

Summary of Giesecke+Devrient Group's Binding Corporate Rules

1. Purpose

Giesecke+Devrient Group ("G+D") is an innovative, transnational company, which means there is a necessity for it to both hold information and use it effectively in order to achieve its business objectives in all business sectors. Advanced information and communications technologies such as the internet, intranet, and email, play an increasingly important role with respect to the accessing of information and its shared use. These technologies enable G+D to quickly and effectively make and implement business decisions, and in this way to fulfill customers' rising expectations.

At the same time, technological transformation is associated with certain risks related to the exchange of information, which G+D – as a responsible company – is committed to taking into account. Employees and contractors, as well as existing and potential customers all have a justified interest in ensuring that the data protection rights of the data subject are protected in the processing and use of personal data.

2. Organizational Scope

The BCR applies to all companies that have joined G+D Group.

3. Description

As part of its commitment to a high degree of data protection, G+D Group has introduced Binding Corporate Rules. These have the purpose of safeguarding assurances and guarantees relating to appropriate levels of data protection pursuant to General Data Protection Regulation (EU 2017/679) in relation to any instance of personal data being processed on behalf of companies in G+D Group in its role as controller, as well as for any instance of processing by a member of G+D Group in its role as processor, and in particular with respect to the transfer of personal data outside the EEA.

4. Training Program

G+D Group has introduced 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 who are involved in the collection of personal data for the development of systems for processing personal data, and the company commits to maintain this training program.

5. Audit Program

Based on a risk-oriented audit program, G+D Group has introduced a comprehensive program to verify that the Binding Corporate Rules are being complied with, and commits to maintaining this program. The audit program encompasses all aspects of the Binding Corporate Rules and includes methods that ensure the implementation of corrective actions.

6. Actions in the event that national legislation prevents compliance with the Binding Corporate Rules

Members of G+D Group shall report to customers any legally binding request from a law enforcement agency to disclose personal data, unless this is legally prohibited, for example due to it being impermissible under criminal law to compromise the confidentiality of a law enforcement agency.

7. Mechanisms for handling complaints

G+D Group has introduced a system for handling complaints and commits to maintaining this system, by way of which any data subject may submit complaints if a member of G+D Group does not comply with the Binding Corporate Rules.

All key details related to this purpose, for the procedure for handling complaints, as well as the contact information required to submit complaints (e-mail address and postal address) are published on the G+D Group corporate website.

8. Data subjects' rights and legal remedies

As a third-party beneficiary, the data subject has the right to enforce the Binding Corporate Rules against any member of G+D Group that processes the data subject's personal data. Third-party beneficiary rights include judicial remedies in the event of a breach of the guaranteed rights and claims to compensation. For the enforcement of their rights as a third-party beneficiary, the data subject has the right to submit complaints to the relevant data protection authority and/or to assert claims within the court jurisdiction of the data exporter or before the appropriate court that is relevant for the parent company. The data subject is explicitly encouraged to initially pursue the complaints procedure outlined in these Binding Corporate Rules before submitting complaints and claims.

9. The customers' rights and legal remedies

In the event of any member of G+D Group breaching its obligations as they arise from these Binding Corporate Rules, or, where applicable, from the service level agreement as determined by the relevant law, that member shall be liable to the customer for its breach. In addition, the customer shall be entitled to assert these Binding Corporate Rules as third-party beneficiary rights with respect to any member of G+D Group that functions as a processor with respect to personal data that G+D Group has received from the customer, insofar as this member of G+D Group has breached its respective obligations arising from these Binding Corporate Rules.

10. Liability

G+D Group members accept that they are liable to data subjects for any breach of third-party beneficiary rights under these Binding Corporate Rules in accordance with the provisions of the Binding Corporate Rules. Data subjects will be assisted in exercising their rights and not disadvantaged or unduly inhibited in any other way.

