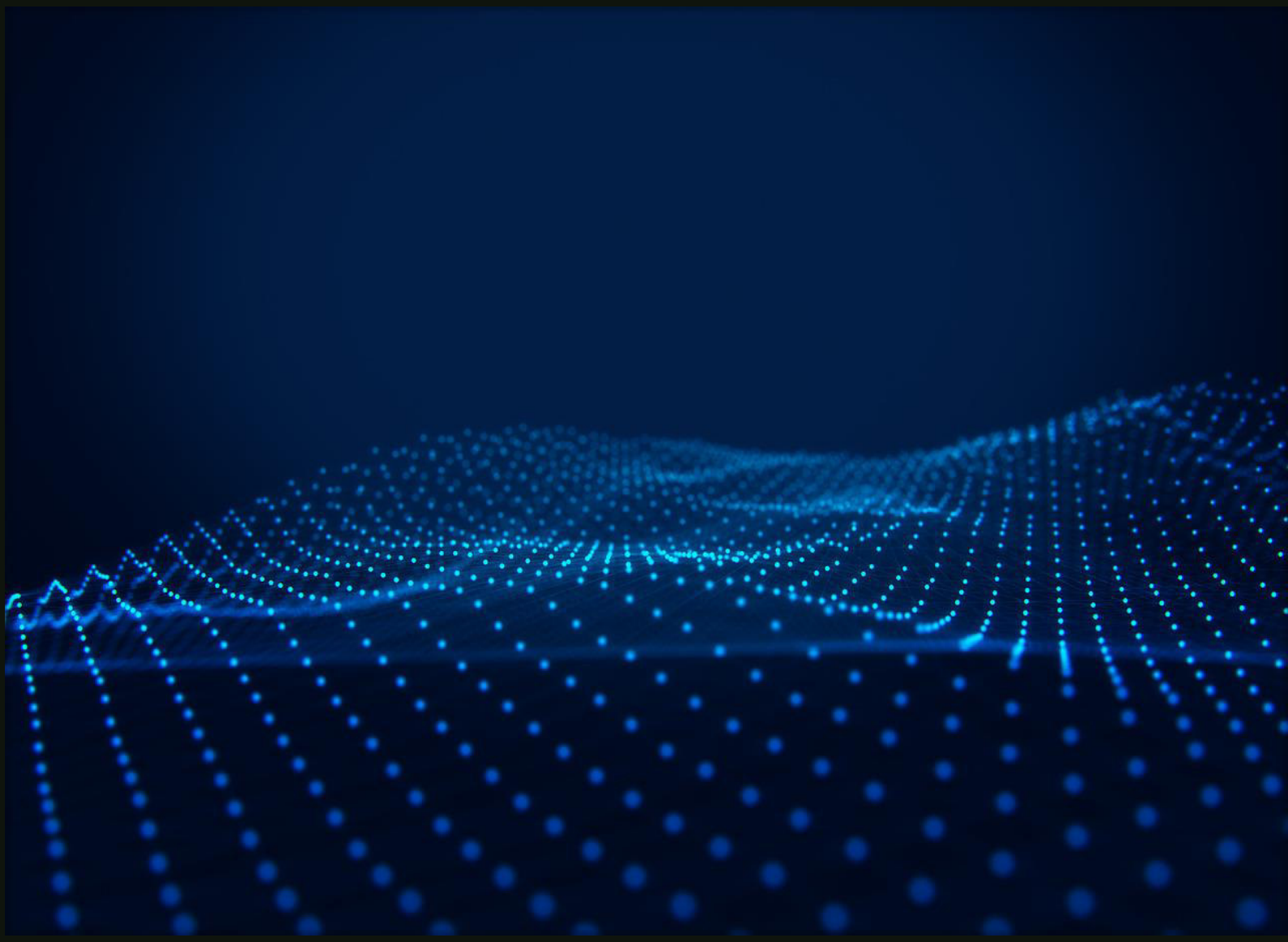

Data Protection Policy EU

Mercedes-Benz Group

Mercedes-Benz

Content

1 Objective of the Policy

The Mercedes-Benz Group includes the safeguarding of data protection rights in its commitment to social responsibility.

In some countries and regions, such as the European Union, lawmakers have defined standards for protecting the data of natural persons ("personal data"), including the condition that this data can be transferred to other countries only if an adequate level of data protection is afforded by the recipient in the destination country.

This Data Protection Policy EU establishes uniform, appropriate standards for data protection within the Group that apply to the two activities below:

- (a) Processing of personal data in regions such as the EU and the European Economic Area (EEA) (hereinafter referred to collectively as the "**EU/EEA**")
- (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. They create appropriate guarantees for the protection of personal data outside the EU/EEA and thus form so-called binding corporate rules ("Binding Corporate Rules Controller - 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 Functional scope

This Data Protection Policy applies to Mercedes-Benz Group AG, its controlled Group companies (hereinafter "**Group companies**") and its employees[1] and members of managing bodies. "Controlled" in this instance means that Mercedes-Benz Group AG may enforce the adoption of this policy directly or indirectly, on the basis of voting majority, majority management representation or by agreement.

The Policy applies to the automated and semi-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 in hard-copy format in Germany.

[1] In terms of content, this always refers to persons of all gender identities.

This Policy applies to the processing of personal data belonging to any of the following entities:

- (a) Group companies and their subsidiaries that are established within the EU/EEA or another country to which this Policy can be extended ("EU/EEA-based companies")
- (b) 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-party country companies with offers for the EU/EEA")
- (c) 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 subparagraph (a) or (b) above or if such data has been disclosed to them ("third-party country companies that receive data from the EU/EEA").

The Policy applies to the processing of personal data:

- EU/EEA-based companies
- Third-party country companies with offers for the EU/EEA
- Third-party 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-party country.

The Group companies that take part in, or are subject to, processing by third-party country companies are listed in Annex 3: *"List of Group companies subject to 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 to the same extent as personal data, this Policy applies equally to data belonging to legal entities.

3 Legally Binding Nature within the Mercedes-Benz Group

The provisions of this Policy are binding regulations for all Group companies that are active in its scope. Therefore, the Group companies, their management and their employees are responsible not only for adhering to the applicable EU regulations and national data protection laws, but also for complying with this Policy.

Group companies – subject to legal requirements – are not entitled to define regulations that deviate from this Policy.

4 Relationship to Legal Requirements

This Policy does not replace EU regulations and national laws. It complements the national data protection laws. If national laws, for example EU legislation, provide for a higher level of protection for personal data, these provisions shall take precedence over the provisions of this Policy. The content of this Policy must be observed even in the absence of corresponding national laws. Monitoring and reporting on third country regulations is described in section 16.

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 of 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 for 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.

5 General Principles for Processing 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 appropriate legal basis exists for the respective case of processing. This also applies to data processing between Group companies. The mere fact that the transferring and receiving companies both belong to the Mercedes-Benz Group is not sufficient justification for data processing.

