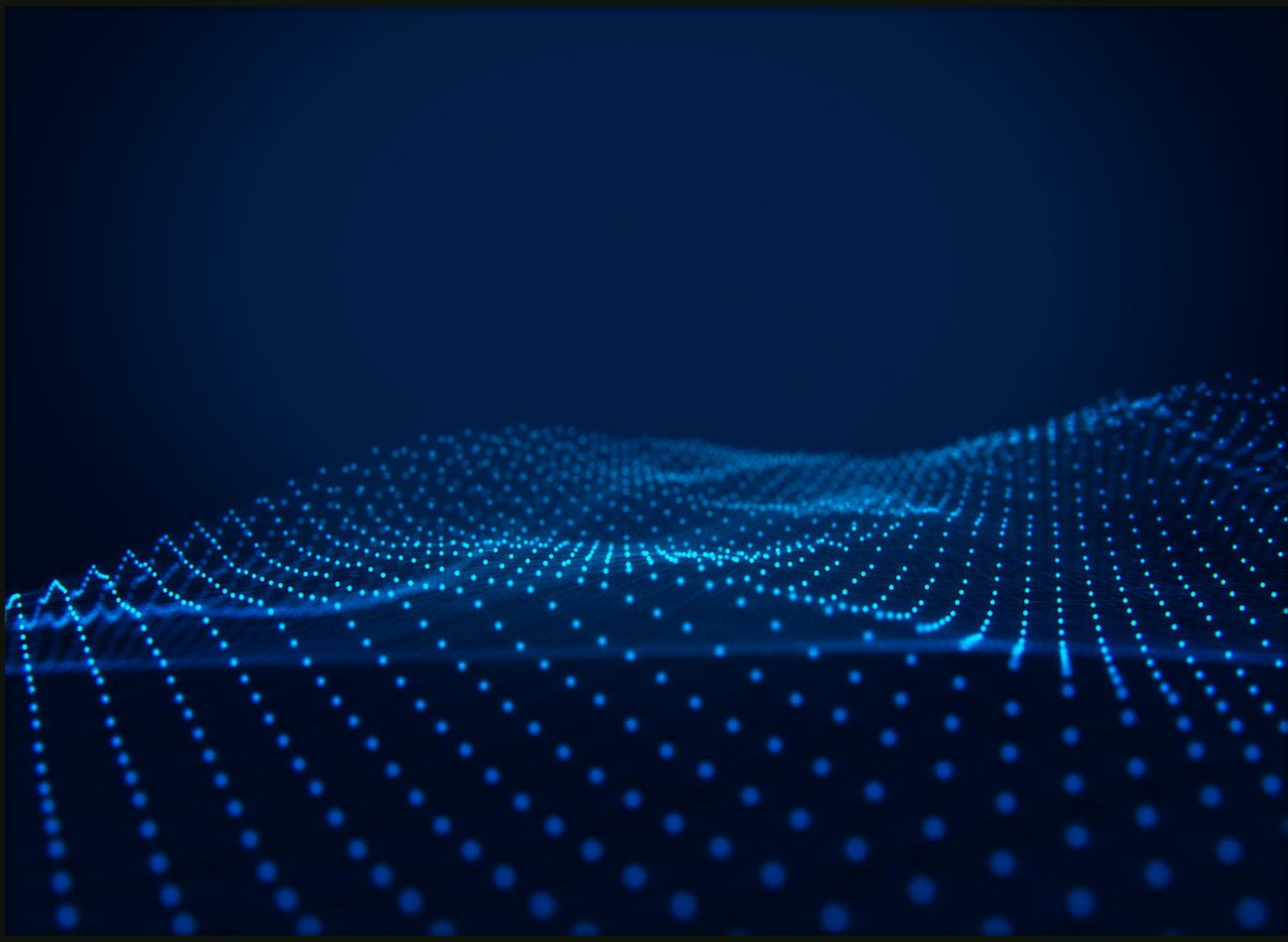

# Data Protection Policy EU

Mercedes-Benz Group

Mercedes-Benz

# Content

## 1 Aim of the Policy

The Mercedes-Benz Group considers the safeguarding of data protection rights as part of its social responsibility.

In some countries and regions, such as the European Union, legislators have defined standards for protecting the data of natural persons ("personal data"), including the requirement that such data may only be transferred to other countries if the local law applicable at the place of destination provides for an adequate level of data protection.

This Data Protection Policy EU establishes uniform and suitable data protection standards within the Group for:

- (a) processing personal data in regions such as the EU/ the European Economic Area (EEA) (hereinafter referred to collectively as the "EU/ EEA") and
- (b) cross-border transmission of personal data to Group Companies outside the EU/ EEA (including subsequent data processing there).

To this end, this Policy enacts binding rules for processing personal data from the EU/ EEA within the Mercedes-Benz Group. These rules provide adequate guarantees for the protection of personal data outside the EU/ EEA and are referred to as ("Binding Corporate Rules for Controllers – BCR-C") for the Mercedes-Benz Group.

