Fostering trust in the digital transformation

GFT Group Data Protection Policy

Owner:
Group Data Protection

Version:
3.5

Date of Publication:
12 April 2024

Classification:
Internal

Revision History

Rev. No	State	Date	Comment	Acting Role
0.1	draft	2012-03-08	first review cycle completed	Data Protection Officers, Information Security Officers, Chief Security Officer, Officer, Group Legal
0.2	enhanced draft	2012-03-14	second review cycle completed	Division Delegates
0.3	proposal	2012-03-20	pre-approval completed	Data Protection Officers, Chief Privacy Officer, Privacy Executive Representative
0.4	final proposal	2012-03-28	final proposal approved	Executive Board, Global Business Committee
1.0	approved version	2012-03-29	promoted to approved version and cleared for distribution	Chief Privacy Officer
1.1	proposed update	2013-04-03	proposed update approved	Privacy Steering Committee
1.2	approved version	2013-04-04	promoted to approved version and cleared for distribution	Chief Privacy Officer
1.3	draft update	2014-02-28	modified to align with organizational changes and EU Data Protection Reform	Chief Privacy Officer
1.4	enhanced update	2014-03-18	draft enhanced and distributed for approval	Chief Privacy Officer
2.0	approved version	2014-12-12	final proposal approved	Executive Board, Privacy and Security Steering Committee, Global Business Committee, emagine Management, Group Financial Committee, Data Protection Office
2.1	proposed minor update	2015-12-12	modified to align with organizational changes and EU Data Protection Reform	Chief Privacy Officer
2.1	approved version	2016-07-25	proposed minor update approved	Privacy and Security Steering Committee, Data Protection Office
2.2	proposed minor update	2017-03-01	modified to cope with globalization of GFT	Chief Privacy Officer
2.2	approved version	2017-03-31	proposed minor update approved	Privacy and Security Steering Committee, Data Protection Office
2.3	proposed minor update	2017-06-30	modified to cope with globalization of GFT	Chief Privacy Officer

2.3	approved version	2017-07-24	proposed minor update approved	Privacy and Security Steering Committee, Data Protection Office
3.0	approved version	2019-04-04	major update approved	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Executive Board (GEB)
3.1	proposed minor update	2021-07-31	Updated the scope of applicability, included new Group-wide roles and added DP risk stage model	Deputy Chief Privacy Officer
3.1	approved version	2021-09-22	Minor update approved	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Policy Management, Group Executive Board (GEB)
3.2	proposed minor update	2022-02-07	Updated Data Protection Training Requirements	Privacy Leadership Team
3.2	approved version	2022-04-05	Minor update approved	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Policy Management (GPM) or Group Executive Board (GEB)
3.3	approved version	2022-12-16	Minor update approved	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Policy Management (GPM) or Group Executive Board (GEB)
3.4	approved version	2023-07-28	Minor update approved (moved "Privacy by Design" to Chapter 1)	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Policy Management (GPM) or Group Executive Board (GEB)
3.5	approved version	2024-04-12	Minor update approved (Management of Policy Changes added, scope of applicability updated due to Sophos Integration, role of Data Protection Manager replaced by Privacy Engineer, Chief Digital Officer replaced by Group Technology Office, section "Responsible AI" added, Annex added)	Privacy Officer Committee (POC), Privacy and Security Steering Committee (PriSecCo), Group Policy Management (GPM)

Document Summary

Policy Title	GFT Group Data Protection Policy
Classification	Internal
Author	Chief Privacy Officer
Approver for Major Versions	Group Executive Board, Privacy and Security Steering Committee, Group Data Protection, Privacy Officer Committee
Approver for Minor Versions	Privacy and Security Steering Committee, Group Data Protection, Privacy Officer Committee, Group Policy Management or Group Executive Board
Date of initial Approval	29.03.2012
Date of last Approval	12.04.2024
Policy contact	dataprotection.group@gft.com
Functional Applicability	GFT Group
Geographical Applicability	Belgium, Brazil, Canada, Chile, Colombia, Costa Rica, France, Germany, Hong Kong, India, Italy, Mexico, Panama, Peru, Poland, Romania, Singapore, Spain, Switzerland, UK, USA, Vietnam
Original Issue Date	29.03.2012
Last Review Date	11.03.2024
Next Review Date	12.04.2025
Version	3.5

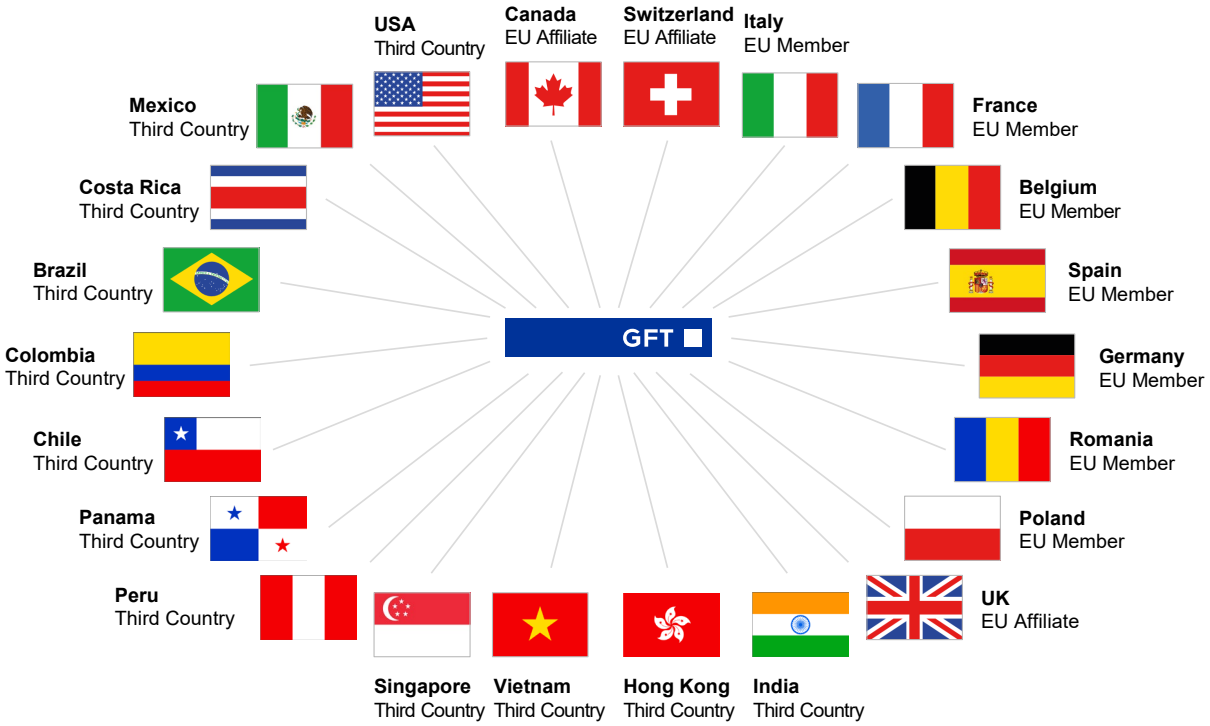
Statement of Proprietary Information

Table of contents

1 Objective, Purpose and Scope

The objective of the GFT Group Data Protection Policy is to explain the framework of the GFT Group which establishes and maintains an adequate and common level of Data Protection within the GFT Group and at GFT Group's interfaces to clients, suppliers and partners. The underlying purpose is to support GFT Group's global delivery model in GFT and to ensure efficient and standardized processing in Corporate Services in compliance with legal requirements in Data Protection and in recognition of the rights and freedoms of the data subjects. GFT Group considers Data Protection as integral part of its everyday business operations.