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 pertaining to customer and partner data

5.2.1 Data processing for a contractual relationship

Personal data of the data subject (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 if they are related to the contractual purpose.

Customer and partner data may be processed to create, fulfill and terminate a contract and as part of the contract preparation 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. wishes to receive information materials on a product), data can be processed to fulfill the request. 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 their data for advertising purposes. If data 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.

collected only for advertising purposes, the data subject can choose whether to provide this data. The data subject must be informed that providing data for this purpose is voluntary. The data subject's consent must be obtained for communication purposes. When giving their consent, data subjects should be given a choice between available forms of contact, such as e-mail and phone (please see section 5.2.3 on consent). If the data subject objects to the use of their 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

Data can be processed on the basis of consent given 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 authorizes this. The type and scope of data processing must be necessary for the lawful data processing activity and must comply with these statutory provisions.

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

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 in the protection of their data outweigh the legitimate interests in processing. Before data is processed, it is necessary to determine whether there are protective interests.

Customer and partner data may be processed on the basis of a legitimate interest if it is not outweighed by the data subject's interests in the protection of their data.

5.3 Legal Basis Pertaining to Employee Data

5.3.1 Data processing for the employment relationship

Under employment relationships, personal data can be processed if needed to create, fulfill and terminate the employment. Personal data of candidates can be processed to help decide whether to enter into an employment relationship. If the candidate is rejected, their 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 an

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

existing employment relationship, data processing must always relate to the purpose of the employment 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 must be observed. In cases of doubt, consent must be obtained from the data subject whenever permitted.

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 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 lawful if requested, required or allowed by national regulations. The type and scope of data processing must be necessary for the lawful data processing activity and must comply with these 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 regulations must cover the specific purpose of the desired 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 person concerned. Declarations of consent must be submitted voluntarily. No penalties can be imposed on employees 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. In certain circumstances, consent may be given verbally. Regardless of how it is given, it must be 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 nature (e.g. filing, enforcing or defending against legal claims) or a financial nature (e.g. acceleration of business processes, valuation of companies). Before data is processed, it is important to determine in each instance whether there are protective interests. Personal data can

Employee data may be processed on the basis of a legitimate interest if it is not outweighed by the data subject's interests in the protection of their data.

be processed based on a legitimate interest if the protective interests of the employee do not outweigh the 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 legitimate interests that the employee affected by the measure may have in exclusion of the measure. The measures may be taken only if they are appropriate in the specific case. The legitimate interest of the Group company and any protective interests of the employees 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 prescribed or permitted under national law. Processing of such data by the Group company may be permitted, in particular, if the data subject has given their express consent, if 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.

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

The processing of personal data relating to criminal convictions and offenses may only take place if there is a legal basis for the respective processing activity and if EU law or the legal provisions applicable to the Group company permit this processing.

If there are plans to process highly sensitive personal data, the Chief Officer for Corporate Data Protection must be informed in advance.

5.5 Automated individual decision making (if applicable, including profiling)

Data subjects may be subjected to fully automated decisions that could have a legal or similarly negative impact on them only if they are necessary to conclude or perform an agreement, 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 (such as 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 and 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 of the GDPR. The information must be provided in a concise, transparent, intelligible and easily accessible form and in clear and plain language. The requirements of the Chief Officer for Corporate Data Protection and of the Data Compliance Department must be observed. This information must be given whenever the personal data is collected for 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 any of the following criteria are met:

- The data subjects already possess the information.
- It is impossible to provide the information.
- It would require unreasonable time and effort to provide the information.

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

5.7 Limitation of purpose

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

Each instance of processing of personal data must be configured such that it is quantitatively and qualitatively limited to the degree necessary for the achievement of the purposes for which the data is lawfully processed. This must be factored into the scope of data collection. If the purpose permits and the work involved is reasonable for the respective goal, anonymized or statistical data must be used.

The processing of personal data must be limited to the degree necessary for the achievement of these purposes.

5.9 Accuracy of data

The stored personal data must be factually correct and, if necessary, up to date. The responsible department must take appropriate measures to ensure that incorrect or incomplete data is deleted, corrected, added or updated.

5.10 Privacy by design and privacy by default

The principle of "privacy by design" aims to ensure that specialist units 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

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

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. Additional measures can include the following:

- Subjecting personal data to pseudonymization 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

Every Group company must introduce suitable technical and organizational measures throughout the entire life cycle of its data processing procedures and implement these in order to ensure that the above principles are complied with at all times.

5.11 Deletion and anonymization

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

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. The persons 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 after deletion or removal of the personal identifiers must be technically feasible in the systems. Provisions established by Mercedes-Benz Group AG concerning the implementation of deletion routines (e.g. software tools, the handout on executing deletion requirements and documentation requirements) must be adhered to.

5.12 Security of processing

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

Personal data must be protected from unauthorized access and unlawful processing or transfer as well as from accidental loss, modification 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.

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 specialist unit should consult with its Business Information Security Officer (BISO), its Information Security

Officer (ISO) and its data protection network. The requirements placed on the technical and organizational measures for protecting personal data are part of 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 the defined purposes. Furthermore, Section 15 applies to the transfer of personal data from the EU/EEA to a third-party country.

All duties listed in this Section 5 establish the data subjects as third-party beneficiaries.

6 Data Protection Impact Assessment

When introducing new processing activities or in the event of a significant change to an existing processing activity, particularly through the use of new technologies, Group companies shall assess whether the processing activity poses a high risk to the privacy of data subjects. The assessment must be performed before processing begins. The nature, scope, context and purpose of the data processing must be taken into account. As part of the risk evaluation, the responsible specialist unit carries out an assessment of the effects of the planned instances of processing on the protection of personal data (data protection impact assessment). If, 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 for Corporate Data Protection must be informed so that they can contact the competent data protection supervisory authority for consultation. Provisions established by Mercedes-Benz Group AG for performing this assessment (software tools, instructions on the performance of an evaluation, etc.) must be observed.

A data protection impact assessment evaluates the consequences the planned processing will have on the protection of personal data.

7 Documentation of Data Processing Procedures

Every Group company is required to document procedures in which personal data is processed in a record of processing activities. The record of processing activities must be maintained in writing, which can be done in electronic format, and made available to the data protection supervisory authority upon request. Provisions for documentation established by Mercedes-Benz Group AG (software tools and instructions on documentation) must be observed.

The data processing procedures are documented using the record of processing activities.

8 Data Processing on Behalf of the Company

8.1 General

Data processing on behalf means that a service provider processes personal data on behalf of and according to the instructions of the client. In these cases, an agreement on processing on behalf of the company 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 between Group companies within the Mercedes-Benz Group. The client retains full responsibility for the correct performance of the data processing.

The provisions of Section 8.3. also apply to third-party clients that are not Group companies.

