

DAIMLER

Правила защиты данных

Вступление

Уважаемые дамы и господа!


В эпоху цифровых технологий мы предоставляем нашим клиентам возможность быть «всегда в сети», даже находясь в своем автомобиле. Обязательной предпосылкой тому является обеспечение сбора и обработки данных. При этом неважно, будь то в автомобиле, в процессе техобслуживания или при покупке автомобиля – для нас всегда действует главный принцип: там, где осуществляется сохранение и передача данных, должен обеспечиваться высокий уровень защиты и безопасности этих данных. Это касается данных наших клиентов, потенциальных покупателей и деловых партнеров в той же степени, как и данных наших сотрудников. Ведь защита данных – это защита личности.

Мы стремимся к тому, чтобы имя «Даймлер» ассоциировалось не только с надежными автомобилями, но и подразумевало определение стандартов для защиты данных. Поэтому, будучи глобально оперирующим предприятием, мы считаем своим долгом соответствовать различным законодательным требованиям во всем мире, которые связаны со сбором и обработкой персональных данных. Наивысший приоритет для нас имеет обеспечение единых и глобально применимых стандартов по обращению с персональными данными. Так как соблюдение прав личности и приватной сферы каждого отдельного индивидуума в нашем понимании лежит в основе доверительных деловых отношений.

В наших общекорпоративных правилах защиты данных мы определили строгие требования, предъявляемые к обработке персональных данных клиентов, потенциальных покупателей, деловых партнеров и сотрудников. Эти правила соответствуют требованиям Общеввропейских правил защиты данных и обеспечивают соблюдение принципов действующих во всем мире национальных и международных законодательных актов по защите данных. Тем самым мы устанавливаем глобально применимые стандарты по защите и безопасности данных на нашем предприятии и регламентируем обмен данными между компаниями нашего концерна. В качестве критериев мы определили семь основных принципов защиты данных, среди которых такие, как прозрачность, минимизация данных и безопасность данных.

Наши руководители и сотрудники обязаны соблюдать настоящие общекорпоративные правила защиты данных и соответствующие законодательные акты по защите данных. Выполняя обязанности уполномоченного концерна по вопросам защиты данных, я отвечаю за соблюдение во всем мире законодательных регламентов и принципов защиты данных на всех предприятиях «Даймлер».

В качестве контактных лиц мы с нашими сотрудниками будем рады ответить на Ваши вопросы по защите и безопасности данных в концерне «Даймлер».



Д-р Йоахим Рис
Уполномоченный концерна по вопросам защиты данных

Содержание

I.	Цель правил защиты данных	4
II.	Область действия и изменение правил	4
III.	Действие законодательства	5
IV.	Принципы обработки персональных данных	5
1.	Добросовестность и правомерность	5
2.	Предназначение	5
3.	Транспарентность	5
4.	Принципы избегания сбора данных и минимизации данных	6
5.	Удаление данных	6
6.	Объективная достоверность и актуальность данных	6
7.	Конфиденциальность и безопасность данных	6
V.	Допустимость обработки данных	6
1.	Данные клиентов и деловых партнеров	7
1.1	Обработка данных в рамках договорных взаимоотношений	7
1.2	Обработка данных в рекламных целях	7
1.3	Согласие на обработку данных	7
1.4	Обработка данных на основе законного разрешения	7
1.5	Обработка данных на основе правомерного интереса	8
1.6	Обработка данных, достойных защиты в особой мере	8
1.7	Автоматизированное принятие индивидуальных решений	8
1.8	Данные пользователей и Интернет	8
2.	Данные сотрудников	9
2.1	Обработка данных в рамках трудовых отношений	9
2.2	Обработка данных на основе законного разрешения	9
2.3	Коллективные регламенты по обработке данных	9
2.4	Согласие на обработку данных	9
2.5	Обработка данных на основе правомерного интереса	10
2.6	Обработка данных, достойных защиты в особой мере	10
2.7	Автоматизированное принятие индивидуальных решений	10
2.8	Телекоммуникация и Интернет	11
VI.	Передача персональных данных	11
VII.	Обработка данных по поручению	12
VIII.	Права затронутого лица	13
IX.	Конфиденциальность обработки	14
X.	Безопасность обработки	14
XI.	Проверка мер по защите данных	14
XII.	Нарушения требований по защите данных	15
XIII.	Ответственность и санкции	15
XIV.	Уполномоченный концерна по вопросам защиты данных	16
XV.	Определения	16

I. Цель правил защиты данных

Концерн «Даймлер» обязуется в рамках своей социальной ответственности соблюдать законы о защите данных глобально. Настоящие правила защиты данных действуют для всех предприятий концерна «Даймлер» во всем мире и основываются на признанных основных принципах защиты данных. Соблюдение норм защиты данных лежит в основе доверительных деловых отношений и репутации концерна «Даймлер» как привлекательного работодателя.

Правила защиты данных являются также предпосылкой для создания одного из необходимых рамочных условий для глобального обмена данными¹ между компаниями концерна. Они обеспечивают требуемый Общеввропейскими правилами защиты данных², а также национальными законодательными актами, адекватный уровень защиты данных для трансграничного обмена данными, в том числе и с теми странами, в которых до сих пор не существует адекватного уровня их защиты³.