11. Mutual Support and Collaboration with Supervisory Authorities

Members of G+D Group commit to appropriately collaborating and providing mutual support in ensuring compliance with these Binding Corporate Rules, and in dealing with any inquiries or complaints by a customer or where applicable, a data subject, and during investigations or inquiries by a supervisory authority.

In addition, members of G+D Group agree to collaborate with the relevant supervisory authorities and to implement the recommendations of supervisory authorities with respect to the interpretation and application of these Binding Corporate Rules.

12. Updates and Amendments to the Binding Corporate Rules

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

13. The Relationship between National Law and the Binding Corporate Rules

All instances of the processing of personal data by a member of G+D Group are subject to the applicable local law. These Binding Corporate Rules apply in addition to – and not instead of – other rights and legal remedies that the data subjects may have in accordance with applicable local law; all of these rights and legal remedies remain unaffected by the Binding Corporate Rules.

If the applicable local law specifies a higher level of protection for personal data than is provided for in these Binding Corporate Rules, local law shall take precedence over these Binding Corporate Rules.

14. Obligations of Members of G+D Group in their Role as Controller

Purposes of Processing and Purpose Limitation

Personal data should only be processed where this is necessary for one or more of the purposes set out below, or is required by the law applicable in each case.

- Personal data that employees of the companies in G+D Group will process for the purpose of HR management, including general management of the employment relationship, employee management in the matrix structure of G+D Group, global collaboration, training programs, performance and development planning, successor planning, guaranteeing an accessible talent pool for key roles within G+D Group, global mobility of employees, and ensuring 24/7 IT support. Special categories of personal data relating to employees in G+D Group are only processed when necessary for entering into and implementing an employment relationship, as well as for implementing obligations and specific rights in the area of employment law. They are only processed for other purposes where this is required by the applicable law, or if the relevant employees have explicitly consented to the processing of their data.
- Personal data that relate to employees or points of contact within business partner organizations are only processed for the purposes of implementing and managing relationships with business partners; for entering into and implementing contractual relationships; for enabling global collaboration for customer projects; for providing customer service and support; and for ensuring compliance with legal specifications.
- Personal data may not be further processed in a manner that does not correspond to the purposes for which it was originally collected.

Data Quality and Proportionality

G+D Group ensures that the processed personal data are accurate and complete, and as up-to-date as is reasonably required for the respective purpose. G+D Group takes all appropriate action to rectify or erase any personal data that are inaccurate, incomplete, or out of date, taking into account the purpose for which they were collected or processed.

The processing of personal data is restricted to data that are appropriate and necessary for the respective purpose, and must not go beyond the purposes for which these data are collected and/or further processed. If personal data are no longer required for the respective purposes, their further processing is not permitted; in this case they must be erased or destroyed.

Legal Basis for the Processing of Personal Data

Personal data should only be processed for one or more of the following reasons:

- Processing necessary for the fulfillment of a contract in which the data subject is a contractual party, or for the implementation of pre-contractual measures that take place at the request of the data subject; or
- Processing necessary for the fulfillment of a legal obligation to which the controller is subject; or
- Processing necessary in order to protect the vital interests of the data subject; or
- Processing necessary for the performance of a task in the public interest or in the legitimate exercising of public powers, which has been transferred to the controller or a recipient to whom the data have been transmitted; or
- Processing necessary in order to realize the justified interest that is safeguarded by the controller or by the recipient/recipients to which the data are transmitted, unless these interests are suspended by overriding interests in safeguarding the fundamental rights and freedoms of the data subject.

If none of the reasons specified above apply, G+D Group must obtain the unambiguous consent of the data subject before processing their personal data. The data subject may revoke their consent at any time with immediate effect, unless otherwise specified by the applicable law. In this case, G+D shall cease all further processing unless processing is required by the applicable law, or is absolutely essential in the course of a contractual relationship with the data subject.

