

1 Description

The G+D Group has set itself the goal of using uniform, globally applicable rules to ensure an appropriate level of protection for the processing of personal data within the G+D Group. As part of this commitment to a high level of Data Privacy, the G+D Group has implemented Binding Corporate Rules (binding internal Data Privacy rules) to ensure safeguards and guarantees for an adequate level of Data Privacy in accordance with EU Regulation 2016/679 (General Data Protection Regulation) for the processing of personal data within the G+D Group, whether in the role of controller or processor, and in particular with regard to their transfer outside the EEA.

The Binding Corporate Rules enable legally compliant data transfers to so-called third countries for which there is no adequacy decision by the European Commission.

The Binding Corporate Rules are binding for all participating companies of the G+D Group and also apply to the employees of these companies. In view of the great importance of the Binding Corporate Rules for the protection of personal data within the G+D Group, the Group management is obliged to ensure effective implementation of and compliance with the Binding Corporate Rules within the G+D Group.

2 Scope of the Binding Corporate Rules

The Giesecke+Devrient Binding Corporate Rules (BCR) apply within the G+D Group, for all Group companies included on the list "Worldwide Data Privacy Contacts". This list is published on the G+D homepage.

3 General Data Privacy principles, including data security and data quality

. The general data protection principles apply to these BCR, in particular the principles of purpose limitation, data minimization, limited storage periods, data accuracy, integrity and confidentiality of data, lawfulness, fair *processing*, transparency, data protection by design and by default, *processing* of special categories of *personal data*, measures to ensure data security and the requirements in respect of onward transfers to bodies not bound by the BCR.

The *G+D Group* undertakes to ensure that *personal data processed* will be accurate, complete and, to the extent reasonably necessary for the applicable purpose, kept up-to-date. The *G+D Group* shall take every reasonable measure to rectify or delete *personal data* which is inaccurate, incomplete or outdated, having regard to the purpose for which they were collected or for which they are further *processed*.

Processing of personal data shall be restricted to data that is reasonably adequate and relevant for the applicable purpose, and not excessive in relation to the purposes for which it is collected and/or further *processed*. If no longer necessary for the respective purposes *personal data* shall not be *processed* any longer and securely deleted or destroyed.

4 Legal basis for processing personal data

Personal data may be processed by the controller only for one or more of the following reasons:

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary in order to comply with a legal obligation to which the controller is subject; or
- The processing is necessary to protect the essential interests of the data subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- The processing is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the data are disclosed, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject.

If none of the above reasons apply, the G+D Group must obtain the unambiguous consent of the data subject before processing his or her personal data. The data subject may revoke his or her consent at any time with effect for the future, unless otherwise required by applicable law. In this case, the G+D Group shall cease all further

processing, unless the processing is required by applicable law or in the context of a contractual relationship to which the data subject is a party.

5 Legal basis for the processing of special categories of personal data

The G+D Group recognizes that the processing of personal data relating to criminal convictions and criminal offenses is prohibited unless it is carried out under the control of official authority or it is permitted under applicable law that provides appropriate safeguards for the rights and freedoms of data subjects.

The *G+D Group* undertakes not to *process sensitive data* if not one or more of the following grounds are applicable:

- The *data subject* has given his/her explicit consent to the *processing* of those *sensitive data* for one or more specified purposes, except where applicable law provides that the prohibition may not be lifted by the *data subject*; or
- The *processing* is necessary for the purposes of carrying out the obligations and specific rights of the *data controller* or the *data subject* in the field of employment law and social security and social protection law in so far as it is authorized by applicable law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the *data subject*; or
- The *processing* is necessary to protect the vital interests of the *data subject* or of another person where the *data subject* is physically or legally incapable of giving his/her consent; or
- The *processing* is carried out by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim in the course of its legitimate activities with appropriate guarantees and on condition that the *processing* relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the *data* is not disclosed to a third party without the consent of the *data subjects*; or
- The *processing* relates to special categories of *personal data* which is manifestly made public by the *data subject*; or
- The processing of the special categories of *personal data* is necessary for the establishment, exercise or defense of legal claims or in case of actions by the courts in the course of their judicial activities; or
- The *processing* of special categories of *personal data* is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care services, and where those special categories of *personal data* is *processed* by a health care professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
-