An agreement in writing between the client and provider is required for data processing by a contractor.

8.2 Provisions for controllers

The following requirements must be met when awarding a contract to a processor, with the department placing the order required to ensure 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 for Corporate Data Protection must be complied with.
- The contract with the processor must be issued in written or electronic form. The instructions on data processing and the responsibilities of the client and processor must be documented.

Before data processing begins, the client must perform sufficient checks to verify that the processor will fulfill the above 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. Relevant certification of the provider is a primary method of documenting its compliance with data protection requirements. Depending on the risk posed by data processing, evaluations must be repeated on a regular basis during the term of the contract.

8.3 Provisions for internal Group processors

The provider can process personal data only as per the instructions from the client.

Processors may hire other Group companies or third parties ("**subcontractors**") to process personal data on their own (subordinated) behalf only with prior consent from the controller. This consent is granted only if the contractor subjects the subcontractor – contractually or by other comparable legally binding means – to the same data protection obligations to which the contractor is subject pursuant to this policy vis-a-vis the Group company and data subjects, as well as to appropriate technical and organizational protective measures. The form

of consent and 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, in particular by providing all information necessary. Such information shall, in particular, concern the safeguarding of the following:

- General principles of processing pursuant to section 5
- Rights of data subjects pursuant to section 10
- Controller's reporting obligations pursuant to section 12
- Provisions pertaining to controllers and processors pursuant to section 8
- Handling of inquiries and investigations by supervisory authorities

If applicable standards or legal provisions stipulate that the provider carry out processing in a manner contrary to instructions, or if these provisions prevent the provider from meeting its obligations under this Policy or under the data processing agreement, then the provider shall immediately inform its client 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 for data processing.

Providers are required to notify their clients about all legally binding requests from government agencies for disclosure of personal data unless this is prohibited for other reasons.

According to the choice of the client, providers must delete or return all personal data provided by the client upon termination of service performance.

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

Internal Group clients must also oblige third-party providers to comply with the above regulations.

The specific duties of the provider to the client establish the data subjects as third-party beneficiaries.

9 Joint Controllership

In the event that multiple Group companies jointly specify the means and purposes for processing personal data (together with one or more third parties, if applicable) (collectively referred to as "joint controllers"), the companies are required to conclude an agreement that specifies their duties and responsibilities toward the data subjects whose data they process. The contract templates provided by the Chief Officer for Corporate Data Protection must be used for that purpose.

If the means and purposes of data processing are defined jointly by multiple Group companies, an agreement in writing must be concluded by the controllers for such "joint controllership."

10 Rights Enforceable by Data Subjects

All rights of data subjects and obligations of Group companies listed in this section 10 establish data subjects as third-party beneficiaries.

Any 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, the one-month period may be extended at maximum by two additional months, in which case the data subject must be informed accordingly.

10.1 Rights of data subjects

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 processing for their personal data The requirements of the Chief Officer of Corporate Data Protection for such information must be observed.
- The right to obtain information about how their data is being processed and what associated rights they have. This is without prejudice to any specific rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws. Upon request, data subjects can receive a copy of their personal data (for a reasonable fee, if applicable) unless legitimate interests of third parties prohibit doing so.
- The right to have personal data corrected or added if it is incorrect or incomplete
- The right to have their data deleted if they withdraw their consent or the legal basis for processing does not exist or ceases to apply. The same applies if the purpose behind the data processing has lapsed or has ceased to be applicable for other reasons. Existing retention periods and protective interests that prohibit deletion must be observed.
- The right to restriction of processing of their data if they dispute its accuracy or if the Group Company no longer needs the data while the data subjects need the data for their legal claims. Data subjects can also request that the Group company restrict the processing of their data if it would otherwise have to delete the data or if it is reviewing an objection by the data subject.

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 of objection
- Right to lodge complaints with the Chief Officer of Corporate Data Protection or the competent supervisory authority

- The right to receive the personal data relating to them, which they have provided on the basis of consent, or in the context of an agreement that was concluded or initiated with them, in a commonly used digital format. They are also entitled to transmit the data to a third party if the data is processed by automated means and this is technically feasible.
- The right to object to direct marketing at any time. It is important to ensure an adequate consent and objection management system.
- 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 their particular personal situation. The Group company shall no longer process the personal data unless it has compelling legitimate grounds for processing that outweigh the interests, rights and freedoms of the data subject or if the processing is required to assert, exercise or defend against legal claims. If there is a legitimate objection, the data must be deleted.

In addition, data subjects are also entitled to assert their rights against the Group company importing the data in a third-party country.

10.2 Complaint procedure

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

A 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.

If the complaint is justified, the Group company will take appropriate measures to ensure compliance with this policy and inform the data subject of the measures taken and their further rights. In the event that the data subject is not satisfied with the response of the Group Company or the complaint is rejected, the data subject is free to challenge this decision or behavior by exercising their rights and should be informed accordingly. To that end, the data subject may contact the competent supervisory authority – in particular, in the country of their habitual residence, place of work or place of alleged infringement – or bring an action in court (section 11.2).This is without prejudice to further legal rights and responsibilities. Irrespective of this internal complaints process, data subjects have the right to lodge a complaint directly with a supervisory authority.

11 Liability and 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-party country will assume liability for any violation of this Policy by such a third-party country Group company that receives data from the EU/EEA for third-party country processing. This liability includes the obligation to remedy unlawful situations and to compensate for tangible and intangible damage that was caused by a violation of this Policy by Group companies from third-party countries.

The data exporter is liable for paying compensation and for remedying policy violations caused by a third-country company.

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

11.2 Place of jurisdiction

Data subjects may bring an action before the courts at the establishment of the controller or processor or at their habitual residence.

Disputes relating to instructions from the competent supervisory authority regarding compliance with the provisions of this Policy shall be subject to the jurisdiction of the competent supervisory authority. The Group companies are subject to this jurisdiction.

Data subjects who claim an infringement of this Policy in the context of third-party country processing can assert their legal claims against both the data-importing and the data-exporting company in the EU/EEA. Therefore, data subjects 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 their habitual residence.

12 The provisions on liability and place of jurisdiction in this section establish data subjects as third-party beneficiaries.Reporting 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 or alteration or unauthorized disclosure or use of personal data. If the personal data breach is likely to pose a risk to the rights and freedoms of natural persons, the Group company must inform the supervisory authority of the breach without delay and, if possible, within 72 hours of the Group

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.

company becoming aware of the breach. In addition, data subjects must be notified immediately in the event of a data breach that is likely to pose a high risk to their rights and freedoms. Processors as defined in section 8.2 are obligated to report data protection incidents immediately to the controller.

If a data breach has been identified or is suspected within a Group company's area of responsibility, every employee is obliged to report this immediately to Mercedes-Benz Group AG as part of 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.

Every personal data breach must be documented, and the documentation must be made available to the supervisory authority on request.