Legal basis for the Processing of Special Categories of Personal Data

G+D Group commits to only processing special categories of personal data if one or more of the following reasons apply:

- The data subject has explicitly consented to the processing of these special categories of personal data; or
- Processing is necessary in order to accommodate the obligations and specific rights of the controller in the area of employment law, insofar as this is permitted based on the national legislation and insofar as appropriate safeguards are provided for; or
- Processing is necessary for the protection of the vital interests of the data subject or another natural person, and the data subject is unable to provide their consent for physical or legal reasons; or
- Processing takes place on the basis of appropriate guarantees from a political, philosophical, religious, or union-oriented foundation, association, or other not-for-profit organization as part of their legal activities, and subject to the requirement that processing relates only to members of the organization or to individuals who have regular contact with these organizations, and that the data are not disclosed externally without the consent of the data subject; or
- Processing refers to special categories of personal data that the data subject has manifestly made public; or
- Processing of special categories of personal data is necessary for the assertion, exercising, or defense of legal entitlements; or
- Processing of special categories of personal data is necessary for the purposes of health care, medical diagnosis, the provision of health care or treatment, or the management of health services, and these special categories of personal data are processed by medical staff who are subject to professional secrecy in accordance with national law including regulations issued by the relevant national bodies, or by other individuals who are subject to a corresponding secrecy obligation.

Information for Data Subjects

Members of G+D Group are obliged to provide data subjects with the following information as a minimum for processing the personal data, insofar as the data subjects do not yet already have this information:

- The identity of the member of G+D Group who is acting as the controller, and this member's representative (if applicable),
- The processing purposes for which the data are intended, and
- All additional information such as the categories of the relevant personal data, the recipients or categories of the recipients of the data, and the existence of rights to access and rectification of the data subject's data, insofar as these are necessary in order to guarantee the data subject lawful and fair processing, taking into account the specific circumstances under which the data are processed.

Data subjects shall be appropriately informed in a similar manner of the processing and/or transfer of their personal data on G+D Group's corporate website, as well as through references to this website where applicable, in business communications, and in corporate brochures.

The Right to Access, Rectification, Erasure, Making Unavailable, and Objection

Data subjects have the right to receive, freely and unhindered – at appropriate intervals, without unreasonable delay or excessive costs – a copy of all personal data relating to them that are processed by the respective member of G+D Group in their capacity as a controller with respect to their personal data, including information about the purposes of processing, all available information about the origin of the personal data and the recipients and categories of recipients to whom the personal data are transferred.

Depending on the case, data subjects may also be entitled to demand the rectification, erasure, or making unavailable of their personal data, particularly if the personal data are incomplete or inaccurate, unless the processing of these personal data in their unchanged form is required by the applicable law. Data subjects have the right to demand from the controller that recipients to whom the data have been transmitted are informed of every rectification, erasure and making unavailable of those data, unless this proves to be impossible or involves the use of a disproportionately high level of resources.

For compelling and justified reasons based on their particular situation, data subjects have the right to submit an objection to the processing of their personal data at any time, unless this processing is required by the applicable law. In the event of a justified objection, G+D Group commits to cease processing.

In addition, data subjects have the right to submit an objection to the processing of their personal data for the purposes of direct marketing (where applicable), free of charge.

Data subjects may assert their rights stated above by contacting the Privacy Officer relevant to the respective member of G+D Group who is acting as the controller with respect to the data subject's personal data. The contact information for the relevant Privacy Officer for each member of G+D Group is published on the G+D Group corporate website.

Security and confidentiality of data

All members of G+D Group have implemented appropriate technical and organizational measures, and commit to maintaining these in order to protect personal data against accidental or illegal destruction and accidental loss, alteration, unauthorized disclosure, and unauthorized access, as well as against all other forms of illegal processing, particularly when personal data are transferred within a network in the context of processing.

Relationships with Processors who are Members of G+D Group

In their role as processors, members of G+D Group who process personal data on behalf of a controller that is part of G+D Group are also committed to these Binding Corporate Rules, to the scope applicable for them.