The scope of the GFT Group Data Protection Policy is global that means it covers all types of GFT Group operations in all business functions and processes, all legal units directly or indirectly affiliated with GFT Technologies SE, all countries where GFT Group is maintaining operations. In particular, the GFT Group Data Protection Policy[1] is relevant for those countries which do not have in place a Data Protection related legislation and/or an acceptable level of Data Protection as defined by the European Commission.



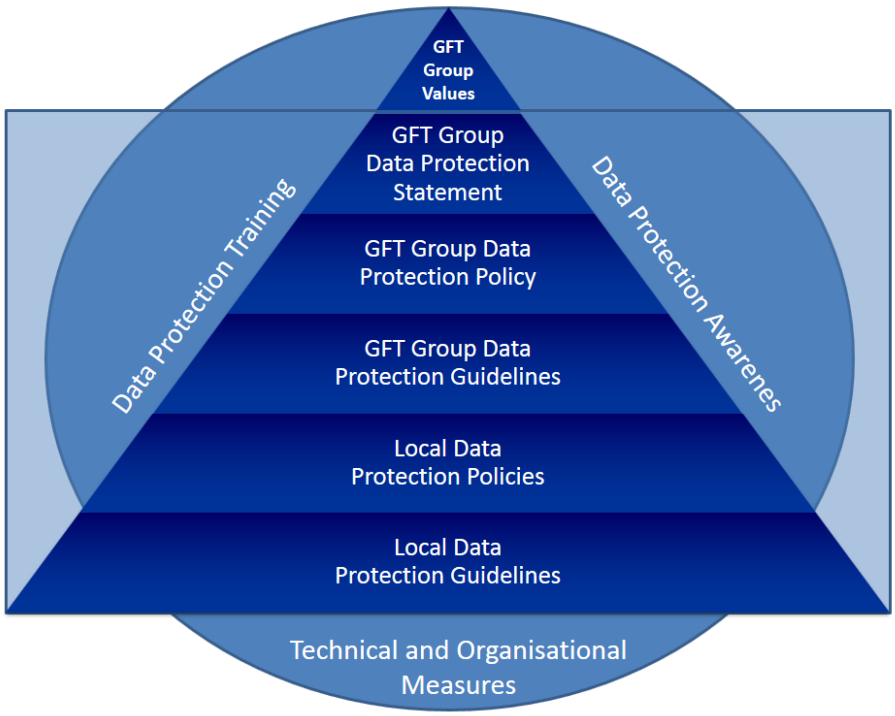
The notions of "Data Protection" and "Privacy" used throughout this document refer to the handling of legal requirements which regulate the processing of personal data. The term 'personal data' means any information relating to a 'data subject". A 'data subject' represents an identified or identifiable natural person.

The term 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Further terms and explanations are provided in the GFT Group Data Protection Glossary.

[1] *guidance for implementing the GFT Group Data Protection requirements in those countries will be given in the corresponding Local Data Protection Policies (if appropriate)*

1.1 GFT Group Data Protection Framework

The GFT Group Data Protection Policy is not a self-contained document but is the core element of GFT Group Data Protection Framework which based on a value driven approach made fast at the GFT Group Values and the GFT Group Data Protection Statement. Policy and Guidelines issued by Group Data Protection represent the core of the GFT Group Data Protection Framework which may be amended by Policies and Guidelines issued by Local Data Protection (if appropriate).

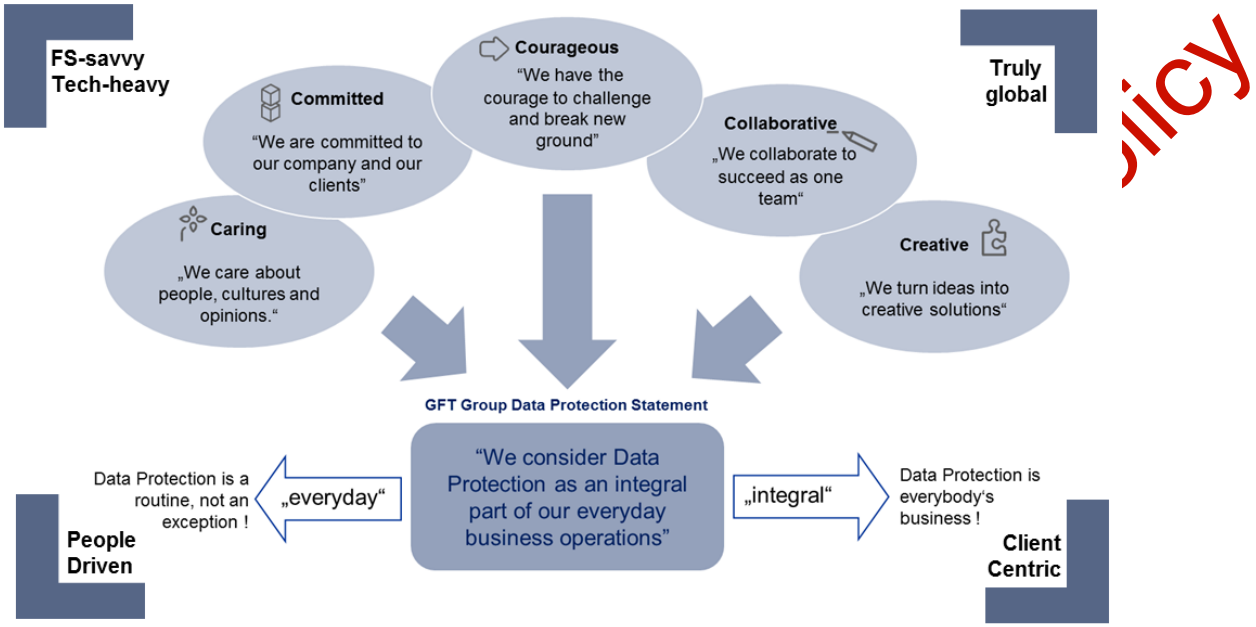


Revisions of the GFT Group Values have to be approved by the GFT Administration Board and the Group Executive Board. Revisions of the GFT Group Data Protection Statement and major versions of the GFT Group Data Protection Policy have to be approved by the Group Executive Board, Privacy and Security Steering Committee and Privacy Officer Committee. Minor versions of the GFT Group Data Protection Policy have to be approved by Group Data Protection. Major versions of Group Data Protection Guidelines have to be approved by the Privacy Officer Committee. Minor version of Group Data Protection Guidelines have to be approved by Group Data Protection. Any Local Data Protection Policy or Guideline has to be approved by Local Data Protection responsible and the Chief Privacy Officer.