13 Data Protection Organization and Penalties

13.1 Responsibility

The members of managing bodies of the Group Companies are responsible for data processing in their areas of responsibility. Therefore, they are required to ensure that the data protection requirements stipulated by law and those contained in this Data Protection Policy EU are met (e.g. national reporting duties). It is the duty of every member of management staff, within their areas of responsibility, to ensure 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 government agencies perform data protection checks, the Chief Officer of Corporate Data Protection must be informed immediately.

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

13.2 Raising awareness and training

Management must ensure that its employees receive and attend the required data protection courses, including those on the content and handling of this Policy, if they have constant or frequent access to personal data, are involved in the collection of data or are involved in the development of tools used to process personal data. The mandatory data protection training courses must be completed by employees every 3 years. The guidelines of the Group Data Protection Officer must be observed.

13.3 Organization

The Chief Officer for Corporate Data Protection is internally independent of instructions regarding the performance of their tasks. He must ensure compliance with national and international data protection laws. He is responsible for this Policy and monitors compliance with the

The Chief Officer of Corporate Data Protection is not subject to instructions.

same. If Group Companies wish to take part in a certification system for binding corporate rules, such participation must be agreed with the Chief Officer for Corporate Data Protection.

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

Under reporting obligations, the Supervisory Board of Mercedes-Benz Group AG must be informed about the annual report of the Chief Officer for Corporate Data Protection.

All data subjects can contact the Chief Officer for 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 details for the Chief Officer for Corporate Data Protection are as follows:

Mercedes-Benz Group AG, Group Data Protection Officer, HPC W079,
70546 Stuttgart, Germany
E-mail: *data.protection@mercedes-benz.com*
Intranet: *https://social.intra.corpintra.net/docs/DOC-71499*

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 courses 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
- Designs the data protection training courses.

13.4 Penalties

Unlawful processing of personal data or other violations of data protection laws are subject to prosecution under the regulatory and criminal laws of many countries and may also result in 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.

Data protection offenses can lead to claims for compensation and to measures under employment law.

13.5 Audits and controls

Compliance with this Policy and applicable data protection laws will be reviewed at Group level regularly – at least once a year – in a risk-based approach. This shall be carried out by means of an internal compliance risk assessment, audits – including those covering specific data protection issues – and other controls. The Chief Officer for Corporate Data Protection also has the right to demand additional assessments. The results must be reported to the Chief Officer for Corporate Data Protection, the responsible Group company and its data protection officer if one has been appointed.

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

14 Amendments to this Policy and Cooperation with Government Agencies

14.1 Responsibility for amendments

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

The Policy can only be changed by means of the defined procedure for amendment of policies (*Policy on Policy Management, A 1*) in coordination with the Chief Officer for Corporate Data Protection. Amendments that have a significant impact on this Policy or could interfere with the level of protection granted (i. e. changes in binding nature) must be reported immediately to the relevant supervisory authorities via the competent supervisory authority, which will grant approval of this Policy as a binding corporate rule.

The Group Data Protection Officer maintains an updated list of all Group companies that are bound by this Policy (Annex 3: *List of Group companies bound by the Data Protection Policy EU*) and tracks and records all updates to this Policy and informs those affected. All necessary information will be made available to the supervisory authorities on request. On the basis of this Policy, no transfer of personal data will be 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 ensure adherence to the Policy.

Data subjects have the right to easily access this Policy. Therefore, the latest version of this Policy will be published online at *https://www.group.mercedes-benz.com* under the "Data Protection" section. This requirement establishes data subjects as third-party beneficiaries.

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 for 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-party countries are obliged to cooperate with the supervisory authority in the event of problems, inquiries or other procedures relating to the processing of personal data in the above-mentioned context. This includes the obligation to accept audits by the supervisory authorities, insofar as this is permitted under the GDPR and their national law. In addition, all GDPR-compliant instructions from the supervisory authorities based on or relating to processing procedures in third-party countries or provisions of this Policy shall be complied with.

The provisions of section 14.2 on cooperating with the authorities establish data subjects as third-party beneficiaries.

The obligation to cooperate with the authorities includes:
- Accepting audits
- Complying with instructions

15 Transfer of personal data from the EU/EEA to a third-party country

15.1 Transmission outside the Mercedes-Benz Group

Group companies may only transfer personal data from the EU/EEA to third parties outside the EU/EEA (including access from a third-party country) if:

- The third-party country offers 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 necessary with the help of the third party, to assess whether the level of protection required by EU law is complied with in the third-party country in order to decide whether 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 take additional measures to ensure an essentially equivalent level of protection as provided for in the EU/EEA, or
- other appropriate safeguards as defined by Art. 46 (2) GDPR are available, or
- exceptionally (i.e. only if the above measures cannot be implemented), an exception applies for certain cases (e.g. the transfer is necessary for the establishment, exercise or defense of legal claims).

15.2 Transmission within the Mercedes-Benz Group

Before transferring personal data to a Group company outside the EU/EEA, Group companies must check whether the laws and practices in

the third-party country prevent them from fulfilling their obligations under this Policy. If necessary, the Group company in the third-party country must implement additional contractual, technical or organizational safeguards to ensure a level of protection that is essentially equivalent to that provided in the EU/EEA.

The specific circumstances of the transfer (in particular data categories, purposes, type of transfer, disclosure to a third party, places of data processing and storage, companies involved) as well as the legal provisions and practices applicable to the Group company in the third-party country, including those that require the disclosure of data to authorities or allow authorities access to this data, must be taken into account.

The Group companies shall document the assessment of sections 15.1 and 15.2 and make them available to the competent supervisory authority upon request. Furthermore, the Group companies make the assessment and the results transparent to all other Group companies so that, for the same types of transmissions by other Group companies, the identified supplementary measures can be implemented or, if no effective supplementary measures could be taken, the transmission must be suspended or terminated within one month. The transferred personal data must be returned or deleted. Provisions established by Mercedes-Benz Group AG for carrying out this assessment (such as tools, instructions on the performance of evaluation) must be observed. Other supplementary measures must be agreed with the data exporter and the Group Data Protection Officer.

The transferred personal data must also be returned or deleted if the transfer has been terminated, the Group company processing the data violates the provisions of this Policy or fails to comply with a binding decision of the competent supervisory authority or a court. The same obligation also applies to all copies of personal data.

16 Monitoring and reporting on the regulations in third-party countries

Group companies in third countries must notify the Group Data Protection Officer immediately if there is reason to believe that the legislation applicable to them prevents the Group companies from fulfilling their obligations under this Policy or has a significant impact on the safeguards provided for in this Policy.

The Group Data Protection Officer will assess the impact and work with the responsible Group company to find a practical solution that fulfills the purpose of this Policy. If, even after this assessment, it is considered that the relevant legal requirement has a significant adverse impact on the safeguards provided for in this Policy, the Group Data Protection Officer will notify the competent supervisory authority. This

shall include legally binding requests for disclosure of personal data by a law enforcement authority or a national security authority if such requests have a significant adverse impact on the safeguards provided for in this Policy. The supervisory authority should be informed of the data requested, the requesting authority and the legal basis for disclosure (unless otherwise prohibited).