II. Область действия и изменение правил

Настоящие правила защиты данных действуют в отношении всех предприятий концерна «Даймлер», т. е. в отношении «Даймлер АГ» и всех зависимых от концерна компаний, а также аффилированных предприятий и их сотрудников. Зависимыми в настоящем смысле считаются компании, в которых «Даймлер АГ» непосредственно или косвенно, на основе обладания большинством голосов, большинства в управлении предприятия или на основе соглашения, вправе требовать принятия настоящих правил защиты данных. Правила защиты данных распространяются на все процедуры обработки персональных данных⁴. В странах, в которых данные юридических лиц защищаются в равной мере с персональными данными, настоящие правила защиты данных действуют в той же степени и для данных юридических лиц. На анонимизированные данные⁵, напр., статистические оценки или исследования, настоящие правила защиты данных не распространяются.

Отдельные компании концерна не вправе принимать регламенты, отклоняющиеся от настоящих правил защиты данных. Дальнейшие правила защиты данных могут быть разработаны при согласовании с уполномоченным концерном по вопросам защиты данных при условии, если это требуется соответствующим национальным законодательством. Изменение настоящих правил предпринимается при согласовании с уполномоченным концерном по вопросам защиты данных в рамках принятой для изменения правил процедуры. Предприятия концерна «Даймлер» незамедлительно оповещаются о предпринятых изменениях в рамках принятой для изменения правил процедуры. Об изменениях, в существенной мере влияющих на обеспечение соблюдения правил защиты данных, необходимо ежегодно докладывать в инстанции по защите данных, которые утверждают настоящие правила защиты данных в качестве обязательных к исполнению внутрикорпоративных регламентов.

Доступ к последней актуальной версии правил защиты данных предоставляется на интернет-сайте «Даймлер АГ» www.daimler.com в разделе указаний по защите данных.

¹ См. XV.

² Директива RL 95/46/EG Европейского парламента и Совета по защите физических лиц при обработке персональных данных и по свободному потоку обмена данными; опубликована на: http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie.

³ См. XV.

⁴ См. XV.

⁵ См. XV.

III. Действие законодательства

Настоящие правила защиты данных включают в себя всемирно признанные принципы защиты данных без замены ими положений действующего законодательства. Они дополняют соответствующее национальное законодательство в сфере защиты данных. Соответствующее законодательство имеет приоритетное значение в случаях, если оно требует отклонений от настоящих правил защиты данных или предъявляет требования, которые выходят за их рамки. Содержащиеся в настоящих правилах защиты данных положения подлежат соблюдению также и при отсутствии соответствующих законодательных актов. Подлежат соблюдению требования национального законодательства об отчетности и обязанности предоставлять заявления.

Каждое предприятие концерна «Даймлер» несет ответственность за соблюдение настоящих правил защиты данных и правовых обязательств. При возникновении подозрений в отношении того, что правовые обязательства противоречат обязанностям, вытекающим из настоящих правил защиты данных, затронутое предприятие концерна должно незамедлительно оповестить об этом уполномоченного концерна по вопросам защиты данных. В случае столкновения предписаний национального законодательства и положений настоящих правил «Даймлер АГ» будет совместно с затронутым предприятием концерна искать действующее на практике решение, которое бы соответствовало целям настоящих правил защиты данных.

IV. Принципы обработки персональных данных

1. Добросовестность и правомерность

При обработке персональных данных должны соблюдаться личные права затронутого лица⁶. Сбор и обработка персональных данных должна производиться добросовестно и правомерным образом.

2. Предназначение

Обработка персональных данных должна преследовать исключительно те цели, которые были определены перед началом сбора данных. Последующие изменения целей возможны только в ограниченной мере и подлежат обоснованию.

3. Транспарентность

Затронутое лицо должно извещаться об обработке его данных. Сбор персональных данных принципиально производится через само затронутое лицо. При сборе данных затронутому лицу должны быть понятны нижеперечисленные аспекты, или оно должно быть соответствующим образом проинформировано о них:

- » кто является ответственной инстанцией,⁷
- » каковы цели обработки данных,
- » третьи лица⁸ или категории третьих лиц, которым, при необходимости, будут переданы данные.

⁶ См. XV.

⁷ См. XV.

⁸ См. XV.

4. Принципы избегания сбора данных и минимизации данных

До обработки персональных данных должна быть проверена необходимость ее проведения и объем, в котором необходимо ее провести, для достижения целей, преследуемых подобной обработкой. Если это возможно для достижения целей и затраты соразмерны преследуемым целям, то следует использовать анонимизированные или статистические данные.

Персональные данные нельзя сохранять про запас для потенциальных будущих целей, если это только не предусмотрено или не разрешено законодательством.

5. Удаление данных

Персональные данные, необходимость в которых исчезает после истечения предусмотренных законодательством или бизнес-процессами сроков хранения,⁹ должны быть удалены. В отдельных случаях, если имеются основания предположить наличие достойных защиты интересов или если данные имеют историческую ценность, данные подлежат дальнейшему хранению до тех пор, пока не будет юридически обоснован достойный защиты интерес или пока архивной службой концерна не будет произведена оценка целесообразности архивирования содержания данных в исторических целях.

6. Объективная достоверность и актуальность данных

Персональные данные должны храниться в файлах в корректном, полном и – насколько это необходимо – актуализированном состоянии. Должны быть приняты адекватные меры для обеспечения удаления, исправления, дополнения или актуализации несоответствующих, неполных или устаревших данных.