This Policy sets out standard and binding corporate rules for processing personal data originating from the EU for the Mercedes-Benz Group, referred to as "binding corporate rules" (BCR).

## 2 Scope

This Data Protection Policy EU applies to Mercedes-Benz Group AG, its controlled Group Companies (hereinafter **Group Companies**) and its employees and members of managing bodies. "Controlled" in this instance means that Mercedes-Benz Group AG may enforces the adoption of this policy directly or indirectly, on the basis of its voting majority, majority management representation, or by agreement.

The Policy applies to fully or partially automated processing of personal data, as well as manual processing in filing systems unless national laws provide for a broader scope. The Policy also applies to all employee data[1] in hard-copy format in Germany.

The Policy applies to the processing of personal data:

[1] To make this policy easier to read, the text uses only the male forms of pronouns for natural persons. In terms of content, people of all gender identities are always intended.

- (a) from Group Companies and their subsidiaries that are established in the EU/ EEA or another country to which this Policy can be extended ("EU/ EEA-based companies"),
- (b) from Group Companies established outside the EU/ EEA, if they offer goods or services to natural persons within the EU/ EEA and/ or monitor the behavior of natural persons within the EU/ EEA ("third country companies with offers for the EU/ EEA") or
- (c) of Group Companies established outside the EU/ EEA, if they have received personal data directly or indirectly from companies that are subject to the Policy under a) or b), or if such data has been disclosed to them ("third country companies that receive data from the EU/ EEA").

Processing outside the EU/ EEA is further referred to in this Policy as processing in a third country.

The Group Companies that take part in, or are subject to, processing by third country companies are listed in the *further applicable regulation "List of Group Companies bound by the Data Protection Policy EU"*.

This Policy can be extended to countries outside the EU/ EEA. In countries where the data of legal entities is protected in the same manner as personal data, this Policy also applies in the same manner to the data of legal entities.

The Policy applies to the processing of personal data from:

- EU/EEA-based companies
- third country companies with offers for the EU/EEA
- third country companies that receive data from the EU/EEA

## 3 Legal Enforceability within the Mercedes-Benz Group

The rules and provisions of this Policy are binding to all Group Companies operating within its scope of application. In addition to the applicable EU legislation and national data protection laws, the Group Companies as well as their management and employees are therefore responsible for compliance with this Policy.
As far as it is not otherwise stipulated by legal requirements, Group Companies are not entitled to adopt regulations that deviate from this Policy.

## 4 Relationship to Legal Requirements

This Policy does not replace EU legislation and national laws. It supplements the national data protection laws. Where the national legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the Policy. The content of this Policy must also be observed in the absence of corresponding national laws.

If compliance with this Policy would result in a violation of national law, or if regulations that deviate from this Policy are required under national law, this must be reported to the Chief Officer Corporate Data Protection and the central compliance organization for the purposes of

data protection law monitoring. In the event of conflicts between national laws and this Policy, the Chief Officer Corporate Data Protection and the central compliance organization will work with the responsible Group Company to find a practical solution that fulfills the purpose of this Policy. The monitoring and reporting on the regulations in third countries is described in Section 16.

## 5 General Principles for the Processing of Personal Data

### 5.1 Lawfulness

Personal data must be processed in a lawful manner and in good faith. Data Processing may only take place if and insofar as an adequate legal basis exists for the processing activity. This also applies to data processing between Group Companies. The mere fact that both, the transferring and receiving Group Company are affiliated to Mercedes-Benz Group does not readily constitute such legal basis.

Any processing of personal data requires an adequate legal basis.

The processing of personal data is lawful if one of the following circumstances for authorization under Section 5.2 or 5.3 applies. Such circumstances for permissibility are also required if the purpose of processing the personal data is to be changed from the original purpose.

### 5.2 Legal basis Customer and Partner Data

#### 5.2.1 Data processing for a contractual relationship

Personal data of the prospective customer, customer, or partner can be processed to establish, perform and terminate a contract. This also includes advisory services for the customer or partner under the contract if this is related to the contractual purpose.

Customer and partner data can be processed to establish, perform and terminate a contract and for the contract negotiation process.

Prior to a contract, personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospective customer relating to contract conclusion. Prospective customers can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospective customers must be complied with.

#### 5.2.2 Data processing for advertising purposes

If the data subject contacts a Group Company with a request for information (e. g. request to receive information material about a product), processing of personal data to meet this request is permitted. Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed in advance about the use of his/her personal data for advertising purposes. If personal data is collected only for advertising purposes, the data subject can choose whether to provide this data. The data subject shall be informed that providing data for this purpose is

If customer and partner data is collected solely for advertising purposes, consent must be obtained from the data subject prior to the start of data processing.

voluntary. As part of the communication process, consent should be obtained from the data subject. When giving consent, the data subject should be given a choice among available forms of contact, such as e-mail and phone (consent see Section 5.2.3). If the data subject objects to the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be restricted or blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

### 5.2.3 Consent to data processing

Personal data can be processed following the consent by the data subject. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy EU. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can also be given verbally. The granting of consent must be documented.

