

## Corporate Policy Data Protection for Data of Customers & Partners

Policy Profile		
Short Title	Data Protection Policy Customers and Partners	
Policy Number	A 18.0	
Purpose of Policy / Summary	The policy regulates all processing of personal data of customers and partners. It creates a uniform and global valid data protection and data security standard which is based on basic principles accepted globally. The policy creates necessary basic conditions for a global data exchange between the companies of the group.	
Scope of Application	This policy applies to all companies and employees of the Daimler Group worldwide.	
Explanation on Scope of Application		
Period of validity of this version	10/1/2009 to 9/30/2014	
Last Revision of this version	11/16/2012	
Approval	Board of Management: 07/28/2009	
Topic (incl. Subtopic)	Integrity & Compliance: (Data Protection)	
Policy responsible	Dr. Joachim Riess - Daimler AG (0400) (CDP)	
Contact Person	Dr. Joachim Riess - Daimler AG (0400) (CDP)	
Documentation	This policy is documented in "Company/Policies & Guidelines/Enterprise Regulation Database (ERD)" in the employee portal at 11/16/2012.	
Documents	<b>Documents</b>	<b>Pages</b>
	Data Protection Policy Customers and Partners	12
	Communication Document	4
Further Applicable Regulations	<ul style="list-style-type: none"> <li>- Privacy Statement</li> <li>- Cookie Statement</li> <li>- Data protection and quality standards for e-Business-applications</li> <li>- MBVD Data protection manual</li> <li>- Declaration of consent for CRM</li> <li>- Data protection and information security criteria for external partners</li> <li>- Standard clauses to ensure data protection and data security in contracts of data processing on behalf</li> <li>- Confidentiality clause data protection</li> <li>- All Information Security Policies</li> </ul>	
Changes to Previous Version		

*Managers of the organizational units affected by this regulation are responsible for ensuring that their employees are aware of this regulation and that they observe it accordingly. Employees are responsible for familiarizing themselves with the provisions of the regulation and observing them.*

## Table of Contents

I. Aim of the Data Protection Policy.....	2
II. Definitions .....	2
III. Scope of and amendments to the Policy.....	3
IV. Application of the Law of Individual Nations .....	4
V. Principles for Processing of Personal Data .....	4
1. Fairness and lawfulness .....	4
2. Restriction to a specific purpose .....	4
3. Transparency .....	4
4. Data Economy.....	5
5. Factual accuracy and up-to-dateness of data .....	5
6. Data requiring special protection.....	5
7. Need-to-know principle.....	6
8. Automated individual decisions .....	6
VI. Data Processing Legitimacy.....	6
1. Data processing for a contractual relationship .....	6
2. Data processing for advertising purposes .....	6
3. Consent to data processing .....	6
4. Data processing based on legal authorization .....	7
5. Data processing based on legitimate interest.....	7
VII. Transmission of Personal Data.....	7
VIII. Data Transmission within the Group .....	7
IX. Data Processing on Behalf.....	8
X. Telecommunications and Internet .....	9
XI. Rights of the Data Subject.....	9
XII. Data Processing Confidentiality .....	10
XIII. Data Processing Security.....	10
XIV. Responsibilities and Sanctions.....	10
XV. Chief Officer Corporate Data Protection.....	10

## I. Aim of the Data Protection Policy

Customer and partner data represent an important competitive factor and make an extensive contribution to value creation in the Daimler Group. These data must be protected against the threats posed by unauthorized access. In addition to this technical security aspect, customers and partners expect us in general to handle their data with care. We cannot build long-term business relationships with our customers and partners unless that relationship is based on trust. Daimler has recognized this challenge, and also acknowledges that its corporate responsibilities include responsible processing of this data. With this Policy, Daimler is adopting a consistent, globally valid data protection and data security standard for processing the personal data of customers and partners in line with globally accepted principles. The Policy undergirds the Group's competitive ability and forms the basis for long-lasting business relationships built on trust.

