GFT

Fostering trust in the digital transformation

GFT Group Data Protection Policy

Owner:
Group Data Protection

Version:
3.8

Date of Publication:
15 November 2024

Classification:
Internal

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.

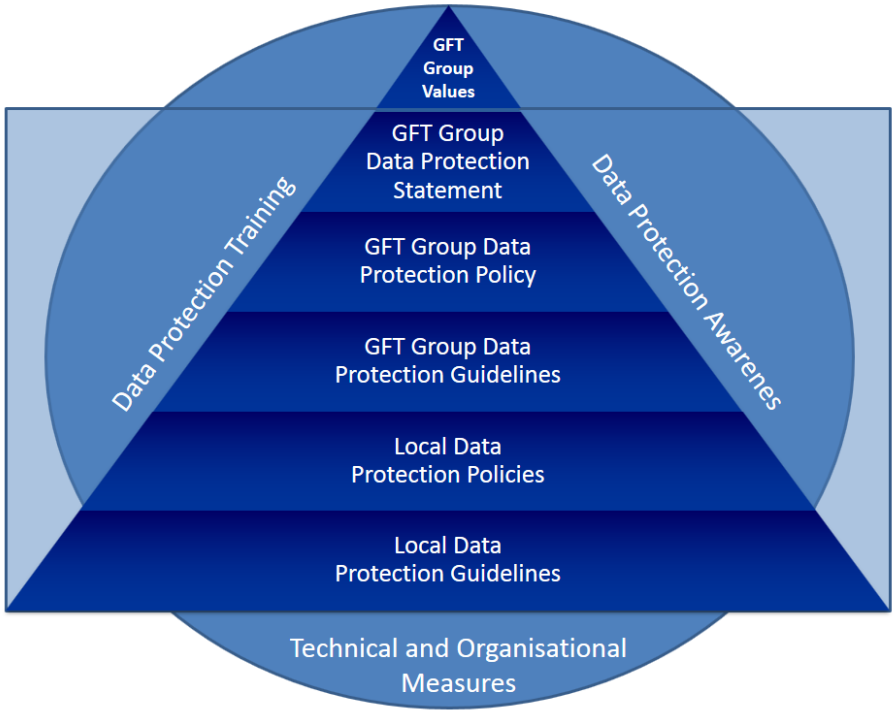
The notions of "Data Protection" and "Privacy" used throughout this document refer to the handling of legal requirements which regulate the processing of personal data. The term 'personal data' means any information relating to a 'data subject". A 'data subject' represents an identified or identifiable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

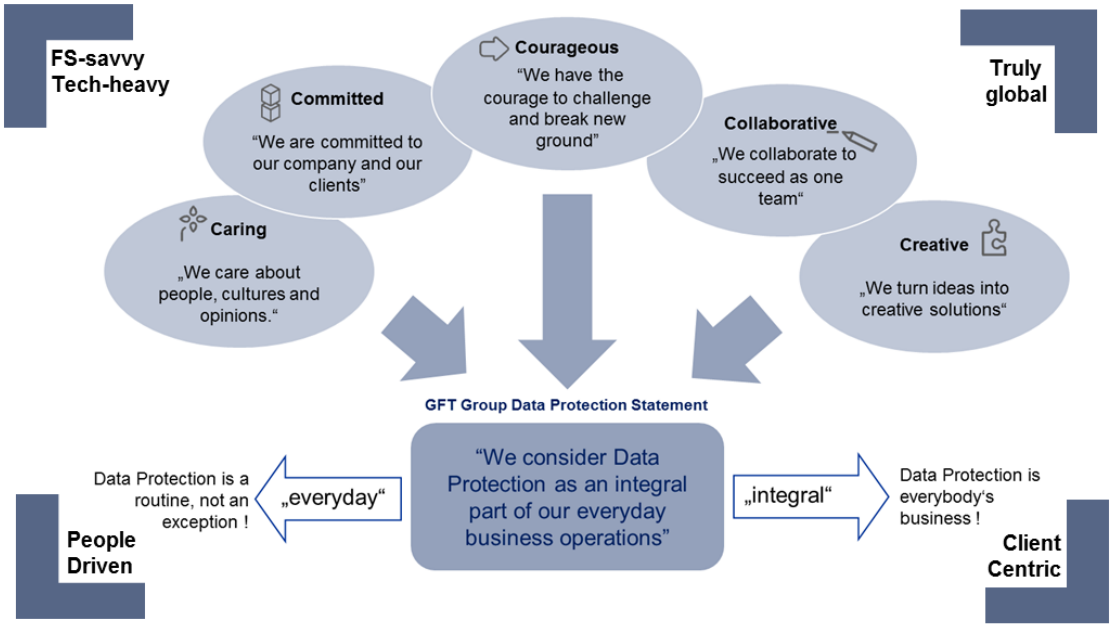


Revisions of the GFT Group Values have to be approved by the GFT Administration Board and the Group Executive Board. Revisions of the GFT Group Data Protection Statement and major versions of the GFT Group Data Protection Policy have to be approved by the Group Executive Board, Privacy and Security Steering 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.

