

DAIMLER

Data Protection and Privacy –
The Daimler Code of Conduct for Customers/Suppliers

Our motto:

Premium Cars Premium Services Premium Privacy

Our challenges:

Desires and demands of our customers

Increased sensitivity of our customers

Heterogeneous legal requirements for data protection

Data protection for transborder data flows

Adequate level of data protection throughout the Group

Uniform image in the competition

Integrative data protection and data security management

Our solutions:

Global approach

Adequate level of data protection based on self-regulation

Data protection is a qualitative and a competitive advantage

Internal data protection organization

Internal law enforcement

Integration of data protection and data security in our products and services

Dear Colleagues,

One important aspect in providing services that meet the needs of our customers and in effectively designing our business processes is the consideration of data protection issues.

As a globally operating company, Daimler AG and its affiliated companies face the task of dealing with legal requirements for the collection and processing of personal data that vary greatly throughout the world. Therefore, particularly as concerns the transborder exchange of personal data between the individual affiliated companies within the Group, legal pre-conditions must be observed. In this respect according to a number of different national laws the transborder transfer of personal data is generally permitted only if the company which receives the data can ensure an adequate level of data protection.

In order to ensure a level of data protection throughout the Group that is adequate for the transborder transfer of personal data while at the same time taking national requirements into consideration, Daimler AG has adopted the "Data Protection and Privacy – The Daimler Code of Conduct" with respect to customer data and data concerning other business partners.

The Chief Officer Corporate Data Protection ensures that the obligations arising from the "Data Protection and Privacy – The Daimler Code of Conduct" are enforced and that national data protection laws are observed. To ensure that these tasks are effectively fulfilled at the local level, and in order to support the Chief Officer Corporate Data Protection in performing his functions, employees are appointed locally as data protection coordinators in the departments and companies, both domestically and in foreign countries. They report to the Chief Officer Corporate Data Protection and are professionally trained by him. You can find the data protection coordinator responsible for you in the data protection department's websites in the Intranet (<http://cdp.intra.corpintra.net>).

If you have any questions concerning the implementation of the "Data Protection and Privacy – The Daimler Code of Conduct", please feel free to contact either the data protection coordinator or myself.



Dr. Joachim Riess
Chief Officer Corporate Data Protection

Content

I. Aim of the Code of Conduct	5
II. Scope of the Code of Conduct	5
III. Application of the Law of Individual Nations	5
IV. Principles for the Processing of Personal Data	6
V. Special Categories of Personal Data	6
VI. Notification and Consent of the Data Subjects	7
VII. Rights of the Data Subjects	8
VIII. Confidentiality of Processing	8
IX. Principles of Data Security	8
X. Marketing Data/Data Processing on Behalf/ Involvement of Third Parties	9
XI. Customer Contact via Telecommunication	9
XII. Remedies/Sanctions/Responsibilities	9
XIII. The Chief Officer Corporate Data Protection	10
Definitions	12

For a global company like Daimler modern information and communication technology is an important element of business processes. Improper use or misuse of this technology can lead to a violation of individual rights. Our aim is to give value in the development of the information society to the protection of these individual rights. The high level of service which our company strives to offer requires us to take note of the customer's and contractor's data protection concerns. Conscious of this aim, Daimler AG and the affiliated companies undertake to comply with the following Code of Conduct.

I. Aim of the Code of Conduct

The aim is to apply such uniform, adequate and global data protection and privacy standards throughout the entire Daimler Group as will comply with statutory requirements imposed on those data flows by the European Data Protection Directive¹ and other national laws requiring an adequate data protection standard for transborder data flow. This Code of Conduct provides a unified level of data protection groupwide, but does not replace the need for legitimation which has to be the basis for all data processing or transfer. Employees and management shall be supported in integrating data protection concerns of our customers and contractors into the company's products and services. This section should be interpreted in conjunction with the following provisions set forth in the Code of Conduct, especially the legal applicability in Section III.