All elements of the GFT Group Data Protection Framework are described in the GFT Group Data Protection Guideline for the Data Protection Framework.

1.2 GFT Group Values & Statement

GFT Group values are common principles in the area of teamwork, client relationships and working environment and represent the cornerstone of GFT Group's company culture. Combined with a clear vision, they are the basis for GFT Group's long-term growth and success. GFT Group's vision in Data Protection is summarized in the GFT Group Data Protection Statement which is built on the GFT Group values:



"Integral" means that Data Protection is everybody's business and describes a work habit which do consider Data Protection not just at the end, but in the beginning and all along each relevant business process and is also known as "Data Protection by Design and by Default". "Everyday" emphasizes the fact that Data Protection is not only relevant in extraordinary projects but in daily routines in particular.

1.3 Data Protection Risk Stage Model

GFT Group Data Protection functions use the Risk Stage Model for risk maturity evaluation and its easier evaluation in context of Group-wide risk appetite by appropriate risk owners. Privacy relevant risks are placed on a scale from 0 to 3 in accordance with following Risk Stage Model:

Stage 0: Blind Risk Acceptance

Accountable Management (on local or functional level) sets up relevant business processes under high pressure and no proper involvement of Data Protection. Accountable Management accepts any related risk (even without being aware of the risks specifically) while considering to move as soon as possible to Stage 1.

Stage 1: Critical Risk Awareness
Accountable Management involves Data Protection late in the setup of an already existing business processes or planning of business processes whose implementation is under high pressure and does not allow any hesitation. Although time and/or resource constraints prevents timely resolution, Data Protection is able to identify relevant risks and/or relevant need for action. Accountable Management accepts any related risk (which is more or less visible at this stage) while considering moving as soon as possible to Stage 2.

Stage 2: Critical Risk Containment
Data Protection focuses on the most visible / critical risks first and may start with most simple or pragmatic mitigations options to provide fastest and most efficient risk containment. In such a situation, accountable Management has to accept some gaps in the resolution of critical risks (which may require actually less pragmatic or more time-consuming approach for fully effective treatment) and no mitigation of less critical or less visible risks while considering to move as soon as possible to Stage 3 for specific risks.

Stage 3: Diligent Risk Minimization
Guided by Data Protection, accountable Management selects specific risks either from critical risks with not fully effective mitigation or less critical risks with no mitigation at all. Data Protection provides recommendations for the most effective treatment of these specific risks. Accountable Management has to take care of the effective and timely mitigation of these specific risks while accepting remaining gaps in the treatment of non-specific risks.

Risk Stage 0 (Blind Risk Acceptance) should be avoided. Any case of Risk Stage 0 (Blind Risk Acceptance) and Risk Stage 1 (Critical Risk Awareness) should be brought by accountable management to the attention of a higher authority for review and approval. Approval of Risk Stage 0 (Blind Risk Acceptance) will be granted on an exceptional and temporary basis only.

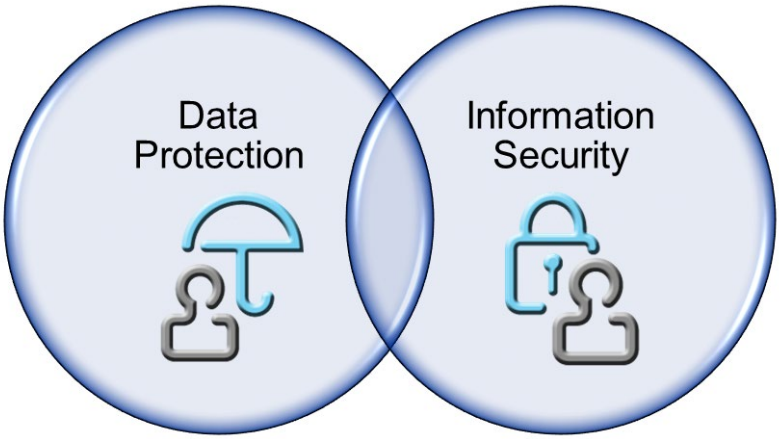
1.4 Global & Local Policies

The GFT Group Data Protection Policy defines the operational structure and minimum implementation requirements for the Data Protection organization on GFT group and local level. However, local amendments on policy or guideline level may be necessary to cope with additional country or business specific requirements in Data Protection. Nonetheless, these local policies and guidelines must comply with the provisions of the GFT Group Data Protection Policy and Guidelines and require approval from Group Data Protection before publication and/or implementation. Client or vendor agreements with Data Protection regulations are considered as special type of local Data Protection Policies or Guidelines. Any special type of

local Data Protection Policies or Guidelines has to be reviewed and approved by the responsible Privacy Officer who has to report to and obtain acceptance from Chief Privacy Officer for any material deviation in some special type of local Data Protection policies from the principles laid out in the GFT Group Data Protection Policy.

1.5 Data Protection & Information Security

Data Protection and Information Security seem to be both concerned with protecting information but have different point of view on the matter: Data Protection focuses on natural persons, the personal data belonging to them and the risks for rights and freedoms of natural persons posed by the processing of their personal data.. Information Security focuses on hardware, software and other facilities containing sensitive information assets (e.g personal data, business secrets, intellectual property) and the mitigation of risks for the organization which could compromise confidentiality, integrity and availability of these information assets.



Requirements for Information Security essential from Data Protection point of view are stated in this document (see section 4.6 of this document) or in the GFT Group Data Protection Guideline for the TOM Standard in more details Further details on Information Security are covered in dedicated GFT Group Security Policies and Procedures.

1.6 Accountability

GFT Group Data Protection is responsible for observing the global Data Protection regulatory environment, analyzing the impact of this environment on GFT operations and developing and maintaining GFT Group's Data Protection Framework in alignment with corresponding requirements. GFT Local and Function Data Protection is responsible for implementing processes in alignment with the policies defined by GFT Group Data Protection, adding country or business specific amendments, providing guidance on how to comply with the standards and identifying deviations from these standards.