7. Конфиденциальность и безопасность данных

В отношении персональных данных действует принцип соблюдения конфиденциальности данных. При личном обращении данные должны обрабатываться конфиденциально и должны быть защищены техническими и организационными мерами от несанкционированного доступа, неправомерной обработки или передачи, а также от утери, изменения или уничтожения по неосторожности.

V. Допустимость обработки данных

Сбор, обработка и использование персональных данных допускаются только при наличии одного из нижеперечисленных юридических оснований. Наличие такого юридического основания для обработки данных необходимо также и в том случае, если должна быть изменена первоначально установленная цель для сбора, обработки и использования персональных данных.

⁹ См. XV.

1. Данные клиентов и деловых партнеров

1.1 Обработка данных в рамках договорных взаимоотношений

Персональные данные затронутого заинтересованного лица, клиента или делового партнера могут подвергаться обработке в рамках обоснования заключения, осуществления и окончания срока действия договора. Сюда включены также консультационные услуги партнеру по договору, насколько это связано с преследуемыми договором целями.

В преддверии заключения договора, т. е. в фазе подготовки договора, разрешается обработка персональных данных с целью составления предложения, подготовки заявки на покупку или исполнения иных связанных с заключением договора пожеланий заинтересованного лица. Во время подготовки договора разрешается установление контакта с заинтересованными лицами, используя предоставленные ими данные. Необходимо соблюдать возможные ограничения, высказанные заинтересованным лицом. При проведении выходящих за рамки данного положения рекламных мероприятий должны соблюдаться следующие требования, изложенные в положении V.1.2.

1.2 Обработка данных в рекламных целях

В случае, если затронутое лицо с целью получения информации обращается в одну из компаний концерна «Даймлер» (например, с просьбой о доставке информационного материала о продукте), то обработка данных для выполнения данной просьбы допустима.

Меры по укреплению связей с клиентами и рекламные мероприятия требуют дальнейших правовых предпосылок. Обработка персональных данных в рекламных целях или в целях изучения рынка и общественного мнения допустима, если это совместимо с целью, ради которой изначально предпринимался сбор данных. Затронутое лицо должно быть извещено об использовании его данных в рекламных целях. Если данные собираются исключительно в рекламных целях, то их указание затронутым лицом производится на добровольной основе. Затронутое лицо должно быть проинформировано о добровольном порядке указания своих данных для этих целей. В рамках коммуникации с затронутым лицом следует получить согласие¹⁰ затронутого лица на обработку его данных в рекламных целях. В рамках получения согласия от затронутого лица ему должна быть предоставлена возможность выбора между имеющимися в распоряжении контактными каналами, например, почтой, электронной почтой и телефоном («Согласие» – см. V.1.3).

Если затронутое лицо возражает против использования его данных в рекламных целях, то дальнейшее использование его данных в этих целях недопустимо и данные должны быть заблокированы для этих целей. Необходимо соблюдать выходящие за рамки данного положения ограничения, которые действуют в некоторых странах в отношении использования данных в рекламных целях.

1.3 Согласие на обработку данных

Обработка данных может производиться на основе согласия затронутого лица. Перед получением согласия от затронутого лица оно должно быть проинформировано в соответствии с положением IV.3. настоящих правил защиты данных. 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 документировано.

1.4 Обработка данных на основе законного разрешения

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.

¹⁰ См. XV.

1.5 Обработка данных на основе правомерного интереса

Обработка персональных данных может также производиться, если это необходимо для осуществления правомерного интереса концерна «Даймлер». Правомерные интересы, как правило, носят правовой характер (например, реализация непогашенной задолженности) или же экономический характер (например, предотвращение нарушения условий договора). Проведение обработки персональных данных на основе правомерного интереса не допускается, если в индивидуальном случае имеются основания предположить, что достойные защиты интересы затронутого лица преобладают по сравнению с интересом, связанным с обработкой данных. Достойные защиты интересы подлежат проверке при любой обработке.

1.6 Обработка данных, требующих повышенной степени защиты

Обработка персональных данных, достойных защиты в особой мере,¹¹ допускается только при условии, если это требуется законодательством или же при наличии явного согласия затронутого лица. Обработка таких данных допускается также в тех случаях, если она в обязательном порядке необходима для предъявления, реализации или защиты претензий, предъявляемых по отношению к затронутому лицу. При планировании обработки данных, требующих повышенной степени защиты, необходимо предварительное уведомление об этом уполномоченного концерна по вопросам защиты данных.

1.7 Автоматизированное принятие индивидуальных решений

Автоматизированная обработка персональных данных, в результате которой оцениваются индивидуальные признаки личности (например, кредитоспособность), не может служить исключительным основанием для принятия решений, которые приведут к негативным последствиям для затронутого лица или нанесению ему ощутимого вреда. Затронутое лицо должно быть извещено о факте и результате автоматизированно принятого индивидуального решения, и ему должна быть предоставлена возможность выразить свое мнение. Во избежание принятия ошибочных решений должно быть обеспечено проведение контроля и проверки достоверности со стороны одного из сотрудников.

1.8 Данные пользователей и Интернет

При сборе, обработке и использовании персональных данных на веб-сайтах или в приложениях затронутые лица должны уведомляться об этом в виде оговорок о защите данных, в случае необходимости, в виде информации о куки-файлах. Указания о защите данных и, при необходимости, куки-файлы с указаниями должны быть интегрированы таким образом, чтобы они могли быть легко распознаваемы и непосредственно доступны для затронутых лиц и постоянно находиться в их распоряжении.