If a Group company in a third-party country is obliged by a legally binding request from a public authority to disclose EU personal data or if the Group company becomes aware of access to such data by public authorities, it will examine the legal admissibility and any options for legal redress. The EU personal data may only be released once any existing legal remedy has been exhausted. The legal assessment and the corresponding procedure must be documented.

The Group company in the third-party country informs the data exporter and, where possible, the data subjects, about official requests and access by authorities to EU personal data in the third-party country. In the case of official requests, the requested data, the legal basis for the disclosure and the feedback (unless otherwise prohibited) must be communicated.
If a Group company in a third-party country is required by a public authority to refrain from disclosing EU personal data to the data exporter or the data subjects , it shall make every reasonable effort to mitigate or lift this prohibition as far as possible. Within this scope of action, the data exporter must be provided annually with general information on the requests received (e.g. number of requests for disclosure, type of data requested, requesting body where possible). These requests must be submitted to the competent supervisory authority upon request.

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 establishes data subjects as third-party beneficiaries.

Adequate level of data protection	Exists in principle for data transmission within the EU/the EEA. Apart from the exceptions defined in the EU GDPR, personal data can be transmitted to a country outside the EU/EEA only if the EU Commission has recognized the appropriateness of the data protection level in the third-party country or other suitable guarantees have been provided. With the Data Protection Policy EU as a so-called Binding Corporate Rule, the Mercedes-Benz Group ensures that appropriate guarantees are in place for transmitting personal data in-house from Group companies in the EU/EEA to Group companies outside the EU/EEA.
Article 46 (2) GDPR	This contains appropriate safeguards for transmitting personal data to third-party countries, e.g: • a legally binding and enforceable document between the authorities or public bodies • standard data protection clauses adopted by a supervisory authority and approved by the EU Commission • approved rules of conduct • approved certification mechanism It is the responsibility of the Group company, if necessary with the help of the third party, to assess whether the level of protection required by EU law is complied with in the third-party country in order to decide whether these appropriate safeguards can be complied with in practice. If this is not the case, the third party must take additional measures to ensure an essentially equivalent level of protection as provided for in the EU/EEA.
Anonymized	In reference to data, this means that a specific person can no longer be identified and no one can recover this identification or that the person could be identified only by investing a great deal of time, expense and capacity.
Supervisory authority, data protection supervisory authority	An independent government agency based in the EU/EEA.
Contractor	A natural person or legal entity who/that processes personal data on behalf of the controller.
Exception for certain cases	This allows a group company, as an exception, to transfer personal data from the EU/EEA to third parties outside the EU/EEA if one of the following conditions is met: • the data subject has expressly consented to the proposed data transfer • the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures at the request of the data subject • the transfer is necessary for the conclusion or performance of a contract concluded by the controller with another natural or legal person in the interest of the data subject • the transfer is necessary for important reasons of public interest • the transfer is necessary to assert, exercise or defend legal claims

	• the transfer is necessary to protect the vital interests of the data subject or other persons if the data subject is physically or legally incapable of giving consent.
Binding Corporate Rules Controller (BCR-C)	A suitable framework for the transfer of personal data from Group companies based in the EU/EEA, which process personal data as a controller, to Group companies based outside the EU/EEA, which process personal data as a controller or processor. They apply only within the Mercedes-Benz Group and must be legally binding for, and enforced at, every relevant Group company.
Highly sensitive data	Data on racial and ethnic background, political opinions, religious or ideological beliefs, union membership, genetic and biometric data, health data, data on sexual life or sexual orientation of the data subject or data on criminal convictions and criminal offenses. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently.
Data subject	Under this Data Protection Policy EU, means any natural person whose data is processed. In some countries, legal entities can be data subjects as well.
Data exporter	A Group company based in the EU/EEA that transfers personal data to a Group company based in a third-party country.
Data Protection Network	Includes the Local Compliance Officers (LCOs), Local Compliance Responsibles (LCR) and the appropriate communicators.
Data protection breach	A violation of data security that results in the unlawful deletion, modification, unauthorized disclosure or use of personal data.
Incident	A violation of information security with a suspected data breach.
Third-party beneficiaries	Data subjects permitted by regulations to directly enforce claims under the Data Protection Policy EU against the Group companies that process data, even if these persons do not have a direct legal relationship to them and the Group companies violate their obligations under the Data Protection Policy EU.
Third party	Anyone who processes personal data, but is not a data subject or a controller. Processors within the EU/EEA are not considered third parties under the EU-GDPR because they are assigned to the controller by law.
Outside countries	All countries outside the EU/EEA.
GDPR	Abbreviation for the EU's General Data Protection Regulation, officially titled "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC."
Consent	A voluntary, legally binding statement that the data subject agrees to data processing. It is issued by the data subject expressly before data processing commences.

European Economic Area (EEA)	An economic area associated with the EU, Norway, Iceland and Liechtenstein.
Applicable legislation	Binding provisions that relate both to the law of the Member States and to the law of third countries.
Prospective customers	Persons who are interested in products or services from one or more Group companies.
Collective agreements	Pay-scale agreements or agreements between employers and employee representatives within the scope allowed under the relevant employment law (such as works agreements).
Employee data	Data from Mercedes-Benz Group employees and also candidates for an employment relationship as well as persons whose employment relationships have ended if the data relates to the inactive employment relationship.
National law, national laws	Refers to the law of the Member States. In point 4 (Relationship to legal requirements), the phrase "national law" refers to the law of the Member States or the law of third countries.
Personal data	All information that relates to an identified or identifiable person. A natural person is considered "identifiable" if they can be identified directly or indirectly, particularly by matching them to a name, an ID number, location data, an online user name or one or more special characteristics that express the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person. It can also suffice if the personal identification can be made by combining information with additional knowledge (even facts that are incidentally known).
Pseudonymized	In reference to data, this means that without using additional information, it can no longer be used to identify a specific data subject – provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.
Processing of personal data	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data controller	Any natural person or legal entity that decides alone or with others about the purposes and methods of processing personal data.
Compatible	This refers to the compatibility test. In assessing whether processing for a purpose other than that for which the personal data were originally collected is compatible, the controller shall take into account the following criteria: • any link between the purposes for which the personal data have been collected and the purposes of the intended further processing,

	• the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller, • the type of personal data, in particular whether special categories of personal data are processed or whether personal data relating to criminal convictions and offenses are processed, • the possible consequences of the intended further processing for the data subjects,
Agreement on contract processing	A contract or other legal instrument under Union or Member State law that binds the processor in relation to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller.
Record of processing activities	A list of the procedures from a controller that processes personal data. This list contains all the following information: • The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and any data protection officer • Purposes of processing • A description of the categories of data subjects and the categories of personal data • The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations • Where applicable, transfers of personal data to a third-party country or to an international organization, including the identification of the third-party country or international organization concerned • If possible, the envisaged time limits for erasure of the different categories of data • If possible, a general description of the technical and organizational measures.
Reasonable	Measures that are suitable, required and appropriate for achieving a legitimate purpose. Measures are suitable if the legitimate purchase can be achieved – or at least assisted – with this measure. Measures are required if there are no lesser means of achieving the same success with equal certainty. Measures are appropriate if they are not unduly burdensome or unreasonable for the data subject.
Competent supervisory authority	Any supervisory authority entrusted with the performance of the tasks and exercise of the powers conferred on it by the General Data Protection Regulation in the respective Member State.