The Policy also creates one of the important basic conditions for the global exchange of data between affiliated group companies, because it guarantees an adequate level of data protection for transborder data flows in compliance with the EU Data Protection Directive<sup>1</sup> and other national laws, including in countries in which no adequate data protection legislation is yet in force.

## II. Definitions

- The EU Commission considers the **level of data protection** in third countries to be **adequate** if the core privacy elements, according to the understanding agreed upon by the EU member states, are essentially protected. In making its decision, the EU Commission takes into account all of the circumstances that play a role in data transmission, or in a category of data transmission. This includes an evaluation of the national legislation, as well as the code of professional conduct and security measures in place in each case.
- Data are **anonymized** when a connection to a person can no longer be made, or when a connection to a person can be restored only with a disproportionately large outlay in terms of time, cost, and labor.
- **Data require special protection** if they relate to the racial or ethnic background, political views, religious or philosophical convictions, trade union membership, health, or sexual orientation of the data subject. Further data categories may be classed as requiring special protection, or the content of these data categories may be filled in differently, according to the laws of individual nations. Similarly, data regarding criminal offenses may often be handled only in compliance with special requirements set out in the applicable national laws.
- Under the terms of this Policy, a **data subject** is any natural person who is the subject of the data being handled. In some countries, the data subject may also be a legal entity.
- A **third party** is any person, other than the data subject in question, who cannot be ascribed to the data controller. Contractors processing data on behalf of the controller (see Sec. IX) are not legally considered third parties.

---

<sup>1</sup> Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; available at [http://ec.europa.eu/justice\\_home/fsj/privacy/law/index\\_en.htm#guideline](http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#guideline)

- Under the terms of this Policy, **third countries** include all states that are not members of the European Union/EEA. An exception is made for states whose level of data protection has been recognized as adequate by the EU Commission.
- **Consent** is a legally binding expression of will, given voluntarily, in which the data subject declares his/her agreement to the processing of data.
- The processing of personal data is considered **necessary** if the valid purpose or legitimate interest could not be achieved without the personal data in question, or could be achieved only at a disproportionately large expense.
- The **EEA** is an economic area associated with the EU, to which Norway, Iceland, and Liechtenstein belong.
- **Personal data** is any information about a specific or definable natural person. A person is considered definable if, for example, a relation to the person can be established by the information from the data combined with supplementary knowledge, even if such knowledge is available only by coincidence.
- **Transmission** is any disclosure of protected data to third parties by the data controller.
- **The processing of personal data** is any action, carried out with or without the assistance of automated processes, that serves to collect, save, organize, store, change, access, use, pass on, transmit, distribute, combine, or reconcile the data. This also includes destroying, deleting, or blocking data and data storage media.
- **The data controller** is the legally independent entity within the Daimler Group that initiated the data processing measure in question through its business activities.

### III. Scope of and amendments to the Policy

This Corporate Policy applies for all of the companies in the Daimler Group, i.e. Daimler AG and all of its dependent subsidiaries, as well as associated companies and their employees. Under the terms of this Policy, a dependent subsidiary is a company that Daimler AG can require either directly or indirectly to adopt the Policy by virtue of a majority voting interest, a majority in the company management, or an agreement. This Corporate Policy applies to all processing of personal data relating to customers and partners. This includes data relating to prospects, suppliers, and shareholders. This Policy also applies for data relating to legal entities, to the extent that the law of the individual nation in question includes legal entities within the scope of data protection law.

Individual Group companies are not entitled to put in place regulations that deviate from this Policy. This Policy can be amended only by the Chief Officer Corporate Data Protection, and only within the terms of the procedure set out for the amendment of Corporate Policies.

Group companies must comply with this Policy in its current valid version. The version that was valid at the time the data was processed will apply only in the case that the subsequent version entails a less advantageous position for the data subject.

In the event that the current version should expire and no new version be put in place, the Group companies must comply with last valid version of this Policy as regards data processed up until that point.