### 5.2.4 Data processing pursuant to legal authorization or obligation

The processing of personal data is also permitted if national legislation requests, requires, or allows this. 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.

Customer and partner data may be processed in order to comply with national legislation.

### 5.2.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest. Legitimate interests are generally of a legal (e. g. collection of outstanding receivables) or commercial nature (e. g. avoiding breaches of contract). Processing cannot take place on the basis of a legitimate interest if, in a specific instance, the data subjects' interests worthy of protection outweigh the legitimate interests in processing. Before data is processed, it is necessary to determine whether there are interests worthy of protection.

Customer and partner data may be processed based on legitimate interest, unless the data subject's interests worthy of protection outweigh the legitimate interest in processing.

## 5.3 Legal Basis Employee Data

### 5.3.1 Data processing for the employment relationship

For employment relationships, personal data can be processed if needed to establish, perform and terminate the employment relationship. Personal data of candidates can be processed to help decide whether to enter into an employment relationship. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the candidate has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other Group Companies. In the existing employment relationship, data processing must always relate to the purpose of the employment

Employee data may be processed to establish, perform and terminate an employment relationship and as part of the application process.

relationship if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt – where permitted – consent must be obtained from the data subject.

A legal basis as listed below must be met to process personal data that is related to the employment relationship but was not originally part of creating, performing or terminating the employment relationship (employee data).

### 5.3.2 Data processing pursuant to legal authorization or obligation

The processing of employee data is also permitted if national legislation requests, requires, or allows this. 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 there is some legal flexibility, the protective interests of the employee must be taken into consideration.

### 5.3.3 Collective agreement on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may still be lawful if authorized through a collective agreement. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of EU and national legislation.

Employee data may be processed if authorized by a collective agreement.

### 5.3.4 Consent to data processing

Employee data can be processed upon consent of the data subject. Declarations of consent must be submitted voluntarily. No penalties can be imposed for refusal of consent. Involuntary consent is not valid. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. If, exceptionally, circumstances do not permit this, consent may be given verbally. Their granting must be in any case properly documented. Before giving consent, the data subject must be informed in accordance with this Data Protection Policy EU.

### 5.3.5 Data processing pursuant to legitimate interest

Employee data can also be processed if it is necessary for a legitimate interest of a Group Company. Legitimate interests are generally of a legal (e. g. filing, enforcing or defending against legal claims) or a commercial nature (e. g. acceleration of business processes, valuation of companies). Before data is processed, it must be determined whether there are interests worthy of protection. Personal data can be processed based on a legitimate interest if the interests worthy of protection of the employee do not outweigh the interest in processing.

Employee data may be processed based on legitimate interest, unless the data subject's interests worthy of protection outweigh the legitimate interest in processing.

Control measures that require the processing of employee data beyond performance of the employment relationship (e. g. performance checks) cannot be taken unless there is a legal obligation or justified reason to do so. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. To this end, the legitimate interests of the Group Company in performing the control measure (e. g. compliance with legal provisions and internal company rules) must be weighed against any protective interests that the employee affected by the measure may have in exclusion of the measure. The measures may only be taken if they are appropriate in the specific case. The legitimate interest of the Group Company and any interests worthy of protection of the employee must be identified and documented before any measures are taken. Moreover, any additional requirements under applicable law (e.g. rights of co-determination for the employee representatives and rights of the data subjects to obtain information) must be taken into account.

### 5.4 Processing of highly sensitive data

The processing of highly sensitive personal data must be expressly permitted or prescribed under national law. Processing of such data by the Group Company may be permitted in particular if the data subject has given his express consent, if the processing is necessary for asserting, exercising or defending legal claims with respect to the data subject or if processing is necessary for the controller to fulfill its rights and responsibilities in the area of labor and employment law. If there are plans to process highly sensitive personal data, the Chief Officer Corporate Data Protection must be informed in advance.

Legal permission or express consent from the data subject is required to process highly sensitive data.

### 5.5 Automated individual Decision Making (possibly incl. Profiling)

The data subjects can be subject to a fully automated decision that could have a legal or similarly negative impact on them only if this is necessary to conclude or perform a contract, or if the data subject has granted consent. This automated decision can include profiling in some cases, i.e. the processing of personal data that evaluates individual personality characteristics (e. g. creditworthiness). In this case, the data subject must be notified about the occurrence and outcome of an automated individual decision and be given the opportunity to have an individual review performed by a controller.

Automated individual decisions and profiling are permitted only under strict conditions.