6 Easy Access to the Binding Corporate Rules

The relevant parts of these Binding Corporate Rules are, and shall continue to be, published on the corporate website of the G+D Group to inform data subjects about their rights. In addition, data subjects shall be provided with a copy of these Binding Corporate Rules upon request to the responsible privacy officer. Contact details of the privacy officer are published on the corporate website of the G+D Group.

7 Information of the persons concerned

All data subjects who have rights as third party beneficiaries shall receive information from the controller about their rights as third party beneficiaries in relation to the processing of their personal data and about the means to exercise those rights. Furthermore, data subjects shall be informed about liability and Data Privacy principles.

The members of the G+D Group in the role of data controller undertake to provide data subjects with at least the following information before processing their personal data, unless the data subjects already have it:

- The identity and contact information of the member of the G+D group acting as the responsible party and his or her representative (if applicable), as well as that of the responsible privacy officer,

Summary of the G+D BCR

- the purposes of the processing for which the personal data are intended and the legal basis for the processing; if the processing is based on legitimate interests, the legitimate interests pursued by the member of the G+D Group or by a third party; if the processing is based on consent, the existence of the right to withdraw consent at any time without affecting the lawfulness of the processing based on consent prior to its withdrawal,
- the categories of personal data concerned, the recipients or categories of recipients of the personal data, the existence of the right of access to the personal data as well as the right to rectify, erase or restrict the processing of the personal data concerning the data subject and the right to object to processing
- the period during which the personal data will be stored or, if this is not possible, to indicate the criteria for determining this period
- whether the provision of personal data is a legal or contractual requirement, whether the data subject is obliged to provide the personal data, and whether any consequences may follow if it is not provided,
- their right to complain to a supervisory authority,
- the existence of automated decision-making, including profiling, and in such cases, meaningful information about the logic involved and the scope and intended effects of such processing for the data subject,
- Data subjects will be informed about the processing and/or transfer of their personal data on the G+D Group's corporate website and, where appropriate, also by means of references to this website, in business communications and company brochures or in a similar, appropriate manner.
- If the personal data has not been collected from the data subject, the G+D Group member responsible shall additionally inform the data subject of the source of the personal data and, to the extent applicable, whether the personal data originates from publicly available sources. The competent G+D member shall provide the information within a reasonable period of time after receipt of the personal data, but no later than within one month, taking into account the particular circumstances under which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication with that person
- if disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed

The responsible member of the G+D Group is not obliged to provide information to the data subject if:

- the person concerned has already been informed
- the disclosure of the information to the data subject is impossible or would involve a disproportionate effort
- the obtaining or disclosure is expressly governed by legislation of the European Union or the Member States to which the controller is subject and which provides for appropriate measures to protect the data subject's legitimate interests
- the personal data is subject to professional secrecy, including a statutory duty of confidentiality, in accordance with the law of the European Union or the law of the Member States and must therefore be treated confidentially.

8 Accountability

Each member of the G+D Group is responsible for and able to demonstrate compliance with these Binding Corporate Rules.

For this reason, all members of the G+D Group maintain directories of processing activities. These contain, in particular, the name and contact details of the controller or processor, the Data Privacy officer, the purposes of the processing, the existing deletion periods and a general description of the categories of data subjects and personal data, the recipients to whom the personal data have been or will be disclosed, the technical and organizational measures taken to ensure the security of the processing. Furthermore, the transfers to third countries that have taken place, including the existing guarantees. In the case of commissioned processing, additionally the categories of processing carried out on behalf. These lists of processing activities can be kept in writing or in electronic form and will be made available to the supervisory authority upon request.