#### **IV. Application of the Law of Individual Nations**

This Policy for data protection comprises the internationally accepted principles of data protection, without replacing the existing national laws. It applies in all cases as far as it is not in conflict with the respective national law; additionally, the national law shall apply if it makes greater demands. National law applies in the case that it entails a mandatory deviation from, or exceeds the scope of, this Policy for data protection. This Policy also applies in countries in which there is no corresponding national legislation in place.

For the transborder flow of data originating from the European Union/EEA or from countries that require an adequate standard of protection for transborder data flows, the party importing the data must comply with the national legislation in force in the country from which the data originated when processing such data. This does not apply for data flows within the European Union/EEA or for transborder data flows into non-EU/EEA countries that have been deemed by the European Commission to have an adequate level of data protection.

The notification requirements for data processing set out in the laws of individual nations must be met. Each legally independent entity within the Daimler Group must check whether and to what extent such notification requirements exist. If there is any doubt, the Chief Officer Corporate Data Protection is available to give advice.

#### **V. Principles for Processing of Personal Data**

##### **1. Fairness and lawfulness**

In processing personal data, the individual rights of the data subjects must be protected. Data must be processed fairly and in accordance with legal provisions.

##### **2. Restriction to a specific purpose**

Personal data may be processed only for the purposes for which they were originally collected. Subsequent changes to the purpose are possible only to a limited extent. Such changes may take place by virtue of a contractual agreement with the data subject, consent given by the data subject, or national legislation.

##### **3. Transparency**

The data subject must be informed of how his/her data is being handled. As a matter of principle, personal data must be collected directly from the data subject concerned. When collecting the data, the data subject must either be aware of or be informed of the following:

- The identity of the data controller

- The purpose for which the data is being processed
- Third parties or categories of third parties to whom the data may potentially be transmitted.

The data subject should be informed that the provision of data for marketing purposes is voluntary.

Guidelines on information that must be provided to the data subject regarding the handling of his/her personal data are set out in Corporate Standards.

In addition to the guidelines set out in Corporate Standards, national legislation may impose additional or differing requirements regarding the content and scope of this information. Such requirements might include, for example, information on the data subject's right to object to contact made for marketing and advertising purposes.

#### **4. Data Economy**

Before any step is taken to process personal data, it must be checked whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. This Policy does not apply for statistical analysis or studies based on anonymized data.

Personal data may not be collected in advance and stored for potential future purposes unless required under the law of the individual nation.

Data that are no longer needed should be deleted in compliance with existing archival requirements.

#### **5. Factual accuracy and up-to-dateness of data**

Personal data must be correct and up to date when stored. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, or supplemented.

#### **6. Data requiring special protection**

Personal data requiring special protection may be processed only under certain conditions.

The processing of such data must be expressly permitted or required according to the applicable national law, or it must be necessary in order to assert, exercise, or defend legal claims against the data subject. The data subject may also give his/her express consent to the data being processed.

## **7. Need-to-know principle**

In the context of increasingly flexible company organization, it must be ensured that employees have access to personal data on a need-to-know basis only. The need-to-know principle means that employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

## **8. Automated individual decisions**

Automated processing of personal data intended to evaluate certain personal aspects of the data subject (e.g. creditworthiness) must meet special requirements. It must not form the sole basis for decisions that have negative consequences or result in significant detriment to the data subject. In order to avoid incorrect decisions, it must be ensured that a test and a plausibility check are carried out by an employee. In addition, the data subject must be informed of the fact that an automated individual decision-making procedure is carried out and of its result, and he/she must be given the opportunity to respond. Stricter requirements for automated individual decisions set out in national legislation must be observed.

# **VI. Data Processing Legitimacy**

## **1. Data processing for a contractual relationship**

The data subject's personal data may be processed solely for the purpose of executing a contract. This includes advisory services for the contracting partner after the contract has been concluded, to the extent that this is consistent with the purpose of the contract. This does not include measures undertaken for customer loyalty or advertising purposes.