GFT Business Representatives in general and Process Activity Owners in particular are responsible for being able to demonstrate the compliance with the data protection policies and guidelines on GFT group Furthermore, they are responsible to ensure that root causes of recurring deviations from the expected standards are resolved and Data Protection Impact Assessments for relevant processing activities are carried out as an integral part of the everyday business operations. Finally, they are responsible for providing adequate resources to Data Protection and for choosing an adequate level of technical and organizational

measures for the processing activities. Responsibility to comply with country specific Data Protection related legal/regulatory requirements resides with the Local Management.

GFT employees are responsible for acting in everyday business operations in compliance with applicable legislation in Data Protection and with provisions of the GFT Group Data Protection Policy and Guidelines and relevant local Data Protection Policies and Guidelines. In particular, every employee involved in the handling of personal data has to treat personal data as confidential, take care of integrity and availability of the personal data, process personal data based on legitimate purposes only, respect the rights of the data subjects and escalate data breaches without hesitation.

1.7 Privacy by Design & by Default

Data Protection by Design considers appropriate technical and organisational measures which are designed to implement relevant data protection principles in an effective manner and to integrate relevant safeguards into the processing of personal data. Data Protection by Default considers appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Data Protection by Design and by Default does not only take place at the time of the processing (execution time) but already at the time of the determination of the means for processing (design time) in order to meet the requirements of applicable data protection legislation and protect the rights of data subjects while taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as relevant data protection risks.

Besides data minimization, pseudonymisation, transparency from the perspective of the data subject and the implementation of an adequate level of security, GFT's Data Protection by Design and by Default approach of GFT is built on state of the art Privacy by Design strategies which are detailed in the GFT Group Data Protection Privacy by Design Guideline.

As a producer of the products, services and applications, GFT will take into account the relevance of Data Protection by Design and Default when developing and designing such products, services and applications with due regard to the state of the art. GFT will make sure that stakeholders of such products, services and applications have the possibility to express Data Protection by Design related expectations and that these expectations are fed into developing and designing process.

At GFT, software developers as well as management representatives who are responsible for software development activities are targeted by privacy engineering awareness measures. Specifically trained Privacy Engineers are implementing GFT's approach to Data Protection by Design and by Default by identifying Data Protection Risks and exploring corresponding mitigation measures in relevant projects to which they were assigned to. They might also be asked for an advice and/or opinion by Function/Local Privacy Officers in cases where their technical expertise would be required. Together they form the Privacy Engineer Community with a Leader directing its overall development on behalf of the Chief Privacy Officer.

1.8 Responsible AI

GFT considers Responsible AI as an integral part of its AI assisted business operations. Responsible AI in this context deals with legal and ethical aspects in the processing of personal data as well in the development and use of algorithms and application of relevant practices in the area of Artificial Intelligence.

For this purpose, GFT has issued the GFT Group Data Protection Guideline for Algorithmic Transparency and Accountability, the GFT Group Data Protection Guideline on Pseudonymization and GFT Group Data Protection Guidelines on Privacy by Design and relevant training measures.

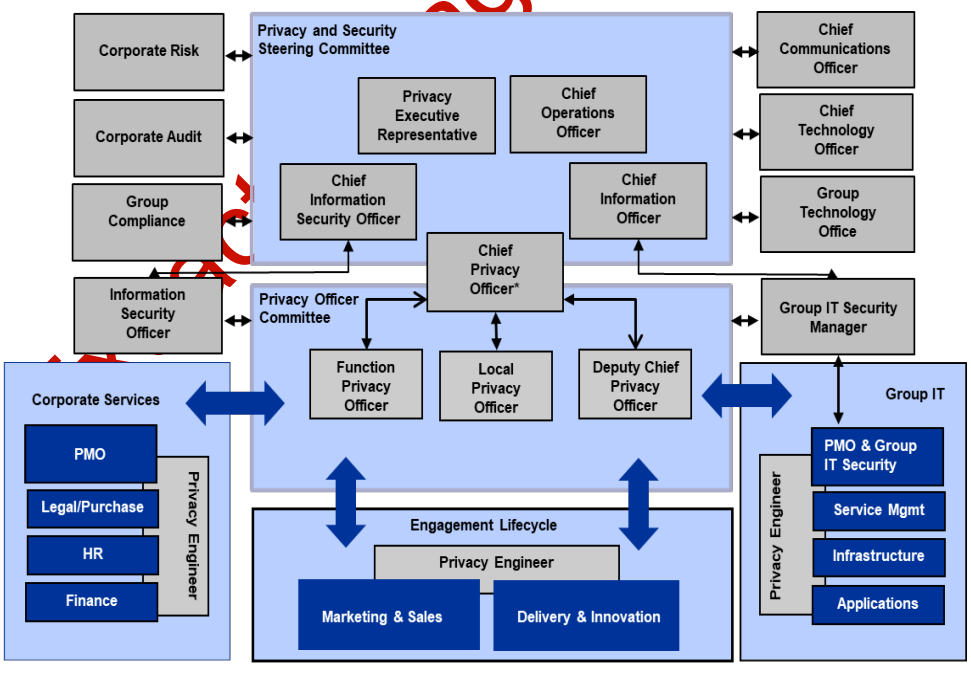
1.9 GFT Group Data Protection Network

The GFT Group Data Protection Networks consists of Data Protection Roles (direct elements of the Data Protection Network) and Data Protection Interfaces (indirect elements of the Data Protection Network).

The Data Protection Roles are representing the parts of the organization which are actively driving the GFT business to integrate Data Protection in every relevant business.