Если для оценки поведения пользователей веб-сайтов и приложений создаются профили пользователей (трекинг), то затронутые лица должны быть в любом случае проинформированы об этом в положениях по защите данных. Персональный трекинг разрешается проводить только в том случае, если это допускается национальным законодательством или с согласия затронутого лица. Если трекинг осуществляется под псевдонимом, то в положениях по защите данных затронутому лицу должна быть предоставлена возможность отказаться от этого (Opt-out).

Если в подлежащих обязательной регистрации разделах веб-сайтов или приложений предоставляется возможность доступа к персональным данным, то идентификация и аутентификация затронутых лиц должна осуществляться таким образом, чтобы обеспечить достижение надлежащего уровня защиты для соответствующего доступа.

¹¹ См. XV.

2. Данные сотрудников

2.1 Обработка данных в рамках трудовых отношений

В рамках трудовых отношений могут подвергаться обработке персональные данные, необходимые для обоснования заключения, осуществления и прекращения трудового договора. При установлении трудовых отношений разрешается обработка персональных данных кандидатов на вакантные 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 необходимо также и для использования данных для дальнейших процедур по подаче заявления на вакантную должность или перед их передачей в другие компании концерна.

В рамках действующих трудовых отношений обработка данных должна всегда соотноситься с целью трудового договора, если не вступает в силу одна из приведенных ниже причин для разрешения обработки данных.

Если в рамках установления трудовых отношений или действующих трудовых отношений необходим сбор дальнейшей информации о кандидате у третьих лиц, то подлежат соблюдению соответствующие требования национального законодательства. В случае сомнений необходимо получить согласие затронутого лица.

Для обработки данных сотрудника, относящихся к трудовым отношениям, но первично не служащих осуществлению трудового договора, соответственно необходимо наличие правовой легитимации. Таковая может иметь форму требований законодательства, коллективных регламентов по обработке данных, принятых с представительствами рабочих и служащих, согласия сотрудника или правомерных интересов предприятия.

2.2 Обработка данных на основе законного разрешения

Обработка персональных данных сотрудника допускается также и в том 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. Если законодательством предусматривается свобода действия, то должны учитываться достойные защиты интересы сотрудника.

2.3 Коллективные регламенты по обработке данных

В случае выхода обработки данных за рамки предназначения осуществления договора, она остается допустимой при условии, если она разрешена коллективными регламентами. Коллективными регламентами считаются тарифные договоры или соглашения между работодателем и представительством рабочих и служащих в рамках возможностей соответствующего трудового права. Регламенты должны распространяться на конкретные цели требуемой обработки и оформляются в рамках законодательства по защите данных.

2.4 Согласие на обработку данных

Обработка данных сотрудника может производиться на основе согласия затронутого сотрудника. Подача заявлений о согласии осуществляется в добровольном порядке. 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. При предварительно проинформированном добровольном указании данных затронутым лицом согласие может быть принято при условии, что национальным законодательством не предписана обязательность явного согласия. Перед получением согласия от затронутого лица оно должно быть проинформировано в соответствии с положением IV.3. настоящих правил защиты данных.

2.5 Обработка данных на основе правомерного интереса

Обработка персональных данных сотрудника может также производиться, если это необходимо для осуществления правомерного интереса концерна «Даймлер». Правомерные интересы, как правило, носят правовой характер (например, предъявление, осуществление или защита правовых претензий) или же экономический характер (например, оценка предприятия).

Проведение обработки персональных данных на основе правомерного интереса не допускается, если в индивидуальном случае имеются основания предположить, что достойные защиты интересы сотрудника преобладают по сравнению с интересом, связанным с обработкой данных. Наличие достойных защиты интересов подлежит проверке при любой обработке данных.

Контрольные меры, требующие обработки данных сотрудников, разрешается принимать только в случае наличия законодательного требования или обоснованного повода. В том числе и при наличии обоснованного повода необходимо проверять соразмерность контрольных мер. Правомерные интересы компании при проведении контрольных мер (например, соблюдение правовых положений и внутрикорпоративных правил) должны быть взвешены с учетом, насколько это допустимо, возможности отказаться от принятия таких мер при наличии требующих повышенной степени защиты интересов затронутого сотрудника. Проведение контрольных мер при этом допускается только при условии их адекватности. Правомерный интерес предприятия и возможные достойные защиты интересы сотрудников должны быть определены и документированы перед принятием любой меры. Кроме того, при необходимости, должны учитываться возникающие на основании законодательства дальнейшие требования (например, право участия в принятии решения представительств рабочих и служащих, а также право затронутых лиц на получение информации).

2.6 Обработка данных, требующих повышенной степени защиты

Персональные данные, требующие повышенной степени защиты, разрешается обрабатывать лишь при наличии определенных предпосылок. Требуемыми повышенной степени защиты, являются данные о расовой и этнической принадлежности, о политических мнениях, о религиозных или философских убеждениях, о принадлежности к профсоюзам, а также о здоровье или половой жизни затронутого лица. На основе положений законодательства к данным, требующим повышенной степени защиты, могут быть отнесены иные категории данных или же категории данных могут иметь отличающееся содержание. Часто также и данные, касающиеся уголовно наказуемых деяний, разрешается обрабатывать только при наличии особых, определенных законодательством предпосылок.

