Corporate Policy Data Protection for Human Resources Data

Policy Profile		
Short Title	Data Protection Policy Human Resources	
Policy Number	A 17.0	
Purpose of Policy / Summary	The policy regulates all processing of personal data of employees. 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: 01.10.2009	
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	Documents	Pages
	Data Protection Policy Human Resources	12
	Communication Document	4
Further Applicable Regulations	Data protection and information security criteria for external part-ners Standard clauses to ensure data protection and data security in contracts of data processing on behalf Confidentiality clause data protection Confidentiality clause Telecommunication All Information Security Policies	
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

Motivated and dedicated employees are an important factor for value creation in the Daimler Group. Treating our employees with the respect they deserve includes safeguarding their personal rights. With the increasing data processing activities at many locations and the possibility of worldwide access to personal HR data, there is an increased danger of company resources and employee privacy rights being abused. Daimler recognizes that its corporate responsibilities include responsible handling of personal HR data. With this Policy, Daimler is adopting a consistent, globally valid data protection and data security standard for processing employees' personal data, based on globally accepted principles. The Policy supports the Group's competitive ability, and represents a basis of trust that enhances Daimler's reputation as a desirable employer.

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[1] 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.

• A **third party** is any person, other than the employee 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.

• 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 **EEA** is an economic area associated with the EU, to which Norway, Iceland, and Liechtenstein belong.

[1] 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

▪ Under the terms of this Policy, **an employee** includes any applicant undergoing the job application process and any person who is in an employment relationship with a Group company, including fixed-term positions, as well as pensioners.

• **Personal HR data** is any information about a specific or definable employee. An employee 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 personal 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 and Amendments of the Policy

This 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 Policy applies to all processing of personal HR data. Personal HR data also include data relating to job applicants and pensioners.

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 Data Protection Policy 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 personal HR 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 HR data, the individual rights of the employees must be protected. Personal HR data must be processed fairly and in accordance with legal provisions.

2. Restriction to a specific purpose

Personal HR 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 employee concerned, collective agreements, consent given by the employee, or national legislation.

3. Transparency

Employees must be informed of how their data is being handled. As a matter of principle, personal data must be collected directly from the employee concerned. When collecting the data, the employee 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.

National legislation or collective agreements may impose additional or differing requirements regarding the content and scope of this information.

4. Data Economy

Before any step is taken to process personal HR data, it must be checked whether and to what extent the processing of personal HR 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 by national legislation in force in the country in question.

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

5. Factual accuracy and timeliness of data

Personal HR 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. Personal HR data requiring special protection

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

The processing of such data must be expressly permitted or required according to the applicable national law. In addition, the processing of such data may be permitted if it is necessary in order for the responsible party to uphold its rights or fulfill its obligations in the domain of employment law. The employee 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 HR data intended to evaluate certain personal aspects of the employee (e.g. skills profile) must meet special requirements. It must not form the sole basis for decisions that have negative consequences or result in significant detriment to the employee concerned. 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 employee concerned 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 collection on the basis of employment relationship

For the purpose of the employment relationship such data may be collected that is necessary for executing the employment contract.

Personal data of applicants may be processed for the purpose of initiating an employment relationship. The data of unsuccessful applicants must be deleted in compliance with deadlines set out in the laws of evidence, unless the applicant has given consent for his/her data to be stored for a subsequent selection process. Consent must also be obtained to use the data for further application procedures or to pass them on to other Group companies. If it should be necessary for the application procedure to collect information on an applicant from a third party, the requirements of respective national law have to be observed. In cases of doubt consent of the applicant must be obtained.

2. Data processing on the basis of employment relationship

Personal HR data may be collected and processed on the basis of an employment contract, for the purposes of executing the employment relationship. The processing of data must always relate to the purpose of the employment contract, if none of the subsequent reasons permitting data processing apply. Particularly requirements deriving from applicable law regarding the handling of personal HR data requiring special protection have to be observed. Even within the employment relationship such data may only be processed and used in accordance with respective national law. If it should be necessary within the employment relationship to collect information on an employee from a third party, the requirements of respective national law have to be observed.

When processing personal HR data that fall within the context of the employment relationship but that are not originally processed for the purpose of executing the employment contract, the legal legitimacy of such data processing must always be demonstrated. Such legitimations may be requirements deriving from law, the consent of the employee or legitimate interests of the company.

3. Collective agreements on data processing

If a data processing activity exceeds the purposes of implementing a contract, if may be permissible if authorized through a collective agreement. Collective agreements are labor agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law (e.g. company agreements under German law). The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national data protection legislation.

4. Consent to data processing

Processing of personal HR data may take place by virtue of consent obtained from the employee concerned. Similarly, the purpose of the data processing activity may be changed if consent is given by the employee concerned. Declarations of consent must be given voluntarily. Consent, which came under social pressure, is not effective. Before consent is given, the employee must be informed as specified in section V.3. of this Policy. For documentation purposes, declarations of consent must generally be obtained either in written or electronic form. In certain circumstances, consent may be given verbally, in which case it must be documented. Instead of explicit consent, consent can also be given implicitly by voluntarily providing data, e.g. on the Intranet. In such cases, internal organization standards must be observed. Special requirements for statements of consent set out in national legislation must be met.