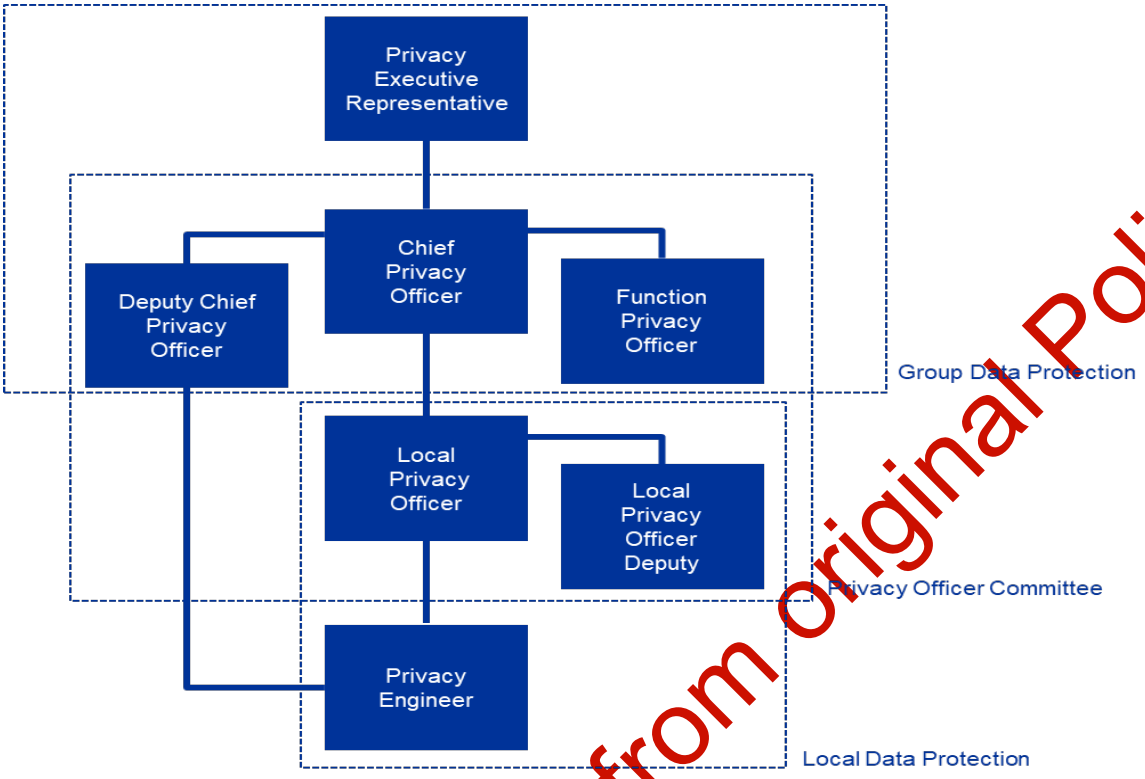
The Group CFO serves as the Privacy Executive Representative. The Chief Privacy Officer reports to the Privacy Executive Representative. The Privacy and Security Steering Committee (PriSecCo) provides executive level supervision, business alignment and sustained management commitment across all business functions and processes.

Function Privacy Officers and Deputy Chief Privacy Officers take care of data protection requirements of relevant functions on group level and/or on behalf of the Chief Privacy Officer. Local Privacy Officers take care of data protection requirements on Local level and/or on behalf of the Chief Privacy Officer acting as Single Data Protection Officer. Each Local Privacy Officer has a functional reporting line to the corresponding Local Management and CPO. Each Function Privacy Officer has a functional reporting line to the corresponding function management and CPO.



*) representing the „Single Data Protection Officer" for the GFT Group according to Art. 37 (2) GDPR

All Privacy Officers are assembled in the Privacy Officer Committee (POC) which represents the core element of the GFT Group Data Protection Network and serves as a bridge between Group Data Protection and Local Data Protection. Privacy Officers may invoke Data Protection Managers as supporting roles to ensure sufficient capacity for Data Protection required for full coverage of all areas in their area of responsibility.



*) representing the „Single Data Protection Officer" for the GFT Group according to Art. 37 (2) GDPR

Privacy Engineers are responsible for privacy related topics in engagements/proposals to which they were assigned to. They might also be asked for an opinion by Local Privacy Officers and Group Data Protection in cases where their technical expertise would be required. Together they form Privacy Engineer Community with a Leader directing its overall development.

Further details about Data Protection Roles and Interfaces are available in the GFT Group Data Protection Guideline for Data Protection Roles and Interfaces.

2 Data Protection Principles

Data Protection Principles provide generic guidance which are helpful in particular in cases where a new situation arises for which no processing pattern has been defined so far. However, there may be still cases where the application of these principles still is unclear or relevant exceptions may be applicable. In such cases, the Data Protection Officer as the subject matter expert in the application of Data Protection Principles provides the necessary guidance.

2.1 Lawfulness, Fairness and Transparency

Personal Data must be fairly handled, respecting the applicable legislation and in conformity with the GFT Group Data Protection Policy and other applicable data protection policies and guidelines. Handling of Personal Data must be adequate, relevant and proportionate to the purposes for which the information has originally been collected. In particular, any handling of Personal Data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair.

In particular, Processing shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for compliance with a legal obligation to which the organization is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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 organization;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

Every organization shall have transparent policies with regard to the processing of Personal Data. The responsible person shall provide information to the data subjects including but not limited to the organization's identity, the intended purpose of processing, the recipients to whom their Personal Data will be disclosed and how data subjects may exercise their rights, as well as any further information necessary to guarantee fair processing of such Personal Data.

2.2 Purpose Limitation and Accuracy

The processing of Personal Data should be limited to the fulfillment of the specific, explicit and legitimate purposes of the organization. The organization should not carry out any processing that is non-compatible with the purposes for which Personal Data were collected unless it has the unambiguous consent of the data subject. The organization should at all times ensure that Personal Data are accurate, as well as sufficient and kept up to date in such a way as to fulfill the purposes for which they are processed. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay.

The organization shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the organization.

2.3 Security of Processing of Personal Data

Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (TOM). These measures should be appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons including but not limited to the following:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Further guidance is provided in section 1.4 and section 4.6 of this document as well as in the GFT Group Data Protection Guideline for the TOM Standard.

2.4 Data Minimization

The principle of data minimization refers to legal requirements that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". That means that the collection of personal information should be limited to what is directly relevant and necessary to accomplish a specified purpose and to retain the data only for as long as is necessary to fulfil that purpose. In other words, organizations should collect only the personal data they really need, and should keep it only for as long as they need it.

The processing of Personal Data should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes set out in the previous section. In particular, the responsible person should make reasonable efforts to limit the processed Personal Data to the minimum necessary. The responsible person shall limit the period of retention of the processed Personal Data to the minimum necessary. Thus, when Personal Data are no longer necessary to fulfill the purposes which legitimized their processing they must be erased or rendered anonymous.

2.5 Storage Limitation and Data Retention

On one hand, Personal data processed for any purpose shall not be kept in a form which permits identification of data subjects for longer than is necessary for the primary purpose for which it was initially collected or for other compatible purposes. Keeping personal data for too long may expose the GFT Group to legal liabilities and cause a bunch of other problems (e.g. increasing consumption of valuable resources, increasing efforts to keep information accurate and secure, increasing scale of effects in the event of a data breach). On the other hand, discarding relevant personal data too soon would be likely to disadvantage of business and of the data subjects. There are various legal requirements and professional guidelines about keeping certain kinds of records for picking the right period of time for erasing various categories of data – such as data needed for income tax and audit purposes, or information on aspects of health and safety. If an

organization keeps personal data to comply with legal requirements like this, it will not be considered to have kept the information for longer than necessary. The following points provide some initial guidance for balancing the storage limitation and data retention principle:

- consider the purpose you hold the information for and with whom you shared it
- review the length of time you keep relevant categories of personal data (also taking into account legal retention periods)
- archive relevant data and restrict the access from everyday processing and use (if feasible, plan for different archive and backup periods)
- securely erase information that is no longer needed for the relevant purposes

Further guidance is provided by the GFT Group Data Protection Guideline for Retention and Erasure of Personal Data.