Before the conclusion of a contract –during the contract initiation phase – the processing of personal data is permitted in order to draw up offers, prepare purchase orders, or for fulfilling any other wish of the prospect leading up to the conclusion of a contract (e.g. a test drive). During the contract initiation phase, it is permitted to contact prospects using the data that they have provided. Any restrictions that the prospects may specify must be observed. For further advertising measures, the requirements set out in VI.2. below must be met.

## **2. Data processing for advertising purposes**

Processing personal data for advertising purposes is permitted as long as this is consistent with the purpose for which the data were originally collected. As part of the communication process with the data subject, consent should be obtained from the data subject to use his/her data for advertising purposes. (See VI.3.).

If the data subject makes an information-related request to a Daimler Group company (e.g. requests to be sent information on a product), the data processing required in order to respond to this request is always permitted, regardless of whether consent has been obtained.

If the data subject objects to his/her data being used for advertising purposes, no further use may be made of the data for such purposes. In addition, existing restrictions regarding the use of data for advertising purposes in place in some countries must be observed. Such restrictions may relate, in particular, to advertising via e-mail, telephone, and fax.

## **3. Consent to data processing**

Data processing may take place by virtue of consent obtained from the data subject. Similarly, the purpose of the data processing may be changed if consent is given by the data subject.

Before consent is given, the data subject must be informed as specified in section V.3. of this Policy. For documentation purposes, statements of consent must be generally obtained either in written or electronic form. In certain circumstances, e.g. during a telephone consultation, consent may be given verbally, in which case the consent must be documented. Special requirements for statements of consent set out in national legislation must be met.

#### **4. Data processing based on legal authorization**

The processing of personal data is also permitted if requested, required, or permitted under the applicable national law. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions.

#### **5. Data processing based on legitimate interest**

The processing of personal data may also be carried out if it is necessary in order to realize a legitimate interest held by either the data controller or a third party. Legitimate interests are usually of a legal nature (e.g. collecting outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence over the interest being pursued through the processing of such data. This must be checked before any data processing is undertaken.

### **VII. Transmission of Personal Data**

For some business processes, it is necessary to pass on personal data relating to customers or partners to third parties. If this does not occur owing to a legal obligation, it must be checked in each instance whether it is in conflict with any interest of the data subject that merits protection. When transferring personal data to a party external to the Daimler Group, the conditions set out in section VI. must be met. If the recipient is located in a third country, he/she must guarantee an adequate level of data protection in line with this Policy. This does not apply if the data transmission is carried out owing to a statutory obligation, or to any other permissible legal obligation. The recipient must be bound under contract only to use the data for the specified purpose.

Data shall be transmitted to government institutions or authorities to the extent required according to the relevant legal provisions in each case.

In the case that data is transmitted to Daimler Group companies by third parties, it must be ensured that the data have been collected lawfully in accordance with the relevant legal provisions, and that the use of such data for the intended data processing activities is permitted.

### **VIII. Data Transmission within the Group**

If a legally independent entity within the Daimler Group passes on personal data to another Group company, from a legal point of view this constitutes transmitting data to a third party. For a data transmission of this kind, the conditions set out in section VI. must be in place.

If personal data are transferred from a Group company with its registered office in the European Union/EEA to a Group company with its registered office in a third country, both the Chief Officer Corporate Data Protection and the company importing the data are obliged to cooperate with any inquiries made by the relevant supervisory authority in the country in which the party exporting the data has its registered office, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data.

In the event that a data subject claims that this Policy has been breached by the Group company located in a third country that is importing the data, the Group company located in the European Union/EEA that is exporting the data undertakes to support the data subject concerned, whose data was collected in the European Union/EEA, in establishing the facts of the matter and also asserting his/her rights in accordance with section XI. of this Policy against the Group company importing the data. In addition, the data subject is also entitled to assert his or her rights, as set out in section XI., against the Group company exporting the data.