5. Data processing based on legal authorization

The processing of personal HR 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. If legal provisions allow a certain amount of discretionary freedom, employees' interests that require protection must be taken into account.

6. Data processing based on legitimate interest

The processing of personal HR 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. asserting, executing, or defending legal claims) or a commercial nature (e.g. carrying out a company evaluation). 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 employee 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.

Control measures, which require a processing of employee data, may only be performed if a legal obligation exists or a justified cause is given. Even with a justified cause being present, a legitimate interest of the enterprise (e.g., adherence to legal provisions or internal rules) must exist, which outweighs possibly existing legitimate interests of the concerned employees in the exclusion of the measure. The legitimate interest of the enterprise and the possible legitimate interests of the employees must be determined and documented before each measure. The measure must be appropriate related to the facts to be examined and the employees to be included into the investigation. If necessary, existing further requirements according to national law (e.g., rights of co-determination of the representatives for the employees and rights of information of the concerned employees) must be considered.

VII. Transmission of Personal Data

For some business processes, it is necessary to pass on personal HR data 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 employee concerned 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 HR 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 an employee 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 employee 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 employee 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 employee 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 HR data is disclosed during data processing on behalf, the controller remains responsible for the data processing activity. Any claims from the employee concerned 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. Guidelines from the Chief Officer Corporate Data Protection must be taken into account when drawing up the contract. If necessary, the Chief Officer Corporate Data Protection will be involved in the process in an advisory capacity.

4. When appointing service providers outside 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. Comparable regulations set out in the data protection laws of other 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

Telecommunications equipment and access to the Internet and Intranet are primarily considered work tools. They may be used in compliance with the relevant legal provisions (laws or collective agreements) and company rules in force at global or national level.

The use of electronic communication networks and services may be logged for security reasons. Checks on individuals may be carried out where there is justified suspicion of abuse. Checks can be initiated only by departments specified in the company organization. The Chief Officer Corporate Data Protection, and, if applicable, an employee representative, must be involved at an early stage.

If, under certain circumstances, it is permitted to use the telecommunications equipment at a particular location for private purposes, the relevant national regulations regarding the secrecy of telecommunications must be observed. This also applies for authorized private use of the e-mail system and Internet connection.

XI. Employee Rights

Every employee has the following rights. The assertion of these rights is to be processed directly by the responsible department. An employee may not suffer any disadvantage as a consequence of asserting his/her rights.

1. The employee 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 HR data are transmitted to third parties, the employee concerned must also be informed of the recipient's identity, or of the category of recipients.

3. If the relevant employment legislation provides for further rights of access to employee documents (i.e. employee files), these rights remain unaffected.

4. If personal HR data are incorrect or incomplete, the employee may request for them to be corrected or supplemented.

5. The employee 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 activity has lapsed or ceased to be applicable for other reasons. Existing archival requirements must be observed.

6. The employee 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 Secrecy

Employees may not collect, process, or use personal data without authorization. Any data processing undertaken by an employee that he/she has not been entrusted to carry out as part of his/her legitimate duties is unauthorized.

The confidentiality obligation also applies for data that are legitimately processed. In particular, it is prohibited to use personal data for private or commercial purposes, to disclose them to unauthorized persons, or make them available in any other way. Under the terms of this Policy, unauthorized persons also include work colleagues, unless a specific colleague is authorized to be party to such information owing to a specific task within his/her area of responsibility.

The confidentiality obligation continues to apply after the employment relationship has ended.

XIII. Data Processing Security

Appropriate technical and organizational measures are implemented in order to guarantee data security. These measures safeguard personal data also from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. These measures 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. For complying with legal data security requirements the Information Security Policy is particularly relevant.

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. In general, group companies that are legally obliged to appoint a data protection officer, will appoint the Chief Officer Corporate Data Protection. Exceptions have to be agreed with the Chief Officer Corporate Data Protection.

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 Policy. 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 employees concerned,

the Chief Officer Corporate Data Protection must be involved in advance of any data processing activity. This applies in particular for personal HR 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 employee may approach the Chief Officer Corporate Data Protection, or the relevant data protection coordinator, 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. If the data coordinator in question cannot resolve a complaint or remedy a breach of the Policy for data protection, the Chief Officer Corporate Data Protection must be brought in immediately. Decisions made by the Chief Officer Corporate Data Protection to remedy data protection breaches must be upheld 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
Intranet: http://intra.corpintra.net/cdp

DAIMLER

Optimization within Policy Project regarding volume, structure and comprehensibility

Communication Document for Policy A 17.0

Data Protection Policy Human Resources (HR)

Purpose of the policy

Motivated and dedicated employees are an important factor for value creation in the Daimler Group. Treating our employees with the respect they deserve includes safeguarding their personal rights. Daimler recognizes that its corporate responsibilities include responsible handling of personal HR data. With this Policy, Daimler is adopting a consistent, globally valid data protection and data security standard for processing employees' personal data, based on 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 HR data.

Main issues of the policy

In processing personal HR data, 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 initiating or executing an employment relationship or by virtue of consent obtained from the data subject.

Please also note the **principles** on the processing of personal HR data 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 Managament of Daimler AG
Valid from: 01.10.2009
Valdid 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