9 Rights of data subjects

Data subjects shall have the right to obtain, freely and without constraint, at reasonable intervals and without undue delay, information about and / or a copy of the personal data concerning them that is processed by the

respective member of the G+D Group acting as controller in relation to their personal data, including in particular information about the purposes of the processing, any available information on the origin of the personal data as well as on the recipients or categories of recipients to whom the personal data are/were disclosed, on the envisaged storage period of their personal data, or, if this is not possible, on the criteria used to determine this period, as well as the categories of personal data processed.

Data subjects have the right to request that their personal data be corrected if the personal data is incomplete or inaccurate, unless the processing of such personal data in its unaltered form is required by applicable law.

Data subjects have the right to request erasure of their personal data, in particular if it is no longer necessary for the purposes for which it was collected / processed, or consent has been withdrawn and there is no other legal basis for the processing, or they have objected to the processing and there are no overriding legitimate grounds for the processing, or the processing was unlawful. This does not apply insofar as the processing is required by applicable law or is necessary for the assertion, exercise or defense of legal claims.

Data subjects have the right, if they dispute the accuracy of the personal data, to request the restriction of processing for the duration of the review by the controller. They may also request restriction of processing instead of erasure of the personal data in the event of unlawful processing. If the controller no longer needs the personal data, data subjects may request restriction of processing if they need the personal data to assert, exercise or defend legal claims. In addition, restriction of processing may be requested if an objection to processing has been lodged and it has not yet been determined whether this is contrary to the legitimate grounds of the controller. Restriction of processing will not be carried out insofar as processing is required by applicable law.

Before the restriction on processing is lifted, the data subject shall be informed of the lifting by the controller.

The controller shall notify all recipients to whom personal data have been disclosed of any rectification or erasure of the personal data or restriction of processing, unless this is impossible or involves a disproportionate effort. The data subject may request to be informed about these recipients.

Data subjects shall have the right to object at any time, on grounds relating to their particular situation, to processing of their personal data which is carried out for the performance of a task entrusted to the controller in the public interest or in the exercise of official authority, or which is based on legitimate interests of the controller or a third party overriding the interests of the data subject, unless such processing is required by applicable law. Unless the member of the G+D Group which is the controller can demonstrate compelling legitimate interests which override the interests of the data subject, and the processing is necessary for the establishment, exercise or defense of legal claims, the member of the G+D Group shall cease the processing if the objection is justified.

In addition, data subjects have the right to object, free of charge, to the processing of their personal data for direct marketing purposes. This personal data will then no longer be processed for direct marketing purposes.

Data subjects may exercise their above-mentioned rights by contacting the Privacy Officer responsible for the respective member of the G+D Group acting as data controller with respect to their personal data. The contact information of the responsible Privacy Officer for each member of the G+D Group will be published on the G+D Group's corporate website. In addition, data subjects have the right to lodge a complaint under the internal complaints procedure.

10 Automated individual decisions

The G+D Group undertakes not to make any decision which produces legal effects or significantly affects the data subject solely on the basis of automated processing of his or her personal data. This provision shall not apply if this is necessary for the conclusion or performance of a contract between the data subject and the controller, or if the data subject has given his or her explicit consent, and the protection of his or her legitimate interests is ensured by suitable measures, such as the possibility of asserting his or her point of view or the intervention of a person on the part of the controller, or if this decision is permitted by a law that also contains measures to protect the data subject's legitimate interests.

11 Security and confidentiality of data

Summary of the G+D BCR

All members of the G+D Group have implemented and undertake to maintain appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other forms of unlawful processing, in particular where the processing involves the transmission of personal data over a network. The technical and organizational measures are also implemented to implement the Data Privacy principles and facilitate compliance with the requirements set by the Binding Corporate Rules in practice (Data Privacy by Design and by Default).

These measures are intended to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data. The processing of special categories of personal data is subject to enhanced security measures.