3 Data Protection Practices

Data Protection Practices represent essential elements of a Data Protection Framework. Special circumstances, types of processing and categories of data require special attention for which specific guidance is given below. However, there may be still be cases where the application of these practices still is unclear or relevant exceptions may be applicable. In such cases, the Local, Function and Chief Privacy Officer (and Deputies) as the subject matter experts in the application of Data Protection Practices represent the primary point of contacts for business who provide the necessary guidance.

3.1 Special and Sensitive Categories of Personal Data

Sometimes the notions of special and sensitive categories of personal data are used synonymously. At GFT however, sensitive categories of personal data will be understood as an umbrella term and special categories of personal data as a subsumable term.

Financial data like Bank Account or Credit Card details, National Identity or Driver's License or Social Security Numbers, Professional Secrets , personal data referring to criminal or administrative offences or to suspected criminal or administrative offences as well as Salary and compensation related information (not including daily rate) and private information relating to an individual's most intimate sphere (without being special) will be considered as sensitive categories of personal data..

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (within the context of a processing of the purpose of uniquely identifying a natural person), data concerning health or data concerning a natural person's sex life or sexual orientation will be considered as sensitive categories of personal data but also as special categories of personal data.

The processing of sensitive categories of personal data requires an increased level of due care. Handling of special categories of personal data is subjected to even stricter constraints by Article 9 of the General Data Protection Regulation. For this reason, any handling of sensitive and/or special categories of personal data has to be reported to the responsible Privacy Officer who will give advice to the proper handling of these categories of personal data within the given regulations.

3.2 Special Types of Processing of Personal Data

Initiatives which intend to create or modify new business processes, applications and/or databases involving special types of processing of personal data should be submitted by the business representative for review and approval by the Local Data Protection for local initiatives and by Group Data Protection for global initiatives before implementation. A similar initiative on local level in several but not all countries does not necessarily establish a global initiative. In case of doubts, the Chief Privacy Officer decides whether an initiative has to be considered as a local or global one.

In cases of special types of processing, the Business Representative has to submit a Data Protection Impact Assessment (DPIA) in addition the description of the initiative in the Data Protection Addendum for Data Protection review and approval.

A special type of processing is assumed when some processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons including but not limited to the following cases:

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
- a systematic monitoring of a publicly accessible area on a large scale
- any further type of processing as defined by Data Protection Authorities of requiring a DPIA
- any further type of processing as defined by Group Data Protection of being special

In case of doubts, the Chief Privacy Officer decides whether an initiative has to be considered as special type of processing and whether and in which form a Data Protection Impact Assessment has to be carried out.

3.3 Rights of the Data Subject

The rights of the data subject detailed below may be exercised:

a) directly by the data subject, who shall satisfactorily establish his/her identity to GFT
b) through a authorized representative, who shall satisfactorily establish his/her status to GFT

The responsible business functions in GFT must implement and maintain procedures to enable data subjects if and to the extent applicable to exercise the rights given below in a simple, fast and efficient way, which do not entail undue delay or cost :

- The right of access: the right to obtain access to the personal data of the subject (e.g by getting a copy of the relevant data) and further information about the processing (including rights of the subject)
- The right to be informed: the right to be provided with clear, transparent and easily understandable information about how rights of the data subjects and how GFT uses personal data of the data subject
- The right to erasure or right to be forgotten: the right to request personal data to be erased where it is no longer necessary for the organization to retain such data
- The right to data portability: the right to obtain and reuse personal data for the data subject's own purposes across different services
- The right to restrict processing: the right to suppress further processing of relevant information (information may still be stored, but access is very limited)
- The right to object to processing: the right to object to certain types of processing (e.g. in cases of legitimate interest which are not strictly necessary)
- The right to lodge a complaint: the right to submit a complaint about the way the organization processes personal data with the responsible data protection officer or data protection regulator
- The right to withdraw consent: the right to withdraw consent at any time and being as easy to withdraw as it has been when the consent has been given at some earlier point of time
- The right to rectification: the right to have information corrected if it is inaccurate or incomplete.
- The rights related to automated processing: the right not to be subject to a decision based solely on automated processing may include the right to explainability of a decision, the right to obtain human intervention in the decision-making process, the right of the data subject to express his or her point of view and to contest the decision

When GFT concludes that, pursuant to the applicable legislation, the exercise of relevant rights under this part is not justified, the data subject should be informed of the reasons that led to this conclusion.

3.4 Disclosure of Personal Data to Third Parties

GFT Group units shall only disclose Personal Data to approved third parties and between GFT Group legal entities in compliance with country specific legal requirements. Cross border data transfers of Personal Data

will only be performed in compliance with country specific requirements of the participating countries, as well as the GFT Group Data Protection Policy. All third parties with whom GFT Group shares Personal Data have to be contractually bound to adhere to the legal Data Protection requirements, relevant GFT policies and standards as well as additional client regulations applicable in the specific case at hand.

In principle, commissioned data processing shall be assumed in cases where a GFT group unit discloses personal data to a third party and treated accordingly. Exemptions from this principle may be granted by the Privacy Officer who is responsible of the GFT Group unit which discloses the personal data.

3.5 Commissioned Data Processing

GFT Group units may use commissioned processing of Personal Data by a third party ensuring that:

a) the processor guarantees, at least, the level of protection defined in this document and in the applicable data protection legislation
b) the controller defines technical and organizational measures in the way required from Data Protection point of view and processor guarantees to implement those measures
c) the legal relationship is established through a contract or legal instrument that allows proving its existence, scope and content, and that sets out the processing service provider's obligation to comply with these guarantees and to ensure the Personal Data are processed in compliance with the instructions of the controlling GFT Group unit

All contracts for commissioned processing of Personal Data must be approved by the responsible Local Privacy Officer. If the project includes personal data of GFT Group units which reside in different countries (multinational projects) or involves cross border transfers, approval of GDP is required additionally. In principle, the templates for commissioned data processing provided by GDP shall be used for that purpose. Exemptions from this principle may be granted on request from the responsible Local Privacy Officer (for local projects) and by GDP (for global projects). In cases of transfers of personal data to third countries, GDP may evaluate the adequate level of protection of personal data by requesting from the relevant Local Privacy Officer all the circumstances surrounding the data transfer, in particular taking into account the nature of the data, the purpose and duration of the proposed processing operation, the country of origin and country of final destination of the data, the laws applicable in the third country, safety measures used in this country and business conduct before approval. Approval of GDP is required as well for any externally facing Data Protection Notice (in co-operation with Legal and Compliance).