In the case of personal data being transmitted from a Group company located in the European Union/EEA to a Group company located in a third country, the data controller transmitting the data shall be held liable for any violations of this Policy committed by the Group company located in a third country with regard to the data subject whose data was collected in the European Union/EEA, as if the violation had been committed by the data controller transmitting the data.

The legal venue is the competent court at the location of the registered office of the company exporting the data.

## **IX. Data Processing on Behalf**

When data is processed on behalf of the data controller, a service provider is engaged to process the data, without taking on responsibility for the associated business process. In the case that personal data is disclosed during data processing on behalf, the controller remains responsible for the data processing. Any claims from the data subject must be made against the controller. In addition, the following measures must be taken when awarding contracts:

1. When selecting a data processor, it must be ensured that the candidate can guarantee the necessary technical and organizational requirements and security provisions. When making the selection, the criteria established by the Chief Officer Corporate Data Protection must be taken into account.
2. The terms and conditions for carrying out data processing on behalf must be set out in a written contract, in which the parties agree on the data protection and information security requirements. In particular, it must be established that the processor may process the data only in accordance with the controller's instructions.
3. Corporate policies must be taken into account when drawing up the contract.

4. When appointing service providers outside of the European Union/EEA to process personal data from the European Union/EEA, the service provider must guarantee an adequate level of data protection in line with this Policy if it intends to process the data in a third country. Similarly, comparable regulations set out in the data protection laws of individual nations must also be observed. In addition, when appointing service providers outside of the European Union/EEA, the requirements set out in section VII. must be met.

## **X. Telecommunications and Internet**

The processing of personal data that have been gathered exclusively through telecommunications with the data subject, including Internet communication, is subject to the relevant local instructions, or the relevant law.

Corporate Standards regarding putting legal obligations into practice when designing Websites must be complied with.

## **XI. Rights of the Data Subject**

Every data subject has the following rights. The assertion of these rights is to be processed directly by the responsible department.

1. The data subject may request information on which personal data relating to him/her have been stored, how the data were collected, and for what purpose.
2. If personal data are transmitted to third parties, the data subject must also be informed of the recipient's identify, or of the category of recipients.
3. If personal data are incorrect or incomplete, the data subject may request for them to be corrected.
4. The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing archival requirements must be observed.
5. The data subject may object to his/her personal data being used for purposes of direct marketing, market research, or opinion research. Access to the data for these purposes must then be blocked.
6. The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

## **XII. Data Processing Confidentiality**

The personal data of customers and partners is treated confidential; any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorised to carry out as part of his/her legitimate duties is unauthorized.

In particular, it is forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or make it available in any other way.

## **XIII. Data Processing Security**

Appropriate technical and organizational measures are implemented in order to guarantee data security. These measures safeguard personal data from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. They relate to the security of data which merit protection, whether processed electronically or in paper form.

These technical and organizational measures form part of an integrated information security management plan, and are constantly revised in accordance with technological developments and organizational changes.

## **XIV. Responsibilities and Sanctions**

The boards of management and management staff of the Group companies, who in each case bear responsibility for data processing activities, are obliged to ensure that legal data protection requirements and requirements formulated in this Policy for data protection are met.

Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing undertaken in their department is carried out in accordance with regulations and with due regard for data protection. Compliance with the Data Protection Policies and the applicable Data Protection Laws is controlled by regular data protection audits.

In many countries, abusive processing of personal data or other violations of data protection laws may lead to criminal proceedings and claims for damages. In principle, contraventions for which individual employees can be held responsible are subject to employment law sanctions in accordance with the applicable national legislation in the country in question (see Guideline on Disciplinary Measures).

## **XV. Chief Officer Corporate Data Protection**

The Chief Officer Corporate Data Protection, being internally independent of professional orders, supervises the observance of national and international data protection regulations. He is responsible for the Policies on data protection, and supervises their compliance. He carries out data protection checks and audits. The Chief Officer Corporate Data Protection is appointed by the Daimler AG board of management.