Employees of the G+D Group have access to personal data only to the extent necessary to perform their duties and for the applicable purpose. All employees who have access to personal data are obliged to treat this personal data with appropriate confidentiality.

12 Relationships with processors

Members of the G+D Group who process personal data on behalf of a controller belonging to the G+D Group are also bound by the Binding Corporate Rules in their capacity as processors to the extent applicable to them.

In their function as processors, these members of the G+D Group are also generally obliged to assist and support the controllers belonging to the G+D Group in fulfilling their obligations under these Binding Corporate Rules (in particular with regard to the obligations of the controllers with regard to safeguarding the rights of data subjects).

If the external processor is located in a third country without an adequate level of Data Privacy, the member of the G+D Group acting as controller or processor also undertakes to take appropriate measures to comply with the obligations arising from requirements for the transfer of personal data to third countries, for example by applying the standard contractual clauses adopted by the European Commission by means of Decision No. 2021/914/EC (for the transfer of personal data to processors in third countries), there is an adequacy decision by the Commission, there are binding internal Data Privacy rules, approved codes of conduct or certification mechanisms, or there is an authorization by the supervisory authority for the transfer.

13 Restriction of transfer and onward transfer outside the G+D Group to and in third country(ies)

If a member of the G+D Group in its capacity as a controller intends to transfer personal data to an external controller in a third country without an adequate level of Data Privacy, it undertakes to take appropriate measures to comply with the requirements arising from the requirements for the transfer of personal data to third countries, for example by applying the standard contractual clauses adopted by the European Commission by means of Decision No. 2021/914/EC (for the transfer of personal data to third countries), there is an adequacy decision by the Commission, there are binding internal Data Privacy rules, approved codes of conduct or certification mechanisms, or there is an authorization by the supervisory authority for the transfer.

14 Training program

The G+D Group has implemented a comprehensive training program for all employees who have permanent or regular access to personal data in the course of performing their work and/or are involved in the collection of personal data or the development of systems for processing personal data, and is committed to maintaining and updating this training program as necessary. The training program covers all relevant Data Privacy and data security aspects of the G+D Group, informs in particular and increases awareness of the Data Privacy requirements resulting from the Binding Corporate Rules.

15 Audit program

Summary of the G+D BCR

The G+D Group has implemented and is committed to maintaining a comprehensive audit program to verify compliance with the Binding Corporate Rules. The audit program covers all aspects of the Binding Corporate Rules and includes methods to ensure the implementation of corrective measures.

If there are indications that the Binding Corporate Rules are not being complied with, an audit is carried out to verify compliance. Further details of the audit program are set out in the G+D Group's audit concept.

The independence of the persons entrusted with the audit in the performance of their duties is guaranteed.

16 Compliance and compliance monitoring

The G+D Group appoints and ensures the continuous appointment of suitable employees who, with the support of the company management, monitor compliance with the Binding Corporate Rules and work towards compliance.

The Group Privacy Officer is appointed by the Group parent company and shall work towards compliance with Data Privacy laws and internal Group Data Privacy requirements, including these Binding Corporate Rules, throughout the Group. The Group Privacy Officer reports to the management of the G+D Group and makes recommendations to it. The Group Privacy Officer issues and monitors the implementation of the company's internal Data Privacy guidelines and regulations, for example by conducting audits, and is responsible for coordinating Data Privacy audits by internal or external auditors.

Local Privacy Officers are appointed for a specific member or members of the G+D Group in a geographic region, with prior approval of the Group Privacy Officer. They assist the Group Privacy Officer in working towards compliance with Data Privacy laws and internal Group Data Privacy requirements. Where necessary, a Data Privacy Officer will be appointed. The Local Privacy Officers are responsible for the implementation of and compliance with the company's internal Data Privacy guidelines, including these Binding Corporate Rules, as well as other national Data Privacy regulations at the local level.

The Privacy Officers can be contacted directly, for which their contact details are published on the G+D Group's corporate website.