### 5.6 Duty of Information / Transparency

The responsible department must inform the data subjects of the purposes and circumstances of the processing of their personal data in line with Articles 13 and 14 GDPR. The information must be in a concise, transparent, intelligible and easily accessible form and in clear and plain language. The requirements of the Chief Officer Corporate Data Protection and Data Compliance must be observed. This information must be given whenever the personal data is collected for

The data subject must be informed of the purposes and circumstances of the processing of their personal data.

the first time. If the Group Company receives the personal data from a third party, it must provide the information to the data subject within a reasonable period after obtaining the data, unless

- the data subject already has the information or
- it would be impossible or
- extremely difficult to provide this information.

### 5.7 Purpose Limitation

Personal data may be processed only for the legitimate purpose that was defined before collection of the data. Subsequent changes to the purpose of processing are only permissible subject to the requirement that the processing is compatible with the purposes for which the personal data was originally collected.

Personal data may be processed only for the legitimate purpose that was defined before collection of the data.

### 5.8 Data Minimization

Any processing of personal data must be limited, both quantitatively and qualitatively, to what is necessary for the achievement of the purposes for which the data is lawfully processed. This must be taken into account during the initial data collection. If the purpose permits, and the effort is in proportion to the objective pursued, anonymized or statistical data must be used.

The processing of personal data must be limited to what is necessary for achievement of the purpose for which the data is lawfully processed.

### 5.9 Accuracy of Data

The personal data stored must be objectively correct and, if necessary, up to date. Appropriate measures must be adopted to ensure that incorrect or incomplete data is deleted, corrected, supplemented or updated.

### 5.10 Privacy by Design & Privacy by Default

The principle of "Privacy by Design" aims to ensure that departments define state-of-the-art internal strategies and adopt measures to integrate data protection principles into the specifications and architecture of business models/ processes and IT systems for data processing from the very beginning during the phase of conceptualization and technical design. In accordance with the principle of "Privacy by Design," the procedures and systems for processing personal data must be designed so that their default settings are restricted to the data processing necessary to fulfill the purpose (principle of “Privacy by Default”). This includes the processing scope, storage period, and accessibility. Further measures could include:

- pseudonymization of personal data as soon as possible
- providing transparency about the functions and processing of personal data
- allowing the data subjects to decide on the processing of their personal data
- enabling the operators of procedures or systems to devise and enhance security features

Data protection principles must be integrated into the architecture of business models, processes and IT systems.

Every Group Company shall implement and maintain appropriate technical and organizational measures throughout the entire life cycle of its processing activities, in order to ensure that the above principles are complied with at all times.

### 5.11 Deletion & Anonymization

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed. This means that personal data must be deleted or anonymized as soon as the purpose of its processing has been fulfilled or otherwise lapses, unless retention obligations continue to apply. Those responsible for individual procedures must ensure the implementation of the deletion and anonymization routines for their procedures. Each system must have a manual or automated deletion routine. Deletion requests from data subjects through deletion or removal of the personal identifiers must be technically feasible in the systems. Requirements that Mercedes-Benz Group AG imposes for the performance of deletion routines (such as software tools, Handout for the implementation of deletion concepts, documentation requirements) must be observed.

Personal data may only be stored for as long as it is necessary for the purpose for which the data is being processed.

### 5.12 Security of Processing

Personal data must be protected from unauthorized access and unlawful processing or transfer, as well as from accidental loss, alteration or destruction. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing and the need to protect the data.

Technical and organizational measures must ensure the security of data processing.

The technical and organizational measures relevant to data protection must be documented by the controller in the context of the Data Protection Impact Assessment and the Record of Processing Activities.

In particular, the responsible department must consult with its Business Information Security Officer (BISO), its Information Security Officer (ISO) and its Data Protection Network. The requirements for the technical and organizational measures for protecting personal data are part of the Corporate Information Security Management and must be continuously adjusted in accordance with technical developments and organizational changes.

### 5.13 (Further) transmission

Transmission of personal data to recipients outside or inside the Group Companies is subject to the authorization requirements for processing personal data under this Section 5. The data recipient must be required to use the data only for defined purposes. Furthermore, the provisions

of Section 15 apply to the transfer of personal data from the EU/EEA to a third country.

All duties listed in this Section 5 are third party beneficiary rights for the data subject.

## 6 Data Protection Impact Assessment

Group Companies shall, when introducing new processings, or in the event of a significant change to an existing processing, particularly through the use of new technologies, assess whether this processing poses a high risk to the privacy of data subjects. The nature, scope, context and purpose of the data processing must be taken into account. As part of the risk analysis, the responsible department carries out an assessment of the impact of the planned processing on the protection of personal data (Data Protection Impact Assessment). If, even after performance of the Data Protection Impact Assessment and use of appropriate measures for risk reduction, the risk to the rights and freedoms of the data subjects remains high, the Chief Officer Corporate Data Protection has to be informed who will contact the competent data protection supervisory authority for consultation. Provisions established by Mercedes-Benz Group AG for performing this assessment (such as software tools, instructions on the performance of an evaluation) must be observed.