Annex 3: List of Group companies subject to the Data Protection Policy EU

Entity	Country	City
Accumotive GmbH & Co. KG	Germany	Kamenz
Accumotive Verwaltungs-GmbH	Germany	Kamenz
AEG Olympia Office GmbH	Germany	Stuttgart
Affalterbach Racing GmbH	Germany	Affalterbach
Anota Fahrzeug Service- und Vertriebsgesellschaft mbH	Germany	Berlin
Athlon Car Lease Belgium N.V.	Belgium	Machelen
Athlon Car Lease International B.V.	Netherlands	Almere
Athlon Car Lease Italy S.R.L.	Italy	Rome
Athlon Car Lease Nederland B.V.	Netherlands	Almere
Athlon Car Lease Polska Sp. z o.o.	Poland	Warsaw
Athlon Car Lease Portugal, lda	Portugal	Sintra
Athlon Car Lease Rental Services B.V.	Netherlands	Almere
Athlon Car Lease Rental Services Belgium N.V.	Belgium	Machelen
Athlon Car Lease S.A.S.	France	Le Bourget
Athlon Car Lease Spain, S.A.	Spain	Barcelona
Athlon France S.A.S.	France	Le Bourget
Athlon Germany GmbH	Germany	Düsseldorf
Athlon Mobility Consultancy N.V.	Belgium	Machelen
Athlon Mobility Services UK Limited	United Kingdom	Milton Keynes
Athlon Rental Germany GmbH	Germany	Düsseldorf
CARS Technik & Logistik GmbH	Germany	Wiedemar
Cúspide GmbH	Germany	Stuttgart
Daimler Fleet Management South Africa (Pty.) Ltd. i. L.	South Africa	Pretoria
Daimler Vans USA, LLC	USA	Sandy Springs GA
EHG Elektroholding GmbH	Germany	Stuttgart

Epsilon Mercedes-Benz Grundstücksverwaltung GmbH & Co. OHG	Germany	Schönefeld
Friesland Lease B.V.	Netherlands	Drachten
Interleasing Luxembourg S.A.	Luxembourg	Windhof
Koppieview Property (Pty) Ltd	South Africa	Pretoria
Lapland Car Test Aktiebolag	Sweden	Arvidsjaur
LEONIE DMS DVB GmbH	Germany	Stuttgart
Li-Tec Battery GmbH	Germany	Kamenz
MBarc Credit Canada Inc.	Canada	Mississauga ON
MBition GmbH	Germany	Berlin
MBition Sofia EOOD	Bulgaria	Sofia
MDC Power GmbH	Germany	Kölleda
Mercedes AMG High Performance Powertrains Ltd	United Kingdom	Brixworth Northamptonshire
Mercedes pay GmbH	Germany	Stuttgart
Mercedes pay USA LLC	USA	Farmington Hills
Mercedes-AMG GmbH	Germany	Stuttgart
Mercedes-Benz - Aluguer de Veículos, Lda.	Portugal	Mem Martins
Mercedes-Benz (Beijing) Parts Trading and Services Co., Ltd.	China	Beijing
Mercedes-Benz (China) Ltd.	China	Beijing
Mercedes-Benz (Thailand) Limited	Thailand	Bangkok
Mercedes-Benz AG	Germany	Stuttgart
Mercedes-Benz Asia GmbH	Germany	Stuttgart
Mercedes-Benz Assignment Services Americas, LLC	USA	Farmington Hills MI
Mercedes-Benz Assuradeuren B.V.	Netherlands	Utrecht
Mercedes-Benz Australia/Pacific Pty Ltd	Australia	Mulgrave VIC
Mercedes-Benz Auto Finance Ltd.	China	Beijing
Mercedes-Benz Automotive Mobility GmbH	Germany	Berlin
Mercedes-Benz Bank AG	Germany	Stuttgart

Annex 3: List of Group companies subject to the Data Protection Policy EU

Mercedes-Benz Bank Service Center GmbH	Germany	Berlin
Mercedes-Benz Banking Service GmbH	Germany	Saarbrücken
Mercedes-Benz Belgium Luxembourg S.A.	Belgium	Brüssel
Mercedes-Benz Broker Biztositási Alkusz Hungary Kft.	Hungary	Budapest
Mercedes-Benz Brooklands Limited	United Kingdom	Milton Keynes
Mercedes-Benz Business Services Sdn Bhd	Malaysia	Puchong
Mercedes-Benz Canada Inc.	Canada	Mississauga ON
Mercedes-Benz Capital Investments B.V.	Netherlands	Utrecht
Mercedes-Benz Cars & Vans Brasil Ltda.	Brazil	São Paulo - SP
Mercedes-Benz Cars Middle East FZE	United Arab Emirates	Dubai
Mercedes-Benz Ceská republika s.r.o.	Czech Republic	Prague
Mercedes-Benz Connectivity Services GmbH	Germany	Stuttgart
Mercedes-Benz Consulting GmbH	Germany	Leinfelden-Echterdingen
Mercedes-Benz Corporate Investments, LLC	USA	Farmington Hills MI
Mercedes-Benz Credit Pénzügyi Szolgáltató Hungary Zrt.	Hungary	Budapest
Mercedes-Benz Customer Assistance Center Maastricht N.V.	Netherlands	Maastricht
Mercedes-Benz Customer Solutions GmbH	Germany	Stuttgart
Mercedes-Benz Danmark A/S	Denmark	Copenhagen
Mercedes-Benz Digital Tech Ltd.	China	Shanghai
Mercedes-Benz Distribution Vietnam Company Limited	Vietnam	Ho Chi Minh City
Mercedes-Benz Egypt S.A.E.	Egypt	New Cairo
Mercedes-Benz Energy GmbH	Germany	Großröhrsdorf
Mercedes-Benz Espana, S.A.U.	Spain	Alcobendas
Mercedes-Benz ExTra LLC	USA	Vance AL
Mercedes-Benz Finance Canada Inc.	Canada	Montreal QC
Mercedes-Benz Finance Co., Ltd.	Japan	Chiba