17 Measures regarding national laws and practices that may affect compliance with the Binding Corporate Rules

G+D Group Members undertake to use the Binding Corporate Rules as a tool for a transfer only if they have determined that, in the third country of destination, the laws and practices applicable to the data importer in the processing of personal data, including any requirements for disclosure of personal data or measures authorizing access by public authorities, do not prevent the data importer from complying with its obligations under these Binding Corporate Rules.

This is based on the understanding that laws and practices that respect the essence of fundamental rights and freedoms and do not go beyond what is necessary and proportionate in a democratic society to protect a paramount objective are not inconsistent with these Binding Corporate Rules. Overriding objectives are :

- (a) national security;
- b) national defense;
- c) public safety;
- (d) the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against and the prevention of threats to public safety;
- (e) the protection of other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, such as in the monetary, budgetary, fiscal, public health and social security fields;
- f) the protection of the independence of the judiciary and the protection of judicial proceedings;

Summary of the G+D BCR

- g) the prevention, detection, investigation and prosecution of violations of professional rules of regulated professions;
- h) control, supervisory and regulatory functions permanently or temporarily connected with the exercise of official authority for the purposes referred to in subparagraphs (a) to (e) and (g);
- i) the protection of the data subject or the rights and freedoms of others;
- j) the enforcement of civil claims.

In assessing the laws and practices of the third country that may affect compliance with the obligations set forth in these Binding Corporate Rules, the members of the G+D Group shall consider, in particular:

- The specific circumstances of the transfer(s) and any intended onward transfer within the third country or to another third country. This includes:
 - o The purpose for which the personal data are transmitted and processed
 - o The types of entities involved in the processing
 - o The economic sectors in which the transmission(s) take place
 - o The categories and format of personal data transferred
 - o The place where the processing of personal data takes place, including their storage
 - o The channels used for transmission
- The laws and practices of the third country of destination relevant to the circumstances of the transfer(s), including those requiring disclosure of data to, or permitting access by, public authorities and those providing for access to such data during the transfer between the country of the data exporter and the country of the data importer, and the limitations and safeguards applicable thereto.
- Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Binding Corporate Rules, including measures applied during the transfer and processing of the personal data in the third country of destination.

This determination is reviewed on an ongoing basis by the respective data exporting member of the G+D Group for developments that may affect the original assessment.

This assessment, as well as the additional measures selected and implemented, are documented by the respective members of the G+D Group and made available to the responsible Data Privacy authority upon request.

If a member of the G+D Group in its role as data importer has reason to believe that applicable legislation and practices may prevent it from fulfilling its obligations under these Binding Corporate Rules, it shall promptly inform the member of the G+D Group that is a data exporter thereof.

After reviewing such notification, or if it otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Binding Corporate Rules, the data exporting member of the G+D group, together with the Privacy Officer, shall immediately take additional measures to be taken by the data exporter and/or data importer to enable the respective member of the G+D group to fulfill its obligations under these Binding Corporate Rules. The Privacy Officer shall inform all other members of the G+D Group of the result of the review so that the result of the review can be adopted in the case of comparable transfers.

The members of the G+D Group undertake, in the event that the audit comes to the conclusion that the Binding Corporate Rules cannot be complied with, despite additional measures, to suspend the transfer(s), as well as all other transfers for which the same reasoning would lead to a comparable result, until compliance with these Binding Corporate Rules can be ensured again, or the transfer is terminated. The same applies if a member of the G+D Group is instructed to do so by the competent Data Privacy authority.

The members of the G+D group undertake that the transfer(s) will be terminated by the data exporting member of the G+D group if the Binding Corporate Rules cannot be complied with and compliance with these Binding Corporate Rules is not restored within one month from the suspension. In this case, the personal data transferred prior to the suspension as well as copies thereof shall be returned to the data exporting member of the G+D group or completely destroyed, at the discretion of the data exporting member of the G+D group.