A Data Protection Impact Assessment evaluates the impact of the planned processing on the protection of personal data.

## 7 Documentation of Data Processing Procedures

Each Group company must document the procedures in which personal data is processed in a Record of Processing Activities. This record should be maintained in writing, including in electronic form, and should be made available to the data protection supervisory authority on request. Provisions established by Mercedes-Benz Group AG for documentation (such as software tools and instructions on documentation) must be observed.

The data processing procedures are documented in a Record of Processing Activities.

## 8 Processing on Behalf

### 8.1 General

Processing on behalf means that a contractor processes personal data as a service provider (processor) on behalf of and according to the instructions of the controller. In these cases, an agreement on processing on behalf in line with relevant statutory requirements (such as the template “Agreement on processing on behalf”), must be concluded both with external processors as well as among Group Companies within the Mercedes-Benz Group. The controller retains full responsibility for the correct performance of the data processing.

The provisions of Section 8.3. also apply to external controllers that are not Group Companies.

Processing on Behalf requires a written agreement between the data controller and the data processor.

## 8.2 Provisions for Controllers

When issuing the order, the following requirements must be complied with, whereby the department placing the order must ensure that they are met:

- The processor must be chosen based on its ability to cover the required technical and organizational protective measures.
- The contractual standards for data protection provided by the Chief Officer Corporate Data Protection must be complied with.
- The order must be placed in writing or in electronic form. The instructions on data processing and the responsibilities of the controller and processor must be documented.

Before data processing begins, the controller must confirm by suitable assessment that the processor will fulfill the aforementioned obligations. Provisions established by Mercedes-Benz Group AG on this subject (such as software tools, instructions on the performance of evaluation, template contracts) must be observed. A processor can document its compliance with data protection requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.

## 8.3 Provisions for internal Processors

The processor can process personal data only as per the controller's instructions.

Processors may engage other Group Companies or third parties ("**subcontractors**") to process personal data in their own (sub) contract only with the controller's prior consent. This consent will be granted only if the processor subjects the subcontractor – contractually or by other comparable legally binding means – to the same data protection obligations to which the processor is subject pursuant to this policy vis-a-vis the Group Company and data subjects. It must also oblige the subcontractor to take the appropriate technical and organizational protective measures. The form of consent as well as information obligations in the event of changes in the subcontracted relationship must be set out in the contract for services.

Processors are obligated to provide appropriate support to the controller in complying with data protection provisions applicable to the latter, especially by providing all the necessary information. This concerns, in particular, safeguarding

- the general principles for processing pursuant to Section 5
- the rights of data subjects pursuant to Section 10
- the notification of data protection incidents pursuant to Section 12
- the provisions for controller and processors pursuant to Section 8

- and the handling of inquiries and investigations by supervisory authorities.

If applicable standards or legal provisions require the processor to carry out the processing contrary to the controller's instructions, or if these provisions prevent the processor from meeting its obligations under this Policy or under the agreement on processing on behalf, then the processor shall immediately inform its controller unless the legal provision in question forbids such notification. This applies accordingly if the processor is unable to comply with the instructions of its controller for other reasons. In such an event, the controller has the right to suspend transmission of the data and/or to terminate the agreement on processing on behalf.

Processors are required to notify their controllers about any legally binding requests from public authorities for disclosure of personal data, unless this is prohibited for other reasons.

At the choice of the controller, processor must delete or return all personal data provided by the controller upon termination of service performance.

Processors are obligated to immediately inform their controller and, if applicable, their controller's client of any asserted claims, requests or complaints from data subjects.

Internal Group controllers also must oblige external processors to comply with the aforementioned regulations.

The specific duties of the processor to the controller are third party beneficiary rights for the data subject.

## 9 Joint Controllership

In the event that multiple Group Companies jointly define the means and purposes of processing personal data (along with one or more third parties, if applicable) (joint controllers), the companies must conclude an agreement that stipulates their duties and responsibilities to the data subject whose data they process.
The contract templates provided by the Chief Officer Corporate Data Protection must be observed.

If the means and purposes of data processing are defined jointly by multiple Group Companies, a written agreement must be concluded between the controllers.

## 10 Enforceable Rights for Data Subjects

All rights of the data subjects and obligations of the Group companies listed in this section 10 are third party beneficiary rights for the data subject.

The inquiries and complaints submitted in accordance with this Section 10 must be answered within one month. Taking into account the complexity and number of the requests, that one month period may be extended at maximum by two further months, in which case the data subject should be informed accordingly.