II. Scope of the Code of Conduct

This Code of Conduct is a corporate guideline and applies both to the processing of personal customer data as well as to personal data of our suppliers or consultants or other business partners.

III. Application of the Law of Individual Nations

As far as the permissibility of data collections and processing is concerned, the national and applicable local law of the respective state is conclusively applicable, where the data is collected and processed. That means, that the processing of personal data collected and processed in other countries than the EU/EEC is subject to the national and local law of the country of origin. Processing of personal data generated in the EU/EEC or in countries requiring an adequate data protection standard in case of data transfers to third countries, is subject to the national law of the country of origin. This does not apply to data transfers within the EU/EEC or to countries which data protection regulations have been deemed to provide an adequate level of protection pursuant to Art. 25 of the European Data Protection Directive.

Any mandatory registration provisions which may exist according to any national data protection law must be observed. Every legally independent company within the Daimler Group must check whether and to what extent such registration obligations exist towards national supervisory authorities or control organs. In case of uncertainty, the Chief Officer Corporate Data Protection may be consulted.

Collection of personal data by and their disclosure to governmental institutions and authorities will only be carried out on the basis of specific relevant national legal provisions.

In all cases this Code of Conduct shall impose only those restrictions that are necessary to meet the legal requirements of those national laws providing restrictions on international data flows.

¹ Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (95/46/EG).

IV. Principles for the Processing of Personal Data

1. In processing personal data, the individual rights of data subjects must be protected.
2. Personal data may only be processed if allowed by law or agreement, or if the data subject has consented. Personal data may only be processed for the purposes for which it was originally collected, and if the purpose is allowed by law, or agreement, or if the data subject has consented.
3. Stored personal data should be accurate and, if necessary, updated. Reasonable steps must be taken to ensure that inaccurate or incomplete data are deleted or corrected.
4. Persons who have access to personal data shall only be those whose function and responsibility specifically include the handling of such personal data; the right of access is restricted according to the nature and scope of the individual function and responsibility.
5. Taking into consideration the legal obligations to preserve records - where applicable - data shall be deleted, if it is no longer needed for the business purposes for which it was originally collected and stored.
6. If a data subject objects to the use of her or his personal data for marketing purposes, then this data may not be used for such marketing purposes.
7. The processing of data should be designed to collect, process or use only the data that is necessary, i.e. as little as possible. Options of anonymizing or pseudonomizing data must be realized if this is possible and seems reasonable in consideration of the expenditure. Statistical evaluations on the basis of anonymized or pseudonomized data do not have to comply with data protection requirements, as far as a connection to the data subject can no longer be made.
8. The data subject has the right not to be subject to a decision which produces unfavorable legal effects concerning her or him or significantly affects her or him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to her or him, such as her or his creditworthiness. Information technology may serve as a decision-making tool but not as the only basis for decisions. If such automated decisions should be made in individual cases the data subject must have the opportunity to express her or his point of view, unless the decision is allowed by law which also lays down measures to safeguard the data subject's legitimate interests.
9. In cases where data processing is planned which could entail particular risks to the personal rights of data subjects, the Data Protection Department is to be involved from the outset before the processing starts. This applies especially to the following categories of data.

V. Special Categories of Personal Data

In principle the processing of personal data concerning racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or details about the health or sexual orientation of the data subject concerned is not permitted, except when the processing of this data is required or allowed by law. Furthermore, a processing of special categories of personal data is also permitted when it is necessary for the establishment, exercise, defense of legal claims or litigation, unless the legitimate interest of the data subject to exclude the processing and usage of her or his personal data prevails. Otherwise, these special data categories can also be processed if the data subject has given explicit consent.

VI. Notification and Consent of the Data Subjects

The following requirements do not apply to data collections conducted in the U.S. In this case the respective national or local law applies.

1. Contractual relations

Personal data about the data subject may be processed on the basis or for the purposes of negotiating and completing or executing a contract. In this connection it may also be processed and used for marketing as well as market research and opinion survey purposes, provided that this is compatible with the purpose for which the data was originally collected.