18 Obligations of the data-importing member of the G+D Group in the event of government requests for information

The members of the G+D Group commit to the following:

- The data importing member of the G+D Group will notify the data exporting member of the G+D Group and, if is able to do so (with the assistance of the data exporter, if applicable), the data subject without undue delay if:
 - o It receives a legally binding request for information from an authority under the law of the country of destination or another third country, which concerns personal data transferred under these Binding Corporate Rules. The notification shall contain information about the personal data requested, the authority requesting the information, the legal basis for this request, and the response to the request.
 - o It becomes aware that an authority has direct access to personal data transferred under these Binding Corporate Rules in accordance with the law of the country of destination. The notification shall include all information available to the data importer.
- If the G+D Group member importing the data is prohibited from notifying the G+D Group member exporting the data and/or the data subject, the G+D Group member requesting the information shall use its best efforts to obtain a waiver of such prohibition in order to provide as much information as possible and as quickly as possible. These efforts shall be documented in order to be able to prove them to the data exporting member of the G+D group upon request.
- The data importing member of the G+D group will provide the data exporting member of the G+D group at regular intervals with as much information as possible about requests for information received. Should the data importing member of the G+D group be (partially) prohibited from doing so, it shall immediately inform the data exporting member of the G+D group thereof. The data importing member of the G+D Group shall retain this information for as long as the personal data is subject to the safeguards of these Binding Corporate Rules. It shall be made available to the competent Data Privacy authority upon request.
- The data-importing member of the G+D Group shall review the legality of the request for information, in particular whether it is within the scope of the authority granted to the authority. It shall challenge the request if, after careful consideration, it concludes that there are reasonable grounds to believe that the request is unlawful under the law of the country of destination, applicable international legal obligations and the principles of international legal relations. The data importing member of the G+D Group will appeal under the same conditions. When challenging a request for information, the data-importing member of the G+D group shall apply for interim measures with the aim of suspending the effects of the request for information until the competent judicial authority has ruled on the legality of the request for information. It shall not release the requested personal data until it is obliged to do so under the applicable procedural rules.
- The data importing member of the G+D group shall document its legal assessment and any challenges to the request for information. To the extent permitted by the law of the country of destination, it shall make this documentation available to the data exporting member of the G+D group. Upon request, the data importing member of the G+D Group shall make the documentation available to the competent Data Privacy authority.
- When responding to a request for information, the data-importing member of the G+D Group shall provide the minimum amount of information permitted by a reasonable interpretation of the request for information.

In any case, the transfer of personal data by a member of the G+D Group to a public authority will not be massive, disproportionate and indiscriminate in a way that goes beyond what is necessary in a democratic society.

19 Internal mechanisms for handling complaints

The G+D Group has implemented and is committed to maintaining an internal complaint handling system through which any data subject may file a complaint about a member of the G+D Group's failure to comply with the Binding Corporate Rules.

For this purpose, all important details of the complaint handling procedure and the contact information required to submit the complaint (e-mail address and postal address) are published on the G+D Group's corporate website.

Summary of the G+D BCR

The G+D Group ensures that the Privacy Officers responsible for handling complaints have an appropriate degree of independence in the exercise of their function.

Data subjects may lodge a complaint regarding non-compliance with the Binding Corporate Rules by e-mail or by post. All complaints must be processed without delay and in any case within one month. Taking into account the complexity and the number of complaints, this period of one month may be extended by a maximum of two additional months. In this case, the data subject will be informed accordingly.

In all cases, the responsible Privacy Officer shall inform the data subject, together with the result of the investigation, of his or her right to lodge a complaint with the competent Data Privacy authority or to bring an action before a competent court.

If a member of the G+D Group processes personal data as a processor of a controller belonging to the G+D Group, the Local Privacy Officer responsible for the processor shall notify the controller without undue delay of any complaint it receives regarding the processing of personal data for the controller. In addition, the Local Privacy Officer shall inform the Data Subject that his/her complaint has been forwarded to the member of the G+D Group acting as Controller with regard to his/her personal data.