Обработка должна быть явно разрешена или предписана законодательством. Дополнительно обработка может быть разрешена, если она необходима для обеспечения ответственной инстанции возможности соблюдения прав и обязанностей в области трудового права. Сотрудник также может добровольно дать свое явное согласие на проведение обработки.

При планировании обработки данных, требующих повышенной степени защиты, необходимо предварительное уведомление об этом уполномоченного концерна по вопросам защиты данных.

2.7 Автоматизированное принятие индивидуальных решений

Проводимая в рамках трудовых отношений автоматизированная обработка персональных данных, в результате которой оцениваются индивидуальные признаки личности (например, при отборе персонала или оценке профилей способностей) не может служить исключительным основанием для принятия решений, которые приведут к негативным последствиям для затронутого сотрудника или нанесению ему ощутимого вреда. Во избежание принятия ошибочных решений в автоматизированном процессе должно быть обеспечено проведение оценки содержания обстоятельств дела физическим лицом. Результаты такой оценки должны лечь в основу принимаемого решения. Кроме того, затронутый сотрудник должен быть извещен о факте и результате автоматизированно принятого индивидуально-го решения, и ему должна быть предоставлена возможность высказывания своего мнения.

2.8 Телекоммуникация и Интернет

Телефонное оборудование, адреса электронной почты, Интранет и Интернет, а также внутренние социальные сети предоставляются предприятием в первую очередь для решения рабочих задач. Они являются средствами труда и ресурсами предприятия. Разрешается их использование в рамках соответствующих действующих правовых предписаний и внутрикорпоративных правил. В случае разрешения пользования в личных целях необходимо соблюдение конфиденциальности данных связи и соответствующих действующих национальных законодательных норм по телекоммуникации, насколько они применимы.

Принципиальный контроль телефонной и электронной коммуникации, а также пользования Интранетом и Интернетом не осуществляется. В целях защиты от атак на ИТ-инфраструктуру или на отдельных пользователей могут быть внедрены защитные меры на входах в сеть «Даймлер», блокирующие проникновение контента, который может нанести ущерб, или анализирующие профиль атак. Из соображений безопасности пользование телефонным оборудованием, адресами электронной почты, Интранетом и Интернетом, а также внутренними социальными сетями может временно протоколироваться. Анализ персональных данных в этой связи допускается только при конкретном обоснованном подозрении в нарушении законов или корпоративных правил концерна «Даймлер». Такие проверки разрешается проводить исключительно уполномоченным на проведение расследований подразделениям при соблюдении принципа соразмерности. Соответствующие национальные законы подлежат соблюдению в той же мере, что и действующие в данной сфере регламенты концерна.

VI. Передача персональных данных

Для осуществления передачи персональных данных получателю вне концерна «Даймлер» или получателю внутри концерна «Даймлер» необходимо выполнение условий, обеспечивающих допустимость обработки персональных данных, которые изложены в главе V. Получатель данных должен дать обязательство об использовании этих данных исключительно в заранее определенных целях.

В случае передачи данных получателю, не входящему в состав концерна «Даймлер» и находящемуся в третьем государстве¹², он обязан обеспечить уровень защиты данных, адекватный настоящим правилам защиты данных. Данное положение не действует, если передача данных осуществляется на основе законных обязательств. Подобное законное обязательство может вытекать из законодательства страны местонахождения компании концерна, осуществляющей передачу данных, или если законодательство такой страны признает законной преследуемую цель передачи данных.

В случае передачи данных третьими лицами предприятиям, входящим в состав концерна «Даймлер», необходимо удостовериться в том, что эти данные разрешается использовать в предусмотренных целях.

При передаче персональных данных одной компанией концерна с местонахождением в Европейском экономическом пространстве другой компании концерна с местонахождением вне Европейского экономического пространства¹³ (в третьем государстве) импортирующая данные компания обязана при всех запросах компетентного надзорного органа, в чьем ведомстве находится экспортирующая данные компания, кооперировать с ним и соблюдать все регламенты, установленные этим надзорным органом в отношении обработки передаваемых данных. То же самое действует и в отношении передачи данных, осуществляемой компаниями концерна из других государств. Если они принимают участие в международной системе сертификации для обязательных корпоративных регламентов по защите данных,

¹² См. XV.

¹³ См. XV.

они должны обеспечить сотрудничество с соответствующими аудиторскими агентствами и ведомствами. Участие в подобного рода системах сертификации должно быть согласовано с уполномоченным концерна по вопросам защиты данных.

Если затронутое лицо утверждает о нарушении настоящих правил защиты данных импортирующей его данные компанией концерна с местонахождением в третьем государстве, то экспортирующая данные компания концерна с местонахождением в Европейском экономическом пространстве обязуется, оказывать поддержку заинтересованному лицу, сбор данных которого осуществляется в Европейском экономическом пространстве в выяснении обстоятельств дела, так и при обеспечении осуществления его прав согласно положениям настоящих правил защиты данных по отношению к импортирующей данные компании концерна. Кроме того, затронутое лицо вправе воспользоваться своими правами также и в отношении экспортирующей данные компании концерна. При утверждении о нарушении экспортирующая данные компания обязана предъявить в отношении затронутого лица подтверждение того, что находящейся в третьем государстве импортирующей данные компании не вменяется в вину нарушение настоящих правил защиты данных при дальнейшей обработке полученных данных.