By collecting her or his personal data, the data subject must be clearly aware or appropriately informed of the following:

- Identity of the company responsible for data processing
- Purpose of processing this data
- Third parties or categories of any third parties to whom the data may be passed
- Optional nature of participating in activities involving market and opinion research.

This processing transparency can be achieved by individual or general information. The data subject must be made aware of her or his access and correction rights in respect of her or his own personal data. Furthermore, she or he must be informed of the fact that she or he can refuse to allow the use of her or his data for purposes of direct marketing, no later than the time of the first inclusion in a mailing.

2. Relationships without contract

If a contractual relationship does not exist, or is not in the process of being negotiated and completed, the data subject must consent to any collection and processing of her or his personal data, unless the collection or processing is permitted or required by law. The same shall apply for any processing or use of the data beyond the original purposes for which it was collected. Before meaningful consent can be given by the data subject, she or he must be informed as prescribed by Sec. VI. clause 1 of this Code of Conduct.

For reasons of proof, a declaration of consent is usually to be obtained in writing. If the consent concerned is obtained in connection with the conclusion of a purchase contract, for example, the section of the contract which contains the consent must be clearly marked on the contract form. In the declaration of consent, the scope and purpose of the data processing must be specified. If special circumstances arise, for example, consultation by telephone, consent may be granted orally in exceptional cases. The drafting of the electronically given declaration of consent must comply with the Data Protection and Quality Standards for e-Business Applications under <http://cdp.intra.corpintra.net> or the relevant applicable job instructions.

3. Data exchange with Third Parties/Data Procurement

As a rule, personal data is to be collected directly from the data subject herself or himself. If data is collected at third parties, or is passed to us by third parties for further processing, care must be taken to ensure that the data subject is or shall be appropriately informed in the course of the first contact in accordance with Sec. VI. clause 1 of this Code of Conduct.

Consent must be obtained for credit-worthiness enquiries. Where data is purchased, it must be ensured that the data has been properly and lawfully obtained in compliance with the respective national law.

4. Data exchange within the Group

If a legally independent entity within the Daimler Group passes data of the data subject to another Group member company, this constitutes disclosure to a third party, which means that, even in such “intra-Group” cases, the criteria pursuant to Sec. VI. clauses 1 and 2 of this Code of Conduct shall likewise be deemed to apply, with the consequence that the transfer of the data must be legitimized.

For personal data transfer to third parties that don't belong to the Daimler Group, Sec. VI. clause 1 and 2 as well as Sec. X. clause 5 of this Code of Conduct are deemed to apply.

VII. Rights of the Data Subjects

Data subjects may contact the competent data protection coordinator, their Daimler representative, or the Chief Officer Corporate Data Protection of the Group with questions or complaints. If they exercise the following rights, their inquiries must be answered as soon as possible.

1. The data subject can demand information regarding the source, type and purpose of the personal data stored about her or him.
2. In the case of disclosure of data to third parties, information concerning the identity of the recipient or the categories of recipients must be disclosed.
3. If, for example, it becomes clear during the implementation of the data subject's right of access, that the data subject's personal data is incorrect or incomplete, the data subject shall be entitled to claim that the information be corrected. If the purpose for the data processing no longer applies, because of the passage of time or for any other reason, or if processing is found to be illegal and this was overlooked during regular audit procedures, the data must be deleted physically, with due regard to applicable legal obligations to preserve records.
4. The data subject has the right to object to the use of her or his personal data for marketing purposes or market research and opinion surveys. In this case, the data must be blocked for these purposes.
5. In principle, the data subject has a right to object to the processing of her or his personal data provided that, after evaluation her or his legitimate interest because of her or his particular personal circumstances is found to outweigh the interest of the company responsible for data processing. This provision does not apply if a legal provision requires the processing or use of these personal data.