With regard to commissioned processing of personal data within the GFT Group, further guidance is given in the GFT Group Data Protection Guideline for Intra Group Data Sharing.

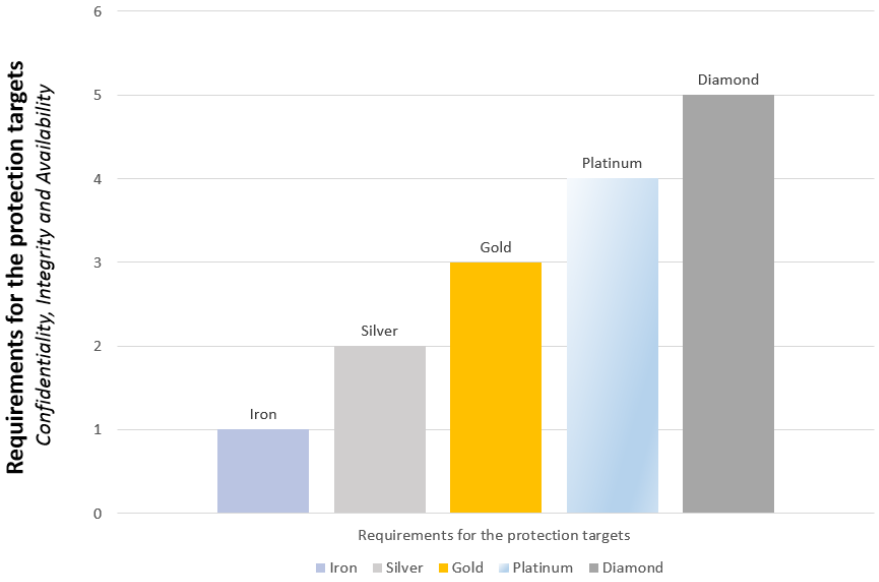
3.6 Technical and Organisational Measures

Personal Data – as a part of GFT Group's critical information assets - will be protected in accordance with legal requirements, as well as applicable security policies and standards. Appropriate technical and organization measures must be taken to ensure confidentiality, integrity and availability of Personal Data.

The technical and organizational measures (TOM) of the GFT Group are based on requirements as stated in Art. 25 and Art. 32 GDPR as well as on the guidelines of the international Information Security Standard ISO/IEC 27001 and are described in detail in the GFT Group Data Protection Guideline for the TOM Standard which serves to protect personal data on from the perspective of the data subject (i.e. the privacy perspective) and complements the perspective on security measures taken to minimize organizational risks (i.e. security perspective).

These technical and organizational measures contribute to achieving the control objectives for resources and processing activities used for the processing of personal data. The control objectives describe the security

level to be implemented according to the protection target and TOM level from the perspective of the data subject (i.e. the privacy perspective).



Data Protection is responsible for suggesting a TOM level which is considered appropriate for the specific processing activity or resource. The Processing Activity or Resource Owner is accountable for taking the decision which TOM Level has to be implemented actually.

3.7 Non-Compliance Handling

Since Data Protection requirements are regulatory in nature, any non-compliance may expose GFT Group to serious risks, including the possibility of fines, regulatory sanctions, enforcement actions, lawsuits, negative publicity, disruptions in operations, loss of revenue, and loss of market share. Thus, all Local Privacy Officers must establish and adopt a program to be in compliance with the GFT Group Data Protection Policy and applicable guidelines as well as local data protection provisions and operational requirements.

Each business function or process must ensure full compliance with the requirements of the applicable Data Protection program. All deviations from the GFT Group Data Protection Policy and local policies must be approved by the responsible Local Privacy Officer and be reported to the Chief Privacy Officer. Deviations are only accepted as a temporary solution, and an action plan must be in place to resume compliance with this policy in a reasonable period of time. A violation of this policy can result in disciplinary action, including dismissal, subject always to applicable employment laws.

3.8 Duty to Inform

Business Representatives in general and Processing Activity Owners in particular on Group, Function, Process, Country or Region level must inform their respective Privacy Officer at the beginning of all processing activities which will involve the handling of Personal Data, including but not limited to development of business concepts for new technology applications, introduction or major changes of business processes and outsourcing including but not limited to the following points:

1. the name of the processing activity owner / steward and the identification of the affected functions, processes and countries

2. the purposes of the processing
3. a description of the categories of data subjects and of the categories of personal data
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations
5. transfers of personal data to a third country or an international organization, including the identification of that third country or international organization (where applicable)
6. the envisaged time limits for erasure of the different categories of data;
7. a general description of the technical and organizational security measures based on a specification of the desired TOM Level as described in the GFT Group Data Protection Guideline for the TOM Standard

In addition, all Data Protection related complaints received from customers, employees, governments or regulatory bodies and any exercising of rights by a data subject must be communicated immediately to responsible Privacy Officer. The responsible Privacy Officer must escalate all material issues to the responsible Local or Function Management and Chief Privacy Officer.

3.9 Training & Awareness

In order to foster the understanding of Data Protection requirements and their implementation as integral part of relevant business operations, GFT considers regular participation of every GFT professional (employees and contractors) in Data Protection Training and execution of supporting Data Protection Awareness campaigns as foundational elements of GFT Group Data Protection Framework.

Exemptions from the GFT Mandatory Data Protection training requirements are only acceptable in extraordinary circumstances and have to be requested formally on basis of a detailed justification and granted by the GFT Mandatory Training Committee and the Chief Privacy Officer

Group Data Protection is responsible to provide the trainers and up-to-date training material for conducting the GFT Group Data Protection Training supporting self-instructed Online Training or instructor-led web-based or classroom training as training types. The GFT Mandatory Data Protection training package called “Foundation” consists of eLearning courses covering at least the following points:

- Why does Data Protection matter?
- What is Personal Data?
- Which types of processing of Personal Data exist?
- Which GDPR specific Data Protection rules have to be known?
- Which GFT specific Data Protection rules have to be known?

The abovementioned “Foundation” Data Protection Training is mandatory for any GFT professional and has to be completed at least once during the period working for GFT and/or its clients (unless there is a different contractual obligation for clients).

Further Data Protection Trainings are available but are not mandatory for all GFT professionals. These optional Data Protection Trainings may target GFT professionals in specific roles, in specific regions or with regard to specific topics or client needs and may involve in relevant cases different training levels with increasing scope of covered material.

The “Foundation” Data Protection Training may be combined with role, topic, region or client specific Data Protection Training requirements in a multiple year spanning incremental training plan tailored to the needs of the individual GFT professional. Both mandatory and optional Data Protection Training measures will contain a quiz of which a specified percentage of the questions have to be answered correctly to pass successfully. The successful completion of a Data Protection Training package will result in a certificate which enables the GFT professional to provide evidence for the successful acquisition of the corresponding knowledge (for compliance needs or career planning purposes).