20 Rights as a third-party beneficiary

The data subject, as a third party beneficiary, has the right to enforce the Binding Corporate Rules against any member of the G+D Group processing the data subject's personal data, provided that the relevant requirements are met and the data subject's claim relates to EEA data.

The rights as a third party beneficiary include judicial remedies for violation of the guaranteed rights and claims for damages.

21 Right to file a complaint and seek redress

The data subject has the right to file a complaint or lawsuit to enforce any of his/her rights as a third party beneficiary. The complaint may be filed either with the competent Data Privacy authority in the EU Member State where he or she has his or her habitual residence, place of work or the place of the alleged breach. The complaint may also be filed with the competent courts of the EU Member States in the area of jurisdiction of the data exporter or with the court having jurisdiction over the group parent company or at its place of habitual residence (at the choice of the data subject). In this regard, the data subject may be represented by a non-profit institution, organization or association duly constituted under the law of a Member State, whose statutory objectives are in the public interest and which is active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of their personal data. The Data Subject is strongly encouraged to first follow the complaint procedures set forth in these Binding Corporate Rules before filing complaints and seeking redress. This is without prejudice to the rights and remedies that data subjects may have under applicable law.

22 Liability

The members of the G+D Group acknowledge that they are liable under these Binding Corporate Rules for a breach of third-party beneficiary rights vis-à-vis data subjects in accordance with the provisions in these Binding Corporate Rules. Data subjects will be supported in exercising their rights and will not be disadvantaged or impeded in any other way.

23 Mutual support and cooperation with Data Privacy authorities

The members of the G+D Group undertake to cooperate and assist each other appropriately in ensuring compliance with these Binding Corporate Rules and in dealing with an inquiry or complaint from a data subject or an investigation or inquiry by a Data Privacy authority.

Furthermore, the members of the G+D Group agree to cooperate with the competent Data Privacy authorities and to comply with the recommendations and decisions of the Data Privacy authorities in the interpretation of these Binding Corporate Rules.

Summary of the G+D BCR

The members of the G+D Group shall provide the competent Data Privacy authority with all information on processing activities covered by these Binding Corporate Rules upon request.

The right to appeal against a decision of the Data Privacy authority remains unaffected. The members of the G+D Group acknowledge that the courts of the respective member state of the Data Privacy authority are responsible for this in accordance with their respective procedural law. The members of the G+D Group undertake to submit to the jurisdiction of this court.

24 Obligations of the members of the G+D Group in their role as processors

G+D group members and all their employees shall process personal data received from customers in the context of commissioned processing as processors exclusively on the customer's behalf and in accordance with the customer's documented instructions, including with regard to the transfer of personal data to a third country, unless this is required by the law of the Union or the Member States to which the G+D group member is subject. In the latter case, the G+D group member will inform the customer of this legal requirement prior to processing, unless the law prohibits such information for important reasons of public interest.

Insofar as a member of the G+D Group cannot guarantee this, for other reasons, it shall inform the customer of this without delay. In such a case, the customer is entitled (in accordance with the provisions of the service agreement) to suspend the data transfer and/or terminate the service agreement.

Insofar as a member of the G+D Group has reason to believe that the obligations arising from these Binding Corporate Rules cannot be fulfilled due to the legal provisions in force or to be applied in the future and that this is likely to significantly impair the guarantees provided by the Binding Corporate Rules, the member of the G+D Group shall immediately inform the Group Privacy Officer, the customer concerned (who in this case is entitled to suspend the data transfer or - taking into account the provisions of the service agreement - to terminate it) and the supervisory authority responsible for the respective customer. The Group Privacy Officer will then inform the management of the G+D Group.