VIII. Confidentiality of Processing

Only authorized personnel obliged to maintain confidentiality may collect, process or utilize personal data. In particular, the use of such data for individual private purposes, the transmission of such data to unauthorized persons, or the making available of such data to unauthorized persons in any other way is prohibited. "Unauthorized persons" shall include colleagues in the workplace, unless authorized by virtue of their function and responsibility and their concrete tasks. A sample text for a declaration of confidentiality can be found in the intranet under <http://cdp.intra.corpintra.net>

The obligation to maintain confidentiality persists after the termination of employment.

IX. Principles of Data Security

The technical and organizational measures necessary to ensure data security shall apply to

- Computers (servers and individual workstations)
- Networks or communication connections
- Applications.

Physical and infrastructural security measures are installed in the concerned servers, including control of access (with differentiated authorization), locking devices and fire precaution measures. All individual workstations are equipped with password protection. Daimler's corporate network is protected against unauthorized external access, for example, from the Internet, by firewall systems. Personal data which need to be transmitted via public networks are always encrypted. Exceptions must be reported and explained to the Data Protection Department. Person and application-related access protec

tion has been installed to protect personal data in our databases. These technical and organizational measures form part of a data protection and data security management which regulates responsibilities and authorizations.

X. Marketing Data/Data Processing on Behalf/Involvement of Third Parties

It frequently occurs that external third parties are integrated into corporate working processes.

The following conditions must be observed if one of the Group member companies is acting as either Principal or as Contractor under a contractual relationship and/or if other third parties are involved in the processing or use of personal data:

1. Only such contractors or third parties are to be selected who can guarantee the technical and organizational requirements and security provisions necessary for the processing.
2. The performance of the processing (on behalf of the principal) must be regulated in a contract documented in writing or in some other appropriate form. If necessary, sample clauses are provided by the Chief Officer Corporate Data Protection who will assist in any other way, if necessary.
3. The principal remains the contact person for any customers, suppliers, consultants and other contractual partners wishing to exercise their rights.
4. External third parties who have been commissioned to carry out data processing or other tasks, for example in the fields of marketing, market research and opinion surveys, must be bound by contract only to process or utilize personal data which they receive from the principal within the framework of the contract. Utilization for their own purposes or for the purposes of third parties must be prohibited by contract.
5. Other co-operations with third parties in which personal data may be disclosed or otherwise made available to these third parties, shall likewise be subject to a data protection and a data security standard which corresponds to this Code of Conduct.
6. Objections by the data subject to her or his involvement in marketing, market research or opinion survey activities (see., Sec. VII. of this Code of Conduct) are also to be observed in the case of the involvement of third parties, and, if necessary, shall be passed on to the concerned intra-Group or outside third parties.

XI. Customer Contact via Telecommunication

Processing of personal data which are collected during telecommunications with the data subject (inclusive internet-communications) must comply with the locally relevant job instructions and the respective relevant law.

XII. Remedies/Sanctions/Responsibilities

The companies in our Group, as the persons responsible for the data processing, are obliged to ensure that the requirements of data protection are observed in relation to the data subjects. Should there be a need for training, the Data Protection Department can be called in to assist. Employees who are working with personal data have to be aware that, in many countries, breaches of data protection laws can be legally punishable, and can lead to claims for compensation or damages.

Employees who are found to be responsible for a breach will, in principle be dealt with according to applicable provisions of law.

Should personal data be transferred from one company of the Group located in the EU/EEC (hereinafter the “data exporter”) to another company of the Group outside the EU/EEC (hereinafter the “data importer”), then the Chief Officer Corporate Data Protection and the data importer are both obliged to co-operate with the competent supervisory data protection authority of that country in which the data exporter has its seat in the course of all inquiries and to respect the decision of the supervisory authority with regard to the processing of the data transferred.

In case a data subject alleges a breach of this Code of Conduct by the data importer located outside the EU/EEC, the data exporter located in the EU/EEC is obliged to lend support to the data subject whose data is collected in the EU/EEC to clarify the situation, as well as to make sure that she or he could enforce her or his rights according to Sec. VII. of this Code of Conduct towards the data importer. The rights granted by Sec. VII. of this Code of Conduct can also be applied against the data exporter.