Mercedes-Benz Finance North America LLC	USA	Farmington Hills MI
Mercedes-Benz Financial Services Australia Pty. Ltd.	Australia	Mount Waverly VIC
Mercedes-Benz Financial Services Austria GmbH	Austria	Eugendorf
Mercedes-Benz Financial Services BeLux NV	Belgium	Brussels
Mercedes-Benz Financial Services Canada Corporation	Canada	Mississauga ON
Mercedes-Benz Financial Services Ceská republika s.r.o.	Czech Republic	Prague
Mercedes-Benz Financial Services España, E.F.C., S.A.	Spain	Alcobendas
Mercedes-Benz Financial Services France S.A.	France	Montigny-le-Bretonneux
Mercedes-Benz Financial Services Hong Kong Ltd.	Hong Kong	Hongkong
Mercedes-Benz Financial Services India Private Limited	India	Pune
Mercedes-Benz Financial Services Investment Company LLC	USA	Farmington Hills MI
Mercedes-Benz Financial Services Italia S.p.A.	Italy	Rome
Mercedes-Benz Financial Services Korea Ltd.	South Korea	Seoul
Mercedes-Benz Financial Services Nederland B.V.	Netherlands	Utrecht
Mercedes-Benz Financial Services New Zealand Ltd	New Zealand	Auckland
Mercedes-Benz Financial Services Portugal - Sociedade Financeira de Crédito S.A.	Portugal	Mem Martins
Mercedes-Benz Financial Services Schweiz AG	Switzerland	Schlieren
Mercedes-Benz Financial Services Singapore Ltd.	Singapore	Singapore
Mercedes-Benz Financial Services Slovakia s.r.o.	Slovakia	Bratislava
Mercedes-Benz Financial Services South Africa (Pty) Ltd	South Africa	Pretoria
Mercedes-Benz Financial Services Sp. z o.o.	Poland	Warsaw
Mercedes-Benz Financial Services Taiwan Ltd.	Taiwan	Taipei
Mercedes-Benz Financial Services UK (Trustees) Ltd	United Kingdom	Milton Keynes

Mercedes-Benz Financial Services UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Financial Services USA LLC	USA	Farmington Hills MI
Mercedes-Benz Finans Danmark A/S	Denmark	Copenhagen
Mercedes-Benz Finans Sverige AB	Sweden	Malmö
Mercedes-Benz Finansman Türk A.S.	Turkey	Istanbul
Mercedes-Benz Fleet Management Singapore Pte. Ltd.	Singapore	Singapore
Mercedes-Benz France S.A.S.	France	Montigny-le-Bretonneux
Mercedes-Benz G GmbH	Austria	Raaba
Mercedes-Benz Gastronomie GmbH	Germany	Stuttgart
Mercedes-Benz Group Australia/Pacific Pty Ltd	Australia	Mulgrave VIC
Mercedes-Benz Group China Ltd.	China	Beijing
Mercedes-Benz Group Services Berlin GmbH	Germany	Berlin
Mercedes-Benz Group Services Madrid, S.A.U.	Spain	San Sebastián de los Reyes
Mercedes-Benz Group Services Phils., Inc.	Philippines	Cebu City
Mercedes-Benz Group Services Poland Sp. z o.o.	Poland	Krakow
Mercedes-Benz Grund Services GmbH	Germany	Schönefeld
Mercedes-Benz Heritage GmbH	Germany	Stuttgart
Mercedes-Benz High Power Charging Europe GmbH	Germany	Stuttgart
Mercedes-Benz High Power Charging Japan G.K.	Japan	Chiba
Mercedes-Benz High Power Charging Korea Ltd.	South Korea	Seoul
Mercedes-Benz High Power Charging Overseas GmbH	Germany	Stuttgart
Mercedes-Benz Holdings UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Hong Kong Limited	Hong Kong	Hong Kong
Mercedes-Benz HPC Canada ULC	Canada	Vancouver
Mercedes-Benz HPC North America LLC	USA	New York NY
Mercedes-Benz Hungária Kft.	Hungary	Budapest

Mercedes-Benz IDC Europe S.A.S.	France	Valbonne
Mercedes-Benz India Private Limited	India	Pune
Mercedes-Benz Insurance Agency LLC	USA	Farmington Hills MI
Mercedes-Benz Insurance Broker S.R.L.	Romania	Voluntari
Mercedes-Benz Insurance Services GmbH	Germany	Stuttgart
Mercedes-Benz Insurance Services Nederland B.V.	Netherlands	Utrecht
Mercedes-Benz Insurance Services Taiwan Ltd.	Taiwan	Taipei
Mercedes-Benz Insurance Services UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Intellectual Property GmbH & Co. KG	Germany	Stuttgart
Mercedes-Benz Intellectual Property Management GmbH	Germany	Stuttgart
Mercedes-Benz International Finance B.V.	Netherlands	Utrecht
Mercedes-Benz Italia S.p.A.	Italy	Rome
Mercedes-Benz Japan G.K.	Japan	Chiba
Mercedes-Benz Korea Limited	South Korea	Seoul
Mercedes-Benz Lease Italia S.r.l.	Italy	Rome
Mercedes-Benz Leasing Co., Ltd.	China	Beijing
Mercedes-Benz Leasing Germany GmbH	Germany	Stuttgart
Mercedes-Benz Leasing GmbH	Germany	Stuttgart
Mercedes-Benz Leasing IFN S.A.	Romania	Voluntari
Mercedes-Benz Leasing Kft.	Hungary	Budapest
Mercedes-Benz Leasing Polska Sp. z o.o.	Poland	Warsaw
Mercedes-Benz Leasing Treuhand GmbH	Germany	Stuttgart
Mercedes-Benz Logistics and Distribution Egypt L.L.C.	Egypt	New Cairo
Mercedes-Benz LT GmbH	Germany	Sindelfingen
Mercedes-Benz Ludwigsfelde Anlagenverwaltung GmbH & Co. OHG	Germany	Schönefeld
Mercedes-Benz Ludwigsfelde GmbH	Germany	Ludwigsfelde
Mercedes-Benz Malaysia Sdn. Bhd.	Malaysia	Puchong