Processor Obligations

Members of G+D Group who act as processors agree to processing personal data received from a controller that is part of G+D Group only on behalf of the controller and pursuant to the controller's instructions; in addition, such members agree to implement appropriate technical and organizational measures in order to protect personal data against accidental or illegal destruction and accidental loss, alteration, unauthorized disclosure, and unauthorized access, as well as against all other forms of illegal processing, particularly when personal data are transferred within a network in the context of processing.

In their role as processors, these members of G+D Group are also generally obliged to give aid and assistance to controllers that are part of G+D Group, in the fulfillment of their obligations pursuant to these Binding Corporate Rules (particularly with respect to the controllers' obligations relating to safeguarding the rights of data subjects).

Controller Obligations

Controllers that are part of G+D Group must select a processor that offers a sufficient guarantee with respect to technical and organizational security precautions for the processing to be performed, and ensure compliance with these measures.

In addition, controllers may only commission these processes by means of a written contract pursuant to Articles 28 GDPR and the applicable local law. In particular, the contract must stipulate that the processor only acts at the instruction of the controller, and implements appropriate technical and organizational security measures – insofar as these do not already apply – pursuant to these Binding Corporate Rules.

Transfer and Onward Transfer of Personal Data to Controllers outside G+D Group

If, in their role as controller, a member of G+D Group intends to transfer personal data to an external controller in a third country that does not have a reasonable level of protection, the controller is obliged to take appropriate action for the fulfillment of those requirements arising from Art. 44 seq. GDPR, for example by applying the standard contractual clauses (for the transfer of personal data to third countries) adopted by the European commission by means of Decision No. 2004/915/EC.

Transfer of Personal Data to Processors outside G+D Group

If, in their role as controller, a member of G+D Group intends to commission an external processor, the controller commits to fulfill its obligations arising from these Binding Corporate Rules in order to meet the requirements of Art. 32 GDPR, and to ensure that these requirements can be applied at national level.

If the registered office of the external processor is in a third country that does not have an appropriate level of data protection, the member of G+D Group that is acting as controller is also obliged to take appropriate action for the fulfillment of the requirements arising from Art. 44 seq. GDPR, for example by applying the standard contractual clauses (for the transfer of personal data to third countries) adopted by the European Commission by means of Decision No. 2010/87/EC.

Measures to be Taken in the event of National Legislation Preventing Compliance with the Binding Corporate Rules

Should a member of G+D Group have any reason to assume that the legislation applicable to it could prevent it from fulfilling its obligations with respect to these Binding Corporate Rules, and should this have a significant effect on the assurances guaranteed through the Binding Corporate Rules, the G+D Group member shall inform the Group Privacy Officer without delay, unless prevented from doing so by a law enforcement agency or by the applicable law. The Group Privacy Officer shall notify the Management Board of G+D Group. Should the G+D Group member be acting as a processor in line with these Binding Corporate Rules, it shall also inform the G+D Group controller from whom it has received the personal data, unless prevented from doing so by a law enforcement agency or by the applicable law.

If the obligations arising from the Binding Corporate Rules contradict national law, the Management Board of G+D Group shall decide on the measures to be taken, consulting the responsible data protection authorities in case of doubt.

15. Obligations of the Members of G+D Group in their Role as Processors

The members of G+D Group and all of their employees shall process personal data received from customers exclusively in their capacity as processors acting on behalf of the Group, and in accordance with the instructions of the Group.

Should a member of G+D Group be unable to guarantee this, for any reason whatsoever, it shall inform the customer accordingly without delay. In such cases, the customer (in accordance with the provisions of the service level agreement) shall be entitled to stop the data transfer and/or cancel the service level agreement.