XIII. The Chief Officer Corporate Data Protection

The Chief Officer Corporate Data Protection, an internal data protection organ which is independent and not bound by internal line management instructions, supervises the observance of national and international data protection regulations and of this Code of Conduct. Spot-checks are also conducted by him. Decentrally-located data protection coordinators undertake the tasks of the Chief Officer Corporate Data Protection locally in accordance with national and local law and this Code of Conduct.

The local management is responsible for the appointment of data protection coordinators. The managing directors are obliged to support the Chief Officer Corporate Data Protection and the data protection coordinators in their functions. In order to avoid breaches, the Data Protection Department is to be involved from the beginning (Sec. IV. clause 9 of this Code of Conduct).

The responsible management personnel will immediately report either to the competent data protection coordinator or to the Chief Officer Corporate Data Protection any violations of this Code of Conduct, and inform him about any complaints. In addition, every employee, customer or any other contractual partner can contact the Chief Officer Corporate Data Protection or a data protection coordinator at any time with suggestions, questions, requests for information or complaints in connection with data protection, data security and privacy matters. Questions and complaints will be treated confidentially.

In case the competent data protection coordinator cannot remedy the complaint or cannot stop a breach of the provisions of this Code of Conduct, she or he is obliged to advise the Chief Officer Corporate Data Protection. The responsible management shall abide by the decisions of the Chief Officer Corporate Data Protection taken to remedy the breaches of this Code of Conduct.

The Chief Officer Corporate Data Protection and his staff can be reached as follows:

Daimler AG, Chief Officer Corporate Data Protection, HPC 0624,
D-70546 Stuttgart, Germany. Tel. +49-(0)7 11-17-9 77 27, Fax +49-(0)7 11-17-9 7699,

email: joachim.riess@daimler.com

or in the intranet under <http://cdp.intra.corpintra.net>

Definitions

- **Data subjects** under the terms of this Code of Conduct are all persons with whom a customer relationship exists or is planned, including so-called “prospects” and “potentials”, in so far as personal data is known about them.
- **Personal data** is any information about a definite or definable person. A person is for example definable when a link to the person can be established by a combination of relevant information with a particular employee’s supplementary knowledge which she or he might possess incidentally.
- **The processing of personal data** is any action, carried out with or without the assistance of automated processes, which serves to collect, save, organize, store, adapt, alter, access, use, pass on, distribute, combine or compare data. It also includes denying access to, deleting or destroying data.
- Data is **rendered anonymous** when a connection to a person can no longer be made, or when a connection to a person can only be restored with a disproportionately large expense in time, cost and labor. Data is **pseudonomized** if the name or another identifier is replaced by a substitute, so that the identification of the person is either impossible or at least rendered considerably more difficult.
- The company **responsible for data processing** in the external relationship (for example, vis-à-vis customers) is the legally independent entity within the Daimler Group which initiated the processing measure in question by its business activities. Internally, an organizational and hierarchy structure defines which personnel are responsible, and to what extent, for ensuring the orderly execution of data processing.
- **Contractors processing on behalf of others** are natural or legal persons who process personal data on commission for a responsible party (acting as principal). For example, these can be service companies in the marketing sector or the operators of computer centers.
- **Third parties** are any natural or legal person or authority who cannot be ascribed to the **party responsible for processing the data**. The party who processes data on behalf of the principal or employees who are entrusted with the processing of personal data according to the company organization are for example not third parties in this sense, provided that the personal data concerned fall within the responsibilities of their function.
- **Disclosure** means to pass data on to a third party, who cannot be ascribed to the party responsible for data processing.
- **Consent** is an expression of will in which a data subject, fully aware of the matter concerned and without recognizable external pressure, gives to understand that she or he agrees with the processing of personal data concerning her or him.
- The **right to object** means that the data subject has a right to opt-out to the extent that she or he may forbid the use of her or his data for marketing purposes or for market research or opinion surveys.