В случае передачи персональных данных компанией концерна с местонахождением в Европейском экономическом пространстве компании концерна с местонахождением в третьем государстве осуществляющий передачу данных оператор привлекается к ответственности в соответствии с настоящим положением за нарушение, совершенное компанией группы, находящейся в третьем государстве в отношении заинтересованного лица, чьи данные были собраны в Европейском экономическом пространстве. Местом подсудности является соответствующий суд по месту нахождения экспортирующей данные инстанции.

VII. Обработка данных по поручению

Обработка данных по поручению имеет место, если проведение обработки персональных данных поручается подрядчику без перехода к нему ответственности за соответствующий бизнес-процесс. В таких случаях, как с внешними подрядчиками, так и между компаниями внутри концерна «Даймлер», должно заключаться соглашение об обработке данных по поручению. При этом предприятие-заказчик несет полную ответственность за правильное осуществление обработки данных. Подрядчику разрешается обрабатывать персональные данные исключительно в рамках указаний заказчика. При поручении задания должны соблюдаться нижеперечисленные критерии, за обеспечение которых отвечает дающее поручение структурное подразделение концерна.

1. Подрядчик выбирается на основании его пригодности для обеспечения требуемых технических и организационных защитных мер.
2. Поручение осуществляется в письменной форме. При этом должны быть задокументированы указания по обработке данных и сферы ответственности заказчика и подрядчика.
3. Подлежат соблюдению предоставленные уполномоченным концерна по вопросам защиты данных стандарты составления договоров.
4. Перед началом обработки данных заказчик должен убедиться в соблюдении подрядчиком его обязанностей. Соблюдение требований по безопасности данных подрядчик может подтвердить, предъявив, в частности, надлежащую сертификацию. В зависимости от степени риска обработки данных должны, при необходимости, в течение срока действия договора регулярно проводиться повторные проверки.

5. При трансграничной обработке данных по поручению подлежат соблюдению требования соответствующего национального законодательства, предъявляемые к пересылке персональных данных за рубеж. В частности, проведение обработки персональных данных из Европейского экономического пространства допускается в третьем государстве только при условии, что подрядчик может подтвердить адекватный уровень защиты данных, соответствующий настоящим правилам защиты данных. Соответствующими инструментами могут служить:
- а. Соглашение о стандартных условиях договоров ЕС по обработке данных по поручению в третьих государствах с подрядчиком и возможными субподрядчиками.
 - б. Участие подрядчика в признанной ЕС системе сертификации по обеспечению надлежащего уровня защиты данных.
 - в. Признание обязывающих корпоративных регламентов подрядчика по обеспечению надлежащего уровня защиты данных соответствующими компетентными надзорными органами по защите данных.

VIII. Права затронутого лица

Каждое затронутое лицо может пользоваться нижеследующими правами. Реализация этих прав подлежит незамедлительной обработке ответственным подразделением и никоим образом не должно идти в ущерб затронутому лицу.

1. Затронутое лицо имеет право требовать информацию о том, какие персональные данные о нем, из какого источника и для каких целей были сохранены. Если соответствующим трудовым правом в трудовых отношениях предусмотрены дополнительные права на ознакомление с документами работодателя (например, с личным делом), то они остаются в силе.
2. Если персональные данные передаются третьим лицам, то необходимо предоставление сведений о личности получателя или о категориях получателей.
3. При неправильности или неполноте персональных данных затронутое лицо может требовать их исправления или дополнения.
4. Затронутое лицо может возразить против обработки своих персональных данных в рекламных целях или в целях изучения рынка и общественного мнения. Для этих целей данные должны быть заблокированы.
5. При отсутствии или упряднении правовой основы для обработки данных затронутое лицо вправе требовать удаления своих 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 интересы затронутого лица, требующие защиты.
6. Затронутое лицо обладает принципиальным правом на возражение против обработки своих данных, которое следует учитывать, если его достойные защиты интересы в силу особой сложившейся личной ситуации превалируют по сравнению с интересом в обработке этих данных. Данное право не действует, если какое-либо правовое предписание обязывает к проведению обработки данных.

Помимо этого каждое затронутое лицо может воспользоваться предоставленными в пунктах III (абз. 2), IV, V, VI, IX, X и XIV (абз. 3) правами стороннего бенефициара, если предприятие, обязавшееся соблюдать правила защиты, не выполняет их предписания, в результате чего ущемляются права затронутого лица.

IX. Конфиденциальность обработки

Обработка персональных данных осуществляется на конфиденциальной основе. Сотрудникам запрещается несанкционированно собирать, обрабатывать или использовать эти данные. Несанкционированной считается всякая обработка, которую предпринимает сотрудник, не уполномоченный или не имеющий на то права в рамках исполнения своих обязанностей. Действует принцип необходимого знания (Need-To-Know): сотрудникам разрешается доступ к персональным данным только в том случае, если и насколько это необходимо для их соответствующей деятельности. Это требует тщательного распределения и разделения ролей и ответственностей, а также их осуществления и поддержания в рамках концепций доступа.

Сотрудникам не разрешается использование персональных данных в собственных личных или экономических интересах, а также передача их неуполномоченным лицам или же любое иное обеспечение этим лицам доступа к данным. В начале вступления в силу трудовых отношений начальники должны проинструктировать своих сотрудников об обязанности соблюдения конфиденциальности данных. Это обязательство остается в силе также и по окончании трудовых отношений.