Where a G+D Group member has any reason to assume that the obligations arising from these Binding Corporate Rules cannot be fulfilled due to legal provisions currently in force, or which will be applicable in the future, and where this is likely to affect the guarantees provided through these Binding Corporate Rules, the G+D Group member shall notify the Group Privacy Officer, the customer affected (which shall be entitled to end the data transfer or cancel the service level agreement in line with the provisions set forth therein) and the supervisory authority responsible for the respective customer, immediately and without culpable delay. The Group Privacy Officer shall then notify the Management Board of G+D Group.

Duty to Cooperate and Provide Assistance

Members of G+D Group shall be obliged to assist customers in complying with the applicable legal provisions (such as the obligation to respect the subjective rights of the data subject, respond to complaints, and be accountable to a supervisory authority) that are also set out in even further detail in these Binding Corporate Rules. Such assistance also includes, for example, ensuring the transparency of, or disclosing, the handling processes of other processors in order to allow the controller to access accurate information with respect to the data subject. In particular, G+D Group members shall be obliged to provide all relevant information pertaining to the customer in the fulfillment of their obligations, within the scope of their capabilities; for example (a) informing the data subject about the processing of their personal data, (b) rectifying or erasing the personal data processed on behalf of the customer, or making these data unavailable upon request by the customer and/or a data subject, or in accordance with the relevant legal provisions, and (c) responding to requests from the supervisory authorities. Upon request from the customer, G+D Group shall take all necessary measures to update, rectify or erase the respective personal data, or erase or anonymize these data from the point at which the identification form is no longer required.

All affected members of G+D Group shall inform all other G+D Group members to which personal data have been transmitted about any rectification, erasure or anonymization of same.

Members of G+D Group shall assist the customer and respond to all requests concerning any form of cooperation and assistance within an appropriate period, provided that this is possible and reasonable.

Rights of the Data Subject

The customer shall be responsible for answering requests from any data subject with regard to access to, or rectification, erasure or making unavailable of his/her respective personal data.

Where a member of the G+D Group receives a direct request from the data subject in relation to his/her personal data, that member shall forward the request to the customer without answering it, unless otherwise specified in the service level agreement.

Technical and Organizational Security Measures

All members of G+D Group have implemented appropriate technical and organizational security measures, and commit to maintaining these in order to protect personal data against accidental or illegal destruction and accidental loss, alteration, unauthorized disclosure, and unauthorized access, as well as against all other forms of illegal processing, particularly when personal data are transferred within a network in the context of processing.

All employees and members of G+D Group shall comply with these technical and organizational security measures.

The employees of G+D Group shall only have access to personal data to the extent deemed necessary for the performance of their duties and the respective applicable purpose. All those who have access to personal data shall be obliged to treat these personal data with the appropriate confidentiality.

These technical and organizational security measures must at least fulfill the requirements set out in the law applicable to the customer as indicated in the service level agreement, as well as the security and confidentiality measures stipulated in the service level agreement.

These technical and organizational measures shall guarantee a level of security that corresponds to the risks associated with the processing of personal data. The processing of special categories of personal data is subject to increased security risks.

Duty of Disclosure in the event of Breaches of Data Security

Every member of the G+D Group shall inform the customer without delay in the event of any unauthorized access to, or unlawful destruction, accidental loss, or alteration of personal data being processed on behalf of the customer.

Obligations Following Termination of the Service Level Agreement

Following termination of the service level agreement, every member of G+D Group that processes personal data on behalf of a customer as part of a service level agreement and within the scope of these Binding Corporate Rules shall be obliged to continue to fulfill certain obligations for a period and of a nature to be specified by the customer, and which may also be outlined in the service level agreement, regardless of the conditions set forth in the service level agreement (e.g. concerning the data format, the duration of the agreement and pricing), and shall either return the personal data under its control [or under the control of the member of the G+D Group] or erase them permanently and confirm to the customer that this has been done.

Where the applicable law prohibits the full or partial return or erasure of personal data processed on behalf of the customer, the customer shall be informed of this by the respective member of G+D Group, which shall ensure that it (a) guarantees the confidentiality of the personal data and (b) no longer actively processes the personal data.