Duty to cooperate and support

The members of the G+D Group undertake to assist the customer in complying with the legal provisions (such as the obligation to respect the rights of the data subject, to respond to requests from data subjects or to respond to investigations or requests from a supervisory authority), which are further detailed in these Binding Corporate Rules. Such support furthermore includes, for example, disclosing processing operations by additional processors in order to enable the controller to provide the data subject with correct information in terms of content. In particular, the members of the G+D Group undertake to provide all relevant information within the scope of their possibilities in order to assist the customer in the fulfillment of its obligations, such as

- (a) inform the data subject about the processing of his/her personal data,
- (b) correct, delete or block the personal data processed on behalf of the customer at the request of the customer and/or a data subject or in accordance with the law and
- (c) respond to investigations and inquiries by regulatory authorities,
- (d) to comply with the customer's obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the member of the G+D Group.

to support.

At the customer's request, the members of the G+D Group will take appropriate technical and organizational measures, to the extent possible, to enable the customer to comply with its obligations to respond to requests from data subjects exercising their rights as described in Chapter III of the GDPR. This includes providing the customer with any useful information to help the customer safeguard the rights of the Data Subjects, in particular to update, correct, erase or, once identification is no longer necessary, delete or anonymize the personal data.

The members of the G+D group shall respond to, assist and support any requests of the customer for cooperation in this regard within a reasonable time and within reason. The members of the G+D group shall

Summary of the G+D BCR

provide the customer with all information necessary to demonstrate compliance with their obligations under Article 28 para. 3 lit. h) of the GDPR. For each customer, all members of the G+D group shall for this reason keep records of all categories of processing activities carried out on behalf of each customer. These records are kept in writing, including in electronic form, and are made available to the supervisory authority upon request. The members of the G+D Group support the customer in implementing appropriate technical and organizational measures to comply with the Data Privacy principles and facilitate compliance with the requirements set out in the Binding Corporate Rules in practice, such as Data Privacy-friendly default settings (Privacy by Design and Privacy by Default).

Rights of the data subject

The customer is responsible for processing requests from a data subject regarding access, correction, deletion or blocking of the respective personal data.

To the extent that a member of the G+D Group receives a direct inquiry from the data subject regarding his or her personal data, such member shall forward the inquiry to the respective customer without responding to it, unless otherwise agreed in the service agreement.

Technical and organizational security measures

All members of the G+D Group have implemented and undertake to maintain appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing, in particular when personal data is transmitted over a network. All employees as well as members of the G+D Group comply with these technical and organizational measures.

Employees of the G+D Group have access to personal data only to the extent necessary to perform their duties and for the applicable purpose. All employees who have access to personal data are obliged to treat this personal data with appropriate confidentiality.

These technical and organizational measures shall at least comply with the requirements of the applicable law specified for the customer in the service agreement, as well as with the specific security and confidentiality measures specified in the service agreement. These technical and organizational measures shall ensure a level of security appropriate to the risks inherent in the processing of personal data. The processing of special categories of personal data is subject to increased security measures.

Duty to report data security breaches

Each member of the G+D Group shall immediately inform the customer of any unauthorized access, unlawful destruction, accidental loss or alteration of personal data processed on behalf of the customer.

Obligations after termination of the service agreement

Depending on the terms of the service agreement (for example, with respect to data format, time and price), each member of the G+D Group that processes personal data on behalf of the customer under the service agreement and these Binding Corporate Rules will, at the request and option of the customer, as may be reflected in the service agreement, upon termination of the agreement, either return the personal data and copies thereof to the customer or delete the personal data under its control and confirm to the customer that it has done so. To the extent that applicable law requires the continued storage of the transmitted personal data, the customer shall be informed of this by the respective member of the G+D Group and the latter shall assure that

(a) it guarantees the confidentiality of the personal data and

(b) it will no longer actively process the personal data.

25 Update and amendment of the Binding Corporate Rules

The Binding Corporate Rules may be updated and/or amended in accordance with the applicable internal guidelines of the G+D Group, for example if it becomes necessary to take into account changes in the regulatory framework or the data processing procedures within the G+D Group.

26 Effective date

The Giesecke+Devrient Binding Corporate Rules came into force on 02.02.2018.