DAIMLER TRUCK

Data Protection Policy EU

Binding Corporate Rules

Contents

1. Introduction

Definition

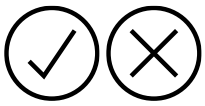
EU GDPR provides for the use of binding corporate rules by a group of undertakings for transfers of personal data within this Group. To this end, the Policy contains provisions for the protection of natural persons with regard to the processing of personal data. "Personal data" means any information relating to an identified or identifiable natural person.

Aim

The Daimler Truck 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 binding corporate rules 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 Daimler Truck 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 Daimler Truck Group.

The binding corporate rules defined in this Policy are subject to approval by the European supervisory authorities to be effective. The Daimler Truck rules were approved in January 2023. Effective November, the binding corporate rules were updated in compliance with revised instructions of the supervisory authorities and the recommendation update 1/2022 of the European Data Protection Board (EDPB). In the following the term “rules” is used in accordance with EU GDPR.

Dos & Don’ts



The managing body of the respective Daimler Truck Group Company is responsible for compliance with the binding corporate rules. Within the Group Companies, the Information Owners are responsible for the protection of the data created, generated, used and/or updated in their areas of responsibility throughout the data life cycle.
In addition, all employees are responsible for using personal data only in a permissible manner and protecting it from unauthorized access.

Further information

Data Privacy & Data Compliance | Audit, Compliance & Legal (tbintra.net)

2. Scope

The binding corporate rules apply to Daimler Truck Holding AG and Daimler Truck AG, its controlled Group Companies (hereinafter **Group Companies**) and its employees and members of managing bodies. "Controlled" in this instance means that Daimler Truck Holding AG and Daimler Truck AG may enforce the adoption of these rules directly or indirectly, on the basis of its voting majority, majority management representation, or by agreement.

The rules apply 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 rules also apply to all employee data[1] in hard-copy format in Germany.

The rules apply to the processing of personal data:

- (a) from Group Companies and their subsidiaries that are established in the EU/ EEA or another country to which these rules 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 rules 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 these rules 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 Daimler Truck Group Companies bound by the Data Protection Policy EU*".

These rules 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, these rules also apply in the same manner to the data of legal entities.

3. Legal Enforceability within the Daimler Truck Group

The provisions of these rules are binding on 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 these rules.
As far as it is not otherwise stipulated by legal requirements, Group Companies are not entitled to adopt regulations that deviate from these rules.

4. Relationship to Legal Requirements

These rules do not replace EU legislation and national laws. They supplement the national data protection laws. Where national legislation, for instance EU legislation, requires a higher level of protection for personal data, it will take precedence over the rules.
The content of these rules must also be observed in the absence of corresponding national laws.

---

[1] To make these rules easier to read, the text uses only the male forms of pronouns for natural persons. The words "he," "his" and "him" are always intended to include all individuals, regardless of gender identity.

If compliance with these rules would result in a violation of national law, or if regulations that deviate from these rules are required under national law, this must be reported to the Chief Data Privacy Officer and the department Data Privacy & Data Compliance for the purposes of data protection law monitoring. In the event of conflicts between national laws and these rules, the Chief Data Privacy Officer and the department Data Privacy & Data Compliance will work with the responsible Group Company to find a practical solution that fulfills the purpose of these rules. 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 Daimler Truck Group does not readily constitute such 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.

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 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 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 (see Section 5.2.3). If the data subject objects to the use of his 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 these rules. 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.

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

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 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 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.

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. The granting of consent must be in any case properly documented. Before giving consent, the data subject must be informed in accordance with these rules.

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.

Control measures that require the processing of employee data beyond performance of the employment relationship (e.g. performance monitoring) 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 potential legitimate interests that the employee affected by the measure may have in excluding 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 special categories of data

Special categories of data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Special categories of data should not be processed unless this is required by law or expressly permitted.

Processing of such data by a Group Company may be allowed in specific cases, if:

- the data subject has given explicit consent to the processing of such data for one or more specified purposes;
- processing is necessary for the controller or data subject to carry out obligations or exercise rights in the field of employment law and social law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing relates to data, which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for the purposes of preventive or occupational medicine when the staff is subject to professional secrecy or an obligation to secrecy;
- processing is necessary for reasons of public interest in the area of public health

Further conditions including limitations may apply due to state law. If there are plans to process special categories of data, the Chief Data Privacy Officer must be informed in advance.

Group Companies are prohibited from processing personal data relating to criminal convictions and offences.

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.

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 EU 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 Data Privacy Officer and the department Data Privacy & Data Compliance 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

- 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.

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.

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

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 always complied with.

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 Daimler Truck Holding AG and Daimler Truck AG imposes for the performance of deletion routines (such as software tools, documentation requirements) must be observed.

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.

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 admissibility 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 processing, 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 Data Privacy Officer has to be informed who will contact the competent data protection Supervisory Authority for consultation.