Mercedes-Benz Manhattan, Inc.	USA	New York
Mercedes-Benz Manufacturing (Thailand) Limited	Thailand	Bangkok
Mercedes-Benz Manufacturing and Import Egypt L.L.C.	Egypt	New Cairo
Mercedes-Benz Manufacturing Hungary Kft.	Hungary	Kecskemét
Mercedes-Benz Manufacturing Poland sp. z o. o.	Poland	Jawor
Mercedes-Benz México International, S. de R.L. de C.V.	Mexico	Distrito Federal
Mercedes-Benz Mexico, S. de R.L. de C.V.	Mexico	Ciudad de México
Mercedes-Benz Mitarbeiter-Fahrzeuge Leasing GmbH	Germany	Stuttgart
Mercedes-Benz Mobility (Thailand) Co., Ltd.	Thailand	Bangkok
Mercedes-Benz Mobility & Technology Service (Beijing) Co., Ltd.	China	Beijing
Mercedes-Benz Mobility AG	Germany	Stuttgart
MERCEDES-BENZ MOBILITY AUSTRALIA PTY LTD	Australia	Melbourne VIC
Mercedes-Benz Mobility Austria GmbH	Austria	Eugendorf
Mercedes-Benz Mobility Beteiligungsgesellschaft mbH	Germany	Stuttgart
Mercedes-Benz Mobility Korea Ltd.	South Korea	Seoul
MERCEDES-BENZ MOBILITY MEXICO, S. DE R.L. DE C.V.	Mexico	Ciudad de México
Mercedes-Benz Mobility Services GmbH	Germany	Stuttgart
Mercedes-Benz Nederland B.V.	Netherlands	Nieuwegein
Mercedes-Benz Nederland Holding B.V.	Netherlands	Utrecht
Mercedes-Benz New Zealand Ltd	New Zealand	Auckland
Mercedes-Benz North America Corporation	USA	Farmington Hills MI
Mercedes-Benz North America Finance LLC	USA	Farmington Hills MI
Mercedes-Benz Österreich GmbH	Austria	Eugendorf
Mercedes-Benz Otomotiv Ticaret ve Hizmetler A.S.	Turkey	Istanbul
Mercedes-Benz Parts Brand GmbH	Germany	Stuttgart
Mercedes-Benz Parts Logistics Asia Pacific Sdn. Bhd.	Malaysia	Puchong

Annex 3: List of Group companies subject to the Data Protection Policy EU

Mercedes-Benz Parts Logistics Ibérica, S.L.U.	Spain	Azuqueca de Henares
Mercedes-Benz Parts Logistics UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Parts Manufacturing & Services Ltd.	China	Shanghai
Mercedes-Benz Pensionsfonds AG	Germany	Stuttgart
Mercedes-Benz Polska Sp. z o.o.	Poland	Warsaw
Mercedes-Benz Portugal, S.A.	Portugal	Sintra
Mercedes-Benz Purchasing Coordination Corporation	USA	Vance AL
Mercedes-Benz Real Estate GmbH	Germany	Berlin
Mercedes-Benz Reinsurance S.A. Luxembourg	Luxembourg	Luxemburg
Mercedes-Benz Renting, S.A.	Spain	Alcobendas
Mercedes-Benz Research & Development North America, Inc.	USA	Sunnyvale
Mercedes-Benz Research & Development Tel Aviv Ltd.	Israel	Tel-Aviv
Mercedes-Benz Research and Development India Private Limited	India	Bengaluru
Mercedes-Benz Retail Group UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Retail Receivables LLC	USA	Farmington Hills MI
Mercedes-Benz Romania S.R.L.	Romania	Bukarest
Mercedes-Benz Schweiz AG	Switzerland	Schlieren
Mercedes-Benz Second Life Solutions LLC	USA	Vance
Mercedes-Benz Service Leasing S.R.L.	Romania	Bukarest
Mercedes-Benz Services Correduria de Seguros, S.A.	Spain	Alcobendas
Mercedes-Benz Services Malaysia Sdn Bhd	Malaysia	Selangor
Mercedes-Benz Sigorta Aracilik Hizmetleri A.S.	Turkey	Istanbul
Mercedes-Benz Singapore Pte. Ltd.	Singapore	Singapore
Mercedes-Benz Slovakia s.r.o.	Slovakia	Bratislava
Mercedes-Benz South Africa Ltd	South Africa	Pretoria
Mercedes-Benz Sverige AB	Sweden	Malmö

Mercedes-Benz Taiwan Ltd.	Taiwan	Taipei
Mercedes-Benz Tech Innovation GmbH	Germany	Ulm
Mercedes-Benz Trust Holdings LLC	USA	Farmington Hills MI
Mercedes-Benz Trust Leasing Conduit LLC	USA	Farmington Hills MI
Mercedes-Benz Trust Leasing LLC	USA	Farmington Hills MI
Mercedes-Benz U.S. International, Inc.	USA	Tuscaloosa AL
Mercedes-Benz Ubezpieczenia Sp. z o.o.	Poland	Warsaw
Mercedes-Benz UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz UK Share Trustee Ltd.	United Kingdom	Milton Keynes
Mercedes-Benz UK Trustees Limited	United Kingdom	Milton Keynes
Mercedes-Benz Unterstützungskasse GmbH	Germany	Stuttgart
Mercedes-Benz USA, LLC	USA	Sandy Springs GA
Mercedes-Benz Used Parts & Services GmbH	Germany	Neuhausen a.d.F.
Mercedes-Benz Vans Hong Kong Limited	Hong Kong	Xianggang
Mercedes-Benz Vans UK Limited	United Kingdom	Milton Keynes
Mercedes-Benz Vans, LLC	USA	Ladson SC
Mercedes-Benz Venezuela S.A.	Venezuela	Valencia
Mercedes-Benz Vermögens- und Beteiligungsgesellschaft mbH	Germany	Stuttgart
Mercedes-Benz Versicherung AG	Germany	Stuttgart
Mercedes-Benz Versicherungsservice GmbH	Germany	Berlin
Mercedes-Benz Verwaltungsgesellschaft für Grundbesitz mbH	Germany	Schönefeld
Mercedes-Benz Vietnam Ltd.	Vietnam	Ho Chi Minh City
Mercedes-Benz Wholesale Receivables LLC	USA	Farmington Hills MI
Mercedes-Benz.io GmbH	Germany	Stuttgart
Mercedes-Benz.io Portugal Unipessoal Lda.	Portugal	Lisbon
Montajes y Estampaciones Metálicas, S.L.	Spain	Esparraguera
Movinx Americas Company, Inc.	USA	Schaumburg
Movinx GmbH	Germany	Berlin

Movinx UK Ltd.	United Kingdom	
Multifleet G.I.E	France	Le Bourget
NAG Nationale Automobil-Gesellschaft Aktiengesellschaft	Germany	Stuttgart
Porcher & Meffert Grundstücksgesellschaft mbH & Co. Stuttgart OHG	Germany	Schönefeld
PT Mercedes-Benz Consulting Services Indonesia	Indonesia	Bogor
Silver Arrow Canada GP Inc.	Canada	Mississauga ON
Silver Arrow Canada LP	Canada	Mississauga ON
Star Assembly SRL	Romania	Sebes
Star Transmission srl	Romania	Cugir
STARCAM s.r.o.	Czech Republic	Most
STARKOM, proizvodnja in trgovina d.o.o.	Slovenia	Maribor
Ucafleet S.A.S	France	Le Bourget
Wagenplan B.V.	Netherlands	Almere
YASA Limited	United Kingdom	Kidlington

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