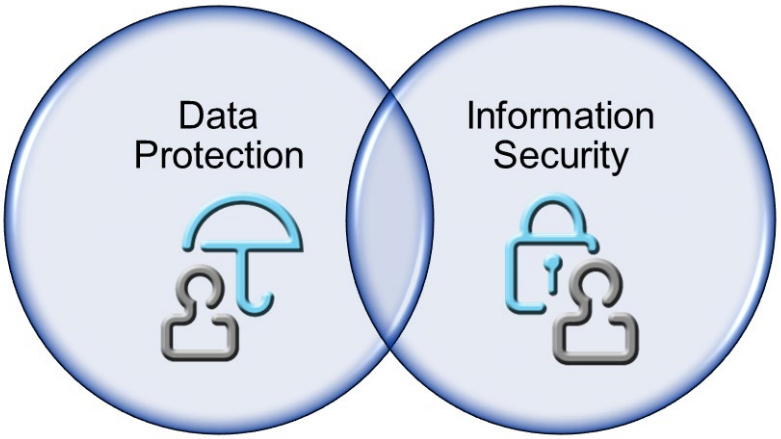
1.4 Global & Local Policies

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 Responsible AI which is based on relevant ethical and legal standards, such as the values and principles from UNESCO's Recommendation on the Ethics of Artificial Intelligence as well as indicators for AI related unacceptable or high risks from EU's AI Act.

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

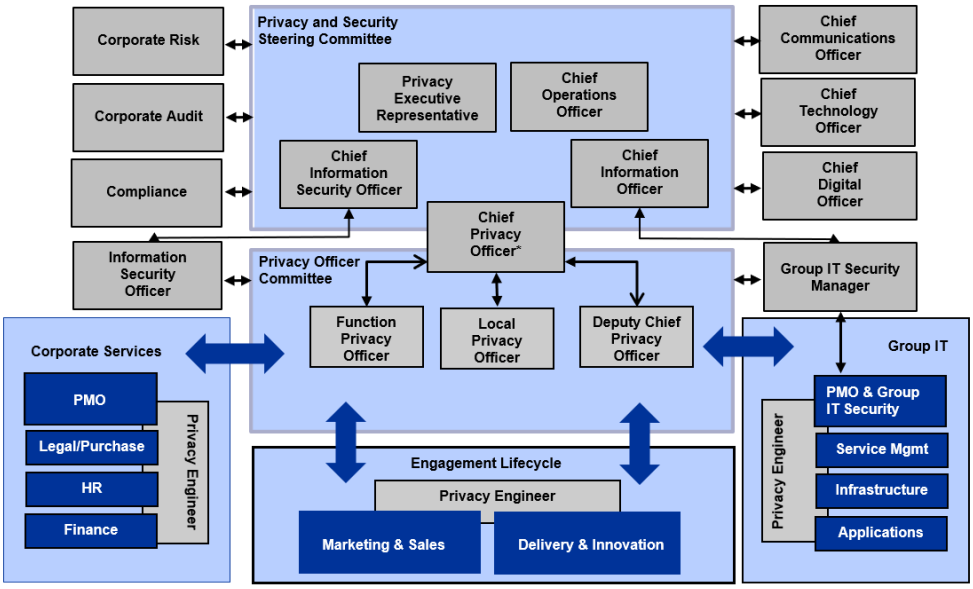
1.9 GFT Group Data Protection Network

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.

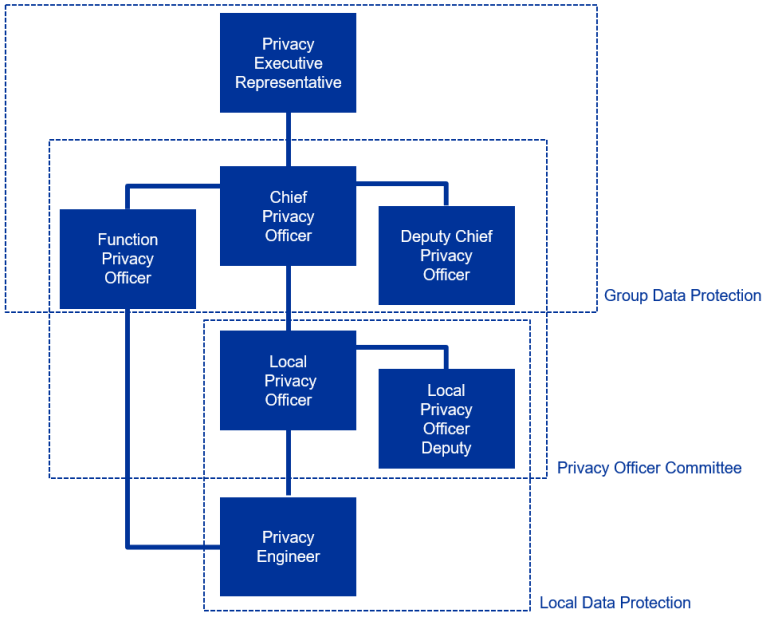
The Group CFO serves as the Privacy Executive Representative. The Chief Privacy Officer reports to the Privacy Executive Representative. The Privacy and Security Steering Committee (PriSecCo) provides executive level supervision, business alignment and sustained management commitment across all business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