### 10.1 Rights of the Data Subject

A data subject in the EU/ EEA has the following rights as specified in more detail in EU law vis-à-vis the responsible Group Company or – if the Group Company is the processor – vis-à-vis the controller:

- the right to be informed of the circumstances of the processing of his personal data. The requirements of the Chief Officer Corporate Data Protection for such information must be observed.
- the right to obtain information about how his data is processed and what rights he is entitled to in this respect. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. Upon request, the data subject can receive a copy of his personal data (possibly for a reasonable fee), unless interests of third parties worthy of protection prohibit this.
- the right to correct or supplement personal data if they are incorrect or incomplete.
- the right to delete his personal data if he withdraws his consent 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 retention periods and interests worthy of protection that prohibit deletion must be observed.
- the right to restriction of processing of his data if he disputes its accuracy or if the Group Company no longer needs the data while the data subject needs the data for his legal claims. The data subject can also request that the Group Company restrict the processing of his data if it would otherwise have to delete the data or if it is reviewing an objection by the data subject.
- the right to receive the personal data relating to him, which he has provided on the basis of consent, or in the context of an agreement that was concluded or initiated with him, in a commonly used digital format. He is also entitled to transmit this data to a third party if the data is carried out by automated means and this is technically feasible.
- the right to object to direct marketing at any time. An adequate consent and objection management system must be ensured.
- the right to object to the processing of personal data that is processed on the legal basis of overriding interests of a Group Company or a third party, for reasons relating to his particular personal situation. The Group Company shall no longer process the personal data unless the Group Company has compelling

In the EU, data subjects have the following rights:
- Right to information
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to data portability
- Right to object
- Right to lodge complaints with the Chief Officer Corporate Data Protection or the competent supervisory authority
- The right to bring action before the competent court

legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. If there is a legitimate objection, the data must be deleted.

In addition, the data subject is also entitled to assert his rights against the Group Company importing the data in a third country.

### 10.2 Complaints Procedure

Data subjects are entitled to file a complaint with the Chief Officer Corporate Data Protection if they feel that this Policy has been violated. Complaints of this kind can be submitted by e-mail (see Section 13.3).

The Group Company established in the EU/ EEA that exports the data will assist data subjects whose personal data was collected in the EU/ EEA in establishing the facts and the assertion of their rights under this Policy against the Group Company that imports the data.

In case the complaint is justified, the Group Company takes adequate measures to ensure compliance with this Policy and informs the data subject about the measures taken and his further rights. In the event that the data subject is not satisfied with the reply of the Group Company or in case the complaint is rejected, the data subject is free to challenge that decision or conduct by exercising his rights and should be informed accordingly. To this end, he may apply to the competent supervisory authority, in particular in the country of his habitual residence, place of work or place of alleged infringement, or bring an action in court (see Section 11.2). Further legal rights and responsibilities shall remain unaffected. Regardless of the internal complaint procedure, data subjects are entitled to lodge a complaint directly with a supervisory authority.

## 11 Liability & Place of Jurisdiction

### 11.1 Liability Provisions

The Group company established in the EU/ EEA ("data exporter") that initially transferred the personal data to a Group company established in a third country will assume liability for each violation of this Policy by such a third country Group Company that receives data from the EU/ EEA for third-country processing. This liability includes the obligation to remedy unlawful situations as well as to compensate for material and non-material damage that was caused by a violation of this Policy by Group Companies from third countries.

The data exporter is exempt from some or all of this liability only if it can prove that the third country Group Company that receives data from the EU/ EEA is not responsible for the action that resulted in damage.

The data exporter is liable to remedy unlawful situations and to compensate for damage caused by a violation of this Policy by a third-country Group Company.

## 11.2 Place of Jurisdiction

The data subject may bring an action before the courts at the establishment of the controller or processor or at his habitual residence.

The data subject who claims an infringement of this Policy in the context of a third country processing can assert his legal claims against both the data importing and the data exporting company in the EU/ EEA. Therefore, the data subject may bring the alleged infringement and the resulting legal claims before the competent courts and regulatory authorities either at the establishment of the controller or at his habitual residence.

The provisions on liability and place of jurisdiction in this Section are third party beneficiary rights for the data subject.

## 12 Notification of Data Protection Incidents

In the event of a potential breach of the data security requirements ("data protection incident"), the Group Companies involved have investigation, information and damage mitigation obligations. A data protection incident is a personal data breach if there is a breach of security leading to the unlawful destruction, alteration, unauthorized disclosure or use of personal data. When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Group Company must, without undue delay and, where feasible, within 72 hours after the Group Company has become aware of it, inform the supervisory authority of the corresponding breach.. Furthermore, the data subjects must be notified of any personal data breach likely to result in a high risk to their rights and freedoms without undue delay. Processors as defined in Section 8.2 are obligated to report data protection incidents immediately to the controller.

Personal data breaches likely to result in a high risk to the rights and freedoms of data subjects must be reported to the competent supervisory authority and the data subjects.

If a data protection incident has been identified or suspected within a Group company's area of responsibility, all employees are required to report this immediately to Mercedes-Benz Group AG in accordance with the Information Security Incident Management Process. Requirements stipulated by Mercedes-Benz Group AG in this regard (such as software tools, instructions on reporting), must be complied with.

