germany, www.group.mercedes-benz.com