X. Безопасность обработки

Персональные данные должны быть в любое время защищены от несанкционированного доступа, неправомерной обработки или передачи, а также от утери, искажения или уничтожения. Это действует независимо от того, осуществляется ли обработка данных в электронном виде или на бумаге. Перед введением новых процессов обработки данных, в особенности, новых ИТ-систем, должны быть определены и внедрены технические и организационные меры, обеспечивающие защиту персональных данных. Эти меры должны быть ориентированы на современный уровень техники, связанные с обработкой данных риски и необходимую степень защиты данных (установленную в процессе классификации информации). В этих целях ответственное структурное подразделение может, в частности, прибегнуть к консультациям своего уполномоченного по информационной безопасности и координатора по вопросам защиты данных. Эти организационно-технические меры по защите персональных данных являются частью интегрированного менеджмента информационной безопасности во всем концерне и подлежат непрерывной адаптации в соответствии с развитием технических возможностей и организационными изменениями.

XI. Проверка мер по защите данных

Соблюдение правил защиты данных и действующих законов по защите данных регулярно проверяется в ходе аудиторских и прочих проверок мер по защите данных. Их проведение входит в обязанности уполномоченного концерна по вопросам защиты данных, координаторов по вопросам защиты данных и прочих обладающих аудиторскими полномочиями подразделений предприятия или же внешних уполномоченных экспертов. О результатах проверок мер по защите данных необходимо сообщать уполномоченному концерну по вопросам защиты данных. Об имеющих существенное значение результатах проверок в рамках соответствующих обязанностей предоставления отчетов должен оповещаться наблюдательный совет «Даймлер АГ». По запросу результаты проверок мер по защите данных предоставляются компетентному надзорному органу по защите данных. Компетентный надзорный орган по защите данных вправе также проводить в рамках предоставленных ему государственным законодательством полномочий свои проверки соблюдения предписаний настоящих правил.

XII. Нарушения требований по защите данных

Каждый сотрудник обязан немедленно докладывать своему соответствующему начальнику, своему координатору по вопросам защиты данных или уполномоченному концерна по вопросам защиты данных о случаях нарушения настоящих правил защиты данных или других предписаний по защите персональных данных (нарушения требований по защите данных¹⁴). Ответственный за службу или подразделение руководитель обязан немедленно оповестить соответствующего координатора по вопросам защиты данных или уполномоченного концерна по вопросам защиты данных о нарушениях требований по защите данных.

В случае

- » неправомерной передачи персональных данных третьим лицам,
- » неправомерного доступа третьих лиц к персональным данным или
- » утери персональных данных

должны быть незамедлительно произведены предусмотренные на предприятии оповещения (управление инцидентами информационной безопасности) с целью обеспечения выполнения действующих на основе законодательства обязанностей заявления о нарушениях требований защиты данных.

XIII. Ответственность и санкции

Правления и руководства компаний концерна отвечают за обработку данных в сфере своей ответственности. Таким образом они обязаны обеспечивать соблюдение законодательных и сформулированных в правилах защиты данных требований по защите данных (напр., обусловленные национальным законодательством обязанности предоставления сведений). В управленческие задачи, стоящие перед руководителями, входит обеспечение надлежащей обработки данных с учетом защиты данных за счет принятия организационных, кадровых и технических мер. За осуществление этих предписаний несут ответственность соответствующие сотрудники. О проверках мер по защите данных, проводимых надзорными органами, необходимо незамедлительно сообщать уполномоченному концерна по вопросам защиты данных.

Соответствующие руководства компаний и заводов должны назначать в поддержку уполномоченному концерна по вопросам защиты данных координатора по вопросам защиты данных. В организационном плане эту задачу может выполнять – при согласовании с уполномоченным концерна по вопросам защиты данных – один координатор по вопросам защиты данных для нескольких компаний или заводов. Координаторы по вопросам защиты данных являются контактными лицами на местах по вопросам защиты данных. Они могут проводить проверки и должны знакомить сотрудников с содержанием правил защиты данных. Соответствующие руководства компаний обязаны оказывать всяческую поддержку в деятельности уполномоченного концерна и координаторов по вопросам защиты данных.

Ответственные за осуществление бизнес-процессов и проектов эксперты обязаны своевременно информировать координаторов по вопросам защиты данных о новых процессах обработки персональных данных. При проведении проектов по обработке данных, в процессе которых могут возникнуть особые риски для личных прав затронутых лиц, уже до начала обработки подключается уполномоченный концерна по вопросам защиты данных. Это, в частности, относится к персональным данным, требующим повышенной степени защиты.

Руководители отвечают за то, чтобы их сотрудники в необходимом объеме проходили обучение обращению с персональными данными.

Недозволенная обработка персональных данных или иные нарушения правовых норм по защите данных в ряде государств преследуются, в том числе и в уголовном порядке, и

¹⁴ См. XV.

могут повлечь за собой претензии о возмещении ущерба. Правонарушения, за которые несут ответственность отдельные сотрудники, могут повлечь за собой применение вытекающих из трудовых правоотношений санкций.