The business management or plant management must indicate to the Chief Officer Corporate Data Protection that they have appointed a data protection coordinator. In organizational terms, and with the agreement of the Chief Officer Corporate Data Protection, one data protection coordinator may also be appointed to carry out this role for several companies or plants. The data protection coordinators act as on-site advisors for data protection issues. They can carry

out checks, and they are responsible for ensuring that employees are familiar with the content of the Data Protection Policies. The management of the company in question is obliged to support the Chief Officer Corporate Data Protection and the data protection coordinators in their activities.

The business units must inform the data protection coordinators of any new activities involving the processing of personal data. The data protection coordinators shall promptly inform the Chief Officer Corporate Data Protection of any data protection risks. If data processing activities are planned that could entail particular risks to the personal rights of the data subjects, the Chief Officer Corporate Data Protection must be involved in advance of any data processing activity. This applies in particular for personal data requiring special protection.

The business units ensure that their employees obtain the necessary education on data protection. The Chief Officer Corporate Data Protection provides a web based training tool.

In the event of data protection breaches or complaints, the management staff responsible must immediately inform the responsible data protection coordinator or the Chief Officer Corporate Data Protection. In addition, any data subject may approach the Chief Officer Corporate Data Protection at any time to raise concerns, ask questions, request information, or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially. Decisions made by the Chief Officer Corporate Data Protection to remedy data protection breaches must be respected by the management of the company in question.

Contact details for the Chief Officer Corporate Data Protection and his staff are as follows:  
Daimler AG, Chief Officer Corporate Data Protection, HPC 0518,  
D-70546 Stuttgart, Tel: +49 (0)711 17 97727  
E-mail: [mbox\\_datenschutz@daimler.com](mailto:mbox_datenschutz@daimler.com)  
Intranet: <http://intra.corpintra.net/cdp>

# DAIMLER

Optimization within  
Policy Project  
regarding volume,  
structure and  
comprehensibility

---

## Communication Document for Policy A 18.0

Data Protection Policy Customers and Partners

Note! Printouts of this regulation may already be out of date. Always check on the ERD to ensure you have the latest version.

A 18.0; Data Protection Policy Customers and Partners Valid from: 10/1/2009 Valid To: 9/30/2014;  
Page 13 of 16 pages (profile + policy + annexes)

## Purpose of the policy

In addition to technical security, customers and partners expect us in general to handle their data with care. We cannot build long-term business relationships with our customers and partners unless that relationship is based on trust. Daimler has recognized this challenge, and also acknowledges that its corporate responsibilities include responsible processing of this data. With this Policy, Daimler is adopting a consistent, globally valid data protection and data security standard for processing the personal data of customers and partners in line with globally accepted principles.

## Target group

This policy applies to all companies and employees of the Daimler Group worldwide. It particularly relates to those employees, who design processes and collect, process and use personal data of customers and partners.

## Main issues of the policy

In processing personal data of customers and partners, the **individual rights** of the data subjects must be protected.

The Policy therefore regulates under which circumstances such data processing is **legitimate**. This can be the case, for example, for the purpose of the proper fulfillment of a contract or by virtue of consent obtained from the data subject.

Please also note the **principles** on the processing of personal data of customers and partners as defined by the Policy, like fairness and lawfulness, restriction to a specific purpose, transparency and data economy.

## Changes from previous version

-

## Approval

The Board of Management of Daimler AG

Valid from: 01.10.2009

Valid to: 30.09.2014

## Requests for action

The boards of management and management staff of the Group companies, who in each case bear responsibility for data processing activities, are obliged to ensure that legal data protection requirements and requirements formulated in this Policy for data protection are met. However, data protection is a task of every employee dealing with personal data and management alike.

## Contacts for questions regarding content

Dr. Joachim Rieß (CDP, Tel. 0711/17-97727)

## Where can I find more information?

Informationen regarding Data Protection can be found on the CDP intranet page:

<http://portal.e.corpintra.net/go/cdp>

Note! Printouts of this regulation may already be out of date. Always check on the ERD to ensure you have the latest version.