Provisions established by Daimler Truck Holding AG and Daimler Truck AG for performing this assessment (such as software tools, instructions on the performance of an evaluation) must be observed.

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 Daimler Truck Holding AG and Daimler Truck AG for documentation (such as software tools and instructions on documentation) must be observed.

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 Daimler Truck 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.

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 measures.
- The contractual standards provided by the Chief Data Privacy Officer 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 Daimler Truck Holding AG and Daimler Truck 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 Provision 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 these rules 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 controllers 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 these rules 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 Data Privacy Officer must be observed.

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 without undue delay but in any event 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 within the first month.

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 Data Privacy Officer 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 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 Data Privacy Officer if they feel that these rules have 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 these rules against the Group Company that imports the data.

In case the complaint is justified, the Group Company takes adequate measures to ensure compliance with these rules 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 their rights and should be informed accordingly. To this end, the data subject may apply to the competent Supervisory Authority, in particular in the country of the data subject's 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 these rules 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 these rules 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.

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 their habitual residence.

The data subject who claims an infringement of these rules in the context of a third country processing can assert their 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 a supervisory authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement, and before the competent court of the Member State where the controller or processor has an establishment, or where the data subject has their habitual residence.

Any dispute related to the competent Supervisory Authorities' exercise of supervision of compliance with these rules will be resolved by the courts of the Member State of that Authority, in accordance with that Member State's procedural law. The Group Companies agree to submit themselves to the jurisdiction of these courts.

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.

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 via the central Information Security Incident Management Process to Daimler Truck AG and to the Chief Data Privacy Officer. Within this process, it is ensured that the responsible data exporter and, in the case of processing on behalf, the controller are informed. Requirements stipulated by Daimler Truck Holding AG and Daimler Truck 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.

All obligations listed in this section 12 are third party beneficiary rights for the data subject.

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 data protection requirements, and those contained in these rules 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 Data Privacy Officer must be informed immediately.

13.2 Awareness Raising & Training

Management must ensure that its employees receive and attend appropriate and up-to-date data protection training, including the content and handling of these rules, 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 data protection training intervals depend on the target group. For particularly relevant target groups, training courses are held annually. The requirements of the Chief Data Privacy Officer and the department Data Privacy & Data Compliance must be observed.

13.3 Organization

The Chief Data Privacy Officer is internally independent of instructions regarding the performance of her tasks. She must ensure compliance with national and international data protection laws. She is responsible for these rules 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 Data Privacy Officer.

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

Daimler Truck Holding AG and Daimler Truck AG's Supervisory Board must be informed of the annual report of the Chief Data Privacy Officer as part of existing reporting duties.

All data subjects can contact the Chief Privacy Officer 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 Data Privacy Officer is:
Daimler Truck AG, Chief Data Privacy Officer, HPC DTF2B,
70745 Leinfelden-Echterdingen, Germany
E-Mail: dataprivacy@daimlertruck.com

The Daimler Truck 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.

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 these rules will be penalized in accordance with internal regulations.

13.5 Audit and Inspections

Compliance with these rules and applicable data protection laws is regularly reviewed at Group level, at least once a year, based on a risk-oriented approach. This is carried out through internal compliance risk assessments, audits including specific data protection topics, and other reviews. The Chief Data Privacy Officer has the right to request additional audits. The results must be reported to the Chief Data Privacy Officer, the responsible Group Company and its data protection officer if one has been appointed.

Daimler Truck Holding 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 EU GDPR and its national law, carry out a data protection audit of any Group Company on compliance with these rules.

14. Amendments to these Rules and Cooperation with Authorities

14.1 Process and Responsibilities in the Event of Termination or Amendments

These rules can only be changed by means of the defined procedure for amendment of policies (Policy on Policy Management, 2-L 1.0) in coordination with the Chief Data Privacy Officer. They are continuously kept up to date. Where a modification to the rules would possibly be detrimental to the level of protection offered by the rules or significantly affect them, it must be communicated in advance to the supervisory authorities, via the lead authority with a brief explanation of the reasons for the update.

A data importer which ceases to be bound by the rules may keep, return, or delete the personal data received under the rules. If the data exporter and importer agree that the data may be kept by the data importer, protection must be maintained in accordance with EU GDPR.

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

The data subject has a right to easily access these rules. Therefore, the latest version of these rules will be published online at *https://www.daimler-truck.com*. This requirement is a third party beneficiary right for the data subject.

The Chief Data Privacy Officer will notify the Supervisory Authority of the main establishment of Daimler Truck Holding AG and Daimler Truck AG and all Group Companies once a year if amendments are made to these rules or the list of affiliated Group Companies with a brief explanation of the reasons justifying the amendment.