Local HR is responsible for setting up the incremental data protection training plan (including the specification of each training module and the target date until which the training requirement has to be satisfied), for monitoring the proper execution of the training plan and maintaining the training records as evidence for the fulfillment of the training requirement.

Global HR is responsible for promoting a consistent set of principles and procedures for planning and executing the Data Protection Training, for monitoring the execution of the training plan on global level and for reporting the planned and actual progress on a quarterly basis to the GFT Mandatory Training Committee and to the Chief Privacy Officer.

The standard awareness campaign is based on articles in a global communication channel highlighting specific aspects in Data Protection and/or Information Security. Other training programs and awareness campaigns are considered as a non-standard elements and are added as appropriate either on a global or local level. Such non-standard training and awareness measures may be triggered by client needs, regulatory developments, organizational changes or need to tailor some topic to a specific audience or to complement the standard elements provided by Group Data Protection by a representation of some local aspect. Any non-standard Data Protection training program or awareness campaign in the GFT Group has to be reviewed and approved by the Chief Privacy Officer.

3.10 Data Breach Handling

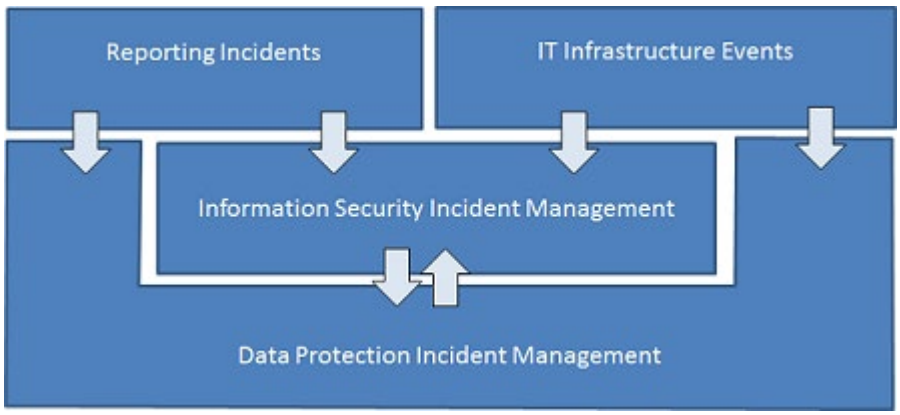
A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Therefore, as soon as GFT becomes aware that a personal data breach has occurred, GFT should notify the personal data breach to the supervisory authority and/or data subjects without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the GFT is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Even shorter periods of time e.g. 24 hours may be applicable in contractually defined notification obligations to clients.

Every GFT employee and partner is expected to report any event which may lead to a data breach without hesitation. Reporting a potential Data Breach is similar to calling the ambulance in case of an accident: A qualified team will respond quickly to the incident reporter and check the site of the accident, provides first care and set up an action plan to prevent or limit further damage. Data Breach Handling at GFT includes a global intake address databreach@gft.com for reporting incidents which should include but not necessarily be limited to the following information:

1. What has happened (malware infection or device loss or policy violation)?
2. Which data has been affected (personal data and/or business information) ?
3. Whose data has been affected (employees and/or clients)?
4. When did it happen (or when did it became known)?
5. Where did it happen (which country, location e.g. airport)?
6. Who is reporting (preferably the person who caused or recognized the incident)?

Reporting of a potential Data Breach is only the first step in a sequence of phases which gears towards effective mitigation of risks to the incident by qualifying the incoming incidents, determining the cause and extent of the incident, describing its harmful effects and separating the concerns of information security and data protection and to take the appropriate measures to avoid future incidents.



Data Protection is responsible for analyzing Data Protection Incidents and a) to owns the privilege to declare a “Personal Data Breach” and b) to determine whether the Personal Data Breach is actually likely to result in a high risks to the rights and freedoms of the data subjects. In case conditions a) + b) are both met. In co-operation with communication function, Data Protection will submit a proposal to notify the data subjects and/or the responsible Data Protection Authority to the responsible business representatives. The decision of the business representatives will be documented.

3.11 Proactive Practices

Group Data Protection encourages the implementation of proactive practices by those involved in any stage of the processing of measures to promote better compliance with applicable laws on Data Protection. Such practices include, among others:

1. the periodic conduct of transparent audits by qualified and preferably independent parties (e.g Corporate Audit) to verify compliance with the applicable laws on the protection of privacy with regard to the processing of Personal Data, as well as with the procedures established by the organization for that purpose
2. the implementation of Privacy Impact Assessments or Data Protection Impact Assessments prior to implementing new information systems and/or technologies for the processing of Personal Data or any other processing which bear high risks for the rights of the data subjects, as well as prior to carrying out any new method of processing Personal Data or substantial modifications in existing processing
3. the promotion of good retention and disposal of personal data including an Annual Clear Out for each processing activity involving personal data

4 Management of Policy Changes

This policy will be reviewed and updated as necessary on an annual basis by the Chief Privacy Officer of the GFT Group.

This is a Group Policy and follows the Group Policy Management Process:

- If content-related changes are to be made to this policy, a draft of the proposed changes must be submitted to Group Policy Management. Group Policy Management will then review the draft and obtain the necessary approval from the Group Executive Board.
- Group Policy Management will communicate any approved content-related changes to this policy to and through Group Management (ExDirs, L7 and L6) and via a news entry on the Group Policies Intranet area.
- If changes are required that do not affect the content (e.g. format, structure, layout), only the date of the document (footer of each page) will be changed.
- Release Notes are maintained and retained by Group Policy Management.

The version number and the month of publication and last review of the policy are indicated on the first page.

Comments and suggestions for improving this policy are welcome. Therefore, any employee who feels that there is something missing from this policy or that it could be improved is encouraged to send their suggestions to (dataprotection.group@gft.com).

5 Annex

List of Documents of the GFT Group Data Protection Framework:

- GFT Group Data Protection Policy (this document)
- GFT Group Data Protection Guideline for Data Protection Framework
- GFT Group Data Protection Guideline for Data Protection Roles and Interfaces
- GFT Group Data Protection Guideline for Employee Data Handling
- GFT Group Data Protection Guideline for Handling of Prospect and Client Data Handling
- GFT Group Data Protection Guideline for Whistleblowing
- GFT Group Data Protection Guideline for Retention and Disposal of Personal Data
- GFT Group Data Protection Guideline on Algorithmic Transparency and Accountability
- GFT Group Data Protection Guideline for Handling Data in MDWH
- GFT Group Data Protection Guideline on Pseudonymization
- GFT Group Data Protection Guideline for the TOM Standard
- GFT Group Data Protection Glossary