Any personal data breach should be documented and the documentation should be made available to the supervisory authority on request.

## 13 Data Protection Organization & Sanctions

### 13.1 Responsibility

The members of managing bodies of the Group Companies are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in this Data Protection Policy EU, for data protection are met (e. g. national reporting duties). Within their area of responsibility, management staff is responsible for ensuring that organizational, HR and technical measures are in place so that any data processing is carried out in accordance with data protection requirements. Compliance with these requirements is the responsibility of the relevant employees. If public authorities perform data protection checks, the Chief Officer Corporate Data Protection must be informed immediately.

The members of managing bodies of the Group Companies are responsible for data processing in their area of responsibility and must ensure that their employees have the required knowledge regarding data protection.

### 13.2 Awareness Raising & Training

Management must ensure that its employees receive and attend the required data protection training, including the content and handling of this Policy, if they have constant or regular access to personal data, are involved in the collection of data or in the development of tools used to process personal data. The requirements of the Chief Officer Corporate Data Protection and Data Compliance must be observed.

### 13.3 Organization

The Chief Officer Corporate Data Protection is internally independent of instructions regarding the performance of his tasks. He must ensure compliance with national and international data protection laws. He is responsible for this Policy and monitors its compliance. If Group Companies want to take part in a certification system for binding corporate rules such participation must be agreed with the Chief Officer Corporate Data Protection.

The Chief Officer Corporate Data Protection is internally independent of instructions.

The Chief Officer Corporate Data Protection is appointed by the Mercedes-Benz Group AG Board of Management and is supported by the Board of Management in fulfilling his tasks. Generally, Group Companies that are legally obligated to appoint a data protection officer will appoint the Chief Officer Corporate Data Protection. The Chief Officer Corporate Data Protection reports directly to the Board of Management of the Mercedes-Benz Group AG and of all Group Companies for which the Chief Officer Corporate Data Protection has been appointed. Specific exceptions have to be agreed upon with the Chief Officer Corporate Data Protection.

Mercedes-Benz Group AG's Supervisory Board must be informed of the annual report of the Chief Officer Corporate Data Protection as part of existing reporting duties.

All data subjects can contact the Chief Officer Corporate Data Protection at any time to express their concerns, ask questions, request

information or lodge complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

The contact information of the Chief Officer Corporate Data Protection is:
Mercedes-Benz Group AG, Chief Officer Corporate Data Protection, HPC E600, 70546 Stuttgart, Germany
Email: data.protection@mercedes-benz.com
Intranet: *https://social.intra.corpintra.net/docs/DOC-105811*

The Mercedes-Benz Group has also established a compliance organization, which is described in greater detail in separate internal regulations. The compliance organization supports and supervises the Group Companies in regard to compliance with data protection laws. It defines the content of the data protection training and stipulates the criteria for the group of participants.

The compliance organization:
- supports and supervises the Group Companies in regard to compliance with data protection laws
- defines the content of the data protection training

### 13.4 Sanctions

Unlawful processing of personal data or other offenses against data protection law can be prosecuted under regulatory and criminal law in many countries, and can also lead to claims for compensation. Breaches for which individual employees are responsible can lead to disciplinary action under employment law. Violations of this Policy will be penalized in accordance with internal regulations.

Unlawful processing of personal data can lead to claims for compensation and disciplinary action.

### 13.5 Audit and Controls

Compliance with this Policy and applicable data protection laws will be reviewed at Group level regularly, at least once a year, on a risk based approach, or on specific request from the Chief Officer Corporate Data Protection, by way of an internal compliance risk assessment, audits including on specific data protection topics and other checks. The results must be reported to the Chief Officer Corporate Data Protection, the responsible Group Company and its data protection officer if one has been appointed.

Mercedes-Benz Group AG's Board of Management must be informed of findings as part of existing reporting duties. On request, the results of the reviews will be made available to the competent data protection supervisory authority. The competent data protection supervisory authority can, as permitted under GDPR and its national law, carry out a data protection audit of any Group Company on compliance with the regulations of this Policy.

## 14 Amendments to this Policy and Cooperation with Public Authorities

### 14.1 Responsibility in the Event of Amendments

The Policy can only be changed by means of the defined procedure for amendment of policies (see Policy on Policy Management, A1) in coordination with the Chief Officer Corporate Data Protection. Changes that have significant effects on the Policy or affect the level of protection offered by the Policy (i.e. changes to the binding character) must be promptly reported to the relevant supervisory authorities via the competent supervisory authority, who issue approval of this Policy as binding corporate rules.

Changes to this Policy must be coordinated with the Chief Officer Corporate Data Protection.