XIV. Уполномоченный концерна по вопросам защиты данных

Уполномоченный концерна по вопросам защиты данных, представляя собой внутрикорпоративный и в профессиональном плане независимый от указаний орган, обеспечивает соблюдение национальных и международных предписаний по защите данных. Он несет ответственность за правила, регулирующие защиту данных, и следит за их соблюдением. Уполномоченный концерна по вопросам защиты данных назначается правлением «Даймлер АГ». Компании концерна, обязанные назначать уполномоченного по вопросам защиты данных, также принципиально назначают уполномоченного концерна в качестве законного уполномоченного по вопросам защиты данных. Индивидуальные исключения подлежат согласованию с уполномоченным концерна по вопросам защиты данных.

Координаторы по вопросам защиты данных своевременно докладывают уполномоченному концерна по вопросам защиты данных о рисках в области защиты данных.

Каждое затронутое лицо может обращаться с предложениями, запросами, запросами сведений или жалобами, связанными с защитой или безопасностью данных, к уполномоченному концерна по вопросам защиты данных или к соответствующему координатору по вопросам защиты данных. Запросы и жалобы по желанию обрабатываются в конфиденциальном порядке.

В случае если ответственный координатор по вопросам защиты данных не в состоянии удовлетворить жалобу или устранить нарушение правил защиты данных, он должен подключить к делу уполномоченного концерна по вопросам защиты данных. Решения, принимаемые уполномоченным концерна по вопросам защиты данных с целью устранения нарушения норм защиты данных, должны учитываться соответствующим руководством компании. О запросах со стороны надзорных органов необходимо всегда оповещать также уполномоченного концерна по вопросам защиты данных.

Контактные данные уполномоченного концерна и его сотрудников:
Daimler AG, Konzernbeauftragter für den Datenschutz, HPC 0518,
(«Даймлер АГ», уполномоченный концерна по вопросам защиты данных)
D-70546 Stuttgart (Штутгарт)
E-Mail: mbox_lobbying@daimler.com
В Интранете по адресу: <http://intra.corpintra.net/cdp>

XV. Определения

- » Адекватный уровень защиты данных третьих государств признается как таковой комиссией ЕС при условии, если обеспечивается существенная защита основной сути приватной сферы в том смысле, в каком она единодушно понимается в государствах-членах ЕС. Комиссия ЕС учитывает при принятии решений все обстоятельства, играющие роль для передачи данных или какой-либо категории передачи данных. Это включает оценку законодательства, а также соответствующих действующих правил поведения и мер безопасности.
- » Анонимизированными считаются данные при условии, если в долгосрочном плане и никем не может быть установлено их отношение к определенному лицу или если их отношение к данному лицу может быть установлено только при несоразмерно большой затрате времени, средств и рабочей силы.

- » Данными, требующими повышенной степени защиты, являются данные о расовой и этнической принадлежности, о политических мнениях, о религиозных или философских убеждениях, о принадлежности к профсоюзам, а также о здоровье или половой жизни затронутого лица. На основе положений законодательства к данным, которые достойны защиты в особой мере, могут быть отнесены дальнейшие категории данных или же категориям данных может быть присвоено различное содержание. Часто также и данные, касающиеся уголовно наказуемых деяний, разрешается обрабатывать только при наличии особых, определенных законодательством предпосылок.
- » Затронутым лицом в смысле настоящих правил защиты данных является любое физическое лицо, данные которого подвергаются обработке. В некоторых странах в роли затронутого лица может также выступать юридическое лицо.
- » Нарушениями требований по защите данных являются все события, при которых возникает обоснованное подозрение в том, что персональные данные противозаконным образом отслеживаются, собираются, изменяются, копируются, передаются или используются. Это может касаться действий как со стороны третьих лиц, так и со стороны сотрудников.
- » Третьим лицом является каждый, за исключением затронутого лица и за исключением ответственной за обработку данных инстанции. Действующие по поручению обработчика данных на территории ЕС не относятся к третьим лицам в смысле правовых норм по защите данных, так как они на законных основаниях числятся за ответственной инстанцией.
- » Третьими государствами в смысле настоящих правил защиты данных являются все государства, не входящие в Европейский Союз / Европейское экономическое пространство. Исключением являются государства, уровень защиты данных в которых признан Комиссией ЕС адекватным.
- » Согласием является добровольное, имеющее обязательную юридическую силу заявление о согласии в отношении обработки данных.
- » Необходимой признается обработка персональных данных в том случае, если допустимые цели или правомерный интерес без соответствующей обработки персональных данных не могут быть реализованы вообще или же могут быть реализованы лишь при несоразмерно высоком уровне затрат.
- » Под Европейским экономическим пространством (ЕЭП) понимается ассоциированное с ЕС экономическое пространство, в которое также включены Норвегия, Исландия и Лихтенштейн.
- » Персональные данные включают в себя все сведения об определенном или определяемом физическом лице. Определяемым данное лицо считается, например, если отношение к нему может быть установлено посредством комбинации сведений даже со случайно имеющейся дополнительной информацией.
- » Передачей является любое разглашение подлежащих защите данных ответственной инстанцией третьим лицам.
- » Обработка персональных данных – это любая выполняемая автоматизированным методом или без него процедура сбора, сохранения в памяти, организации, хранения, изменения, запроса, использования, пересылки, передачи, распространения или комбинирования, а также синхронизации данных. Сюда включены также устранение, удаление и блокировка данных и носителей данных.
- » Ответственной инстанцией является та юридически самостоятельная компания концерна «Даймлер», в результате деятельности которой возникает необходимость принятия соответствующих мер по обработке данных.