14.2 Cooperation with Authorities

Group Companies are obligated to cooperate with the competent supervisory authorities on any issue related to these rules, to take into account their advice and to abide by their decisions. This encompasses the duty to accept inspections and required audits by supervisory authorities, including where necessary on-site.

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 Daimler Truck 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 defense of legal claims).

15.2 Transfer within the Daimler Truck Group

No transfer is made to a Group Company outside EU/ EEA unless the company is effectively bound by these rules and can deliver compliance.

Before the transfer of personal data to a Group Company outside EU/ EEA the Group Companies have to assess that the law and practices in the third country of destination applicable to the processing of the personal data do not prevent them from fulfilling their obligations under these rules. This includes any requirements to disclose personal data or measures authorizing access by public authorities.

In assessing the laws and practices of the third country which may affect the respect of the commitments contained in these rules, the Group Companies have to take due account, in particular, of the following elements:

- the specific circumstances of the transfers (including purposes, types of entities involved in the processing, economic sector, data categories, locations of the processing and transmission channels used), the laws and practices of the third country of destination applicable to the Group Company including those requiring to disclose data to public authorities or authorizing access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer as well as applicable limitations and safeguards
- any relevant contractual, technical or organizational safeguards put in place to supplement the provisions under these rules.

Where safeguards must be taken in addition to those envisaged under the rules, the data exporter and the Chief Data Privacy Officer must be informed and involved in the assessment.

The Group Company in the third country is obliged to promptly notify the data exporter, if it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under these rules. This information should also be provided to the liable Group Company(ies).

Upon verification of such a notification the liable Group Company (data exporter) along with the Chief Data Privacy Officer commits to promptly identify supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Group Company acting as data exporter and/or data importer to enable them to fulfil their obligations under these rules. The same applies if a Group Company acting as data exporter has reasons to believe that a Group Company acting as its data importer can no longer fulfil its obligations under these rules.

Where the liable Group Company (data exporter) and the Chief Data Privacy Officer assess that the rules - even if accompanied by supplementary measures - cannot be complied with or if instructed by the competent Supervisory Authority, the data transfer as well as all transfers for which the same assessment and reasoning would lead to a similar result, must be suspended until compliance with the provisions of these rules is again ensured. If compliance with these rules cannot be restored within one month of suspension, the transfer must be ended. The personal data transferred prior to the suspension and any copies thereof must be returned to the data exporter or destroyed.

The Group Companies appropriately document the assessment as well as the selected and implemented supplementary measures. This documentation is made available to the competent Supervisory Authority upon request.
The responsible Group Company also informs all other Group Companies of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfer is carried out by another Group Company or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

Provisions established by the Daimler Truck Group for performing this assessment (such as tools, instructions on the performance of an assessment) must be observed.

The data importer promptly informs the data exporter if it is unable to comply with the rules, for whatever reason including the situations described above.

Where the data importer is in breach of the rules or unable to comply with them, the data exporter should suspend the transfer.

At the choice of the data exporter the data importer immediately returns or deletes the personal data that has been transferred under these rules in its entirety including any copies where the data exporter has suspended the transfer and compliance with the rules cannot be restored within one month, the data importer is in substantial or persistent breach of the rules or the data importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under the rules.

The data importer certifies the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer continues to ensure compliance with these rules. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with the rules and will only process the data to the extent and for as long as required under local law.

All obligations listed in this section 15 are third party beneficiary rights for the data subject.

16. Monitoring and Reporting on the Regulations of Third Countries

Data exporters must continuously monitor developments that may affect the level of protection in the countries to which they transfer data, together with the Group Company in the third country and the Chief Data Privacy Officer.
Group Companies in third countries must promptly inform the data exporter and where possible the data subject if they receive a legally binding request by a public authority for disclosure of personal data transferred pursuant to these rules or if they become aware of any direct access to such data by public authorities.

If prohibited from notifying the data exporter and/or data subject, the Group Company will use its best efforts to obtain a waiver of such prohibition.

The Group Company will provide the data exporter, at regular intervals, within its scope of action with as much relevant information as possible on the requests received. If this is partially or completely prohibited, the Group Company informs the data exporter accordingly without undue delay.

The Group Company will preserve the relevant information for as long as the personal data is subject to the safeguards provided by these rules and shall make it available to the competent Supervisory Authorities upon request.

The Group Company in the third country must review the legality of the request for disclosure, challenge the request if necessary and pursue possibilities of appeal. When challenging a request, the Group Company will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

The Group Company must document the result of the review, the legal assessment and any challenge to the request for disclosure and, if permissible, make the documentation available to the data exporter and upon request to the competent Supervisory Authority.

The Group Company in the third country will provide the minimum amount of information permissible when responding to a request for disclosure.

Transfers of personal data by a Group Company 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.

Daimler Truck AG
Fasanenweg 10
70771 Leinfelden-Echterdingen
Germany