The Chief Officer Corporate Data Protection keeps a fully updated list of all Group Companies that are bound by this Policy (further applicable regulation "*List of Group Companies bound by the Data Protection Policy EU*") and keeps track of and record any updates to this Policy and provides the necessary information to the data subjects or supervisory authorities upon request. On the basis of this Policy, no transfer of personal data is made to a new Group Company until the new Group Company is effectively bound by this Policy and follows the respective data compliance measures to deliver compliance.

The data subject has a right to easily access this Policy. Therefore, the latest version of this Policy will be published online at *https://www.group.mercedes-benz.com*. This requirement is a third party beneficiary right for the data subject.

If amendments are made to this Policy or the list of affiliated Group Companies, the supervisory authority of the main establishment of Mercedes-Benz Group AG will be notified of this once a year by the Chief Officer Corporate Data Protection with a brief explanation of the reasons justifying the amendment.

### 14.2 Cooperation with Authorities

Group Companies that carry out or participate in processing in third countries are obligated to cooperate with the supervisory authorities in matters concerning problems, inquiries or other procedures in connection with the processing of personal data in the context mentioned above. This encompasses the duty to accept audits by supervisory authorities, as permitted under GDPR and their national law. In addition, advices in line with GDPR from the supervisory authorities based on processing procedures in third countries or provisions of this policy shall be complied with.

The obligation to cooperate with the authorities includes:

- accept audits
- Complying with advices

The provisions of 14.2 on cooperating with the authorities are third party beneficiary rights for the data subject.

## 15 Transfer of Personal Data from the EU/ EEA to a Third Country

### 15.1 Transfer outside the Mercedes-Benz Group

Group Companies may only transfer personal data from the EU/ EEA to third parties outside of the EU/EEA (including granting access from a third country) if:

- the third country provides an adequate level of data protection recognized by the EU Commission, or
- the transfer is subject to the EU standard contractual clauses. It is the responsibility of the Group Company, if needed with the help of the third party, to assess whether the level of protection required by EU law is respected in the third country, in order to determine if the guarantees provided by the EU standard contractual clauses can be complied with in practice. If this is not the case, the third party must implement supplementary measures to ensure an essentially equivalent level of protection as provided in the EU/ EEA, or
- further appropriate safeguards as defined by Article 46 (2) of the GDPR are in place, or
- on an exceptional basis (i.e. only where it is impossible to implement the above measures), a derogation for specific situations applies (e.g. the transfer is necessary for the establishment, exercise or defence of legal claims).

### 15.2 Transfer within the Mercedes-Benz Group

Before transferring personal data to a Group Company outside of the EU/EEA, the Group Companies must assess whether the laws and practices in the third country prevent them from fulfilling their obligations under this Policy. If necessary, supplementary contractual, technical or organisational safeguards must be implemented by the Group Company in a third country to ensure an essentially equivalent level of protection as provided in the EU/ EEA.

The specific circumstances of the transfer (especially categories of data, means of transfer, further transfer to a third party) as well as the laws and practices applicable to the Group Company in the third country, including those requiring the disclosure of data to public authorities or authorising access by such authorities, must be taken into account.

The Group Companies document the assessment of Section 15.1 and 15.2 and make it available to the competent supervisory authority on request. Furthermore, the Group Companies make the assessment and the results transparent to all other Group Companies so that the identified supplementary measures could be applied in case the same type of transfers is carried out by any other Group Company or, where effective supplementary measures could not be put in place, the transfers at stake will be suspended or ended. Provisions established by Mercedes-Benz Group AG for performing this assessment (such as tools, instructions on the performance of an evaluation) must be observed

## 16 Monitoring and Reporting on the Regulations of Third Countries

Group Companies in third countries must notify the Chief Officer Corporate Data Protection immediately, if they have reasons to believe that legislation applicable to them prevents the Group Company from fulfilling their obligations under this Policy or have substantial effect on the guarantees provided by this Policy.

The Chief Officer Corporate Data Protection will evaluate the impact and will work with the responsible Group Company to find a practical solution that fulfills the purpose of this Policy. If, even after this evaluation, the relevant legal requirement is still expected to have a substantial adverse effect on the guarantees provided by this Policy, the Chief Officer Corporate Data Protection will notify the competent supervisory authority. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body, if the request has a substantial adverse effect on the guarantees provided by this Policy. The supervisory authority should be informed about the data requested, the requesting body, and the legal basis for disclosure (unless otherwise prohibited).

If a Group Company in a third-country is required by a public authority to refrain from notifying the data protection supervisory authority about the disclosure of personal data, it shall take all suitable measures to mitigate this prohibition as far as possible or to repeal it, and to annually provide general information on the requests it received to the competent supervisory authorities (e.g. number of applications for disclosure, type of data requested, requester if possible).

In any case, transfers of personal data to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

This provision is a third party beneficiary right for the data subject.

Group Companies in third countries must notify the Chief Officer Corporate Data Protection if they have reasons to believe that legislation applicable to them prevents the Group Company from fulfilling their obligations under this Policy or have substantial effect on the guarantees provided by this Policy

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