DEUTSCHE BÖRSE GROUP

Deutsche Börse Group

Compliance Requirements for External Service Providers

November 2021

Public

Contents

1 Introduction

Compliance with applicable laws, rules, regulations and professional standards constitutes a fundamental principle of Deutsche Börse Group (DBG) corporate culture. We require our External Service Providers to know, understand and abide by the requirements set forth in this Compliance Policy. In addition, and were applicable, External Service Providers are responsible for implementing and maintaining systems and procedures to ensure compliance of their employees with the provisions of applicable laws, rules, regulations and professional standards as well as with the requirements and obligations laid down in this policy. They must also ensure that they adhere to local requirements in the various jurisdictions in which DBG operates and External Service Providers perform tasks for or on behalf of DBG.

The purpose of this policy is to inform External Service Providers which provisions and requirements we want them to be aware of and adhere to.

External Service Providers this policy applies to are described under section 1.2.

The respective chapters of this Compliance Requirements for External Service Providers summarize the applicable professional obligations in the following areas, which have general applicability across DBG entities and beyond either as a matter of law or of DBG policy. It is expected that all External Service Providers have awareness relevant to their duties.

- Prevention of Money Laundering and Terrorism Financing
- Prevention of Other Criminal Offences (Fraud)
- Financial Sanctions & Embargoes
- Prevention of Market Abuse (Insider Dealing and Market Manipulation)
- Management of Conflicts of Interest
- Prevention of Bribery and Corruption
- Data Protection
- Compliance & Regulatory Coordination (incl. MaRisk Compliance)

More detailed information on particular requirements is contained in corresponding chapters of the respective Compliance guidelines which, where necessary, will be attached to this document. References to certain laws in various jurisdictions can be included but these references are by no means exhaustive. (References to the important Compliance relevant laws with general applicability can be found in the DBG intranet page under Group Compliance.)

External Service Providers should be aware that regulatory requirements may flow not only from regulations that apply directly to the activity being undertaken but on occasion from third country regulations that apply extra-territorially or because DBG has entered into voluntary agreements with foreign supervisory or tax authorities.

1.1 Compliance Function and Whistleblowing System

The DBG Compliance Function refers to the Compliance Department of Deutsche Börse Group (“Group Compliance”) but also, as the case may be, to the compliance departments of the respective group entities. If in

this policy reference is made to Compliance or the Compliance Function this shall mean Group Compliance, which can be addressed under compliance@deutsche-boerse.com.

Within Compliance the Money Laundering Reporting Officer (MLRO) and its deputy are the designated contact for issues in connection with the Prevention of Money Laundering and Terrorism Financing and the Prevention of other Criminal Offences (Fraud). The MLRO can be addressed under MLRO_DBG@deutsche-boerse.com.

For issues in connection with the Prevention of Market Abuse, Conflicts of Interest and Bribery and Corruption Employees & Securities Compliance is the designated contact, which can be addressed under compliance-ecp@deutsche-boerse.com.

Financial Sanctions & Embargoes is the designated contact for sanctions-related issues and can be addressed under sanction_GC@deutsche-boerse.com.

In order to create an environment of trust and protections Group Compliance has also implemented a Whistleblowing System. The Whistleblower hotline can be addressed under

Direct Link: https://www.bkms-system.com/deutsche-boerse

Deutsche Boerse landing page: https://deutsche-boerse.com/whistleblower

Or by phone under

+49 30 99257146.

1.2 Applicability

This Policy applies to legal or natural persons who perform tasks for or act on behalf of DBG, including external service providers such as agents, consultants, or distributors (henceforth “External Service Providers”). However, it does not apply to temporary staff working for DBG for more than 30 calendar days. For those the internal DBG Policies, as laid down in the complete Compliance Handbook, apply.

1.3 Reporting obligations

External Service Providers have an obligation and are encouraged to report any alleged violation of the laws and regulations or stricter internal requirements, as listed below, or any compliance risks that they may become aware of regarding their business relation to Deutsche Börse Group to the Compliance Function of the Deutsche Börse Group directly.

Alternatively, External Service Providers of DBG are encouraged to confidentially report tips or leads about perpetrated or suspected cases of criminal conduct and related violations of the compliance provisions that might adversely affect DBG, particularly any financial injuries harming DBG to the Whistleblower hotline.

2 Prevention of Money Laundering and Terrorism Financing

2.1 Purpose

This chapter summarizes the legal and regulatory requirements that apply with respect to the prevention of money laundering and terrorism financing. A breach of these obligations could constitute a criminal offense.

2.2 Definitions

Money laundering is the process through which persons or entities attempt to use the financial system to conceal the true origin and/or the true ownership of the monetary proceeds of activities considered by law to be criminal (or predicate) offenses. Money laundering usually includes three distinct processes placement, layering and integration, although not always in this order and not always all together.

Terrorism financing constitutes the gathering or supply of funds or proceeds intended for use in the commission of terrorist acts or the activities of terrorist groups.

2.3 Obligations

Specific procedures of control and communication must be put in place to mitigate the risk of and attempt to operations related to money laundering and terrorism financing. The main legal requirements are contained in:

- The German Money Laundering Act (GwG/Geldwäschegesetz), the German Criminal Code (StGB/Strafgesetzbuch), the German Banking Act (KWG/Kreditwesengesetz) Interpretation- and Application Guidance in relation to the German Money Laundering Act (Auslegungs- und Anwendungshinweise der BaFin) and related BaFin circulars.
- The Luxembourg Criminal Code, the Luxembourg law on the financial sector and the Luxembourg law relating to the fight against money laundering and terrorism financing and CSSF circulars.
- The Swiss Criminal Code, the Act on the prevention of money laundering and terrorism financing, Ordinance of FINMA on the prevention of money laundering and terrorism financing, the Swiss Federal Act on Stock Exchanges and Securities Trading, and the Swiss Federal Law on Banks and Savings Banks.
- The Singaporean Penal Code as well as AML-related Acts, Subsidiary Legislation Notices and Directions on AML/CTF as well as further guidance issued by the Monetary Authority of Singapore.
- Other relevant national regulations, e.g., UK, US, consistent with global regulatory- or industry standards, e.g., defined by FATF.

The regulators have outlined main categories of professional obligations to which DBG in turn requests their business partners to adhere to:

- To establish an effective risk management system that is appropriate for the nature and size of their business
- To determine and evaluate the risks of money laundering and terrorist financing associated with the business activities they engage in
- To establish and document an annual Risk Analysis appropriate to the specific risk that they are exposed to

- To implement internal safeguards, including internal principles, procedures and controls to mitigate the inherent risks
- To establish a comprehensive and appropriate due diligence procedure for customers and for related parties

Where applicable,

- to furnish employees with initial and ongoing AML- / CTF-Trainings to foster understanding and raise awareness
- to establish measures to prevent the abuse of new products and technologies for committing money laundering and terrorism financing
- to appoint a money laundering reporting officer and a deputy
- to cooperate with and in certain circumstances to report suspicious activity to the competent authorities

As a matter of policy, DBG applies comprehensive diligence measures not only with respect to its own customers in the traditional sense of an account relationship, but more generally follows a risk-based approach with respect to broader parties, such as External Service Providers with which business is conducted.

The above listed obligations might impact the relationship with External Service Providers, in a way that Deutsche Börse Group applies risk mitigating measures within its business conduct with the Service Provider to prevent being misused for money laundering, the financing of terrorism or other criminal offence.

The External Service Provider likewise should notify DBG about any suspicion or concern that they become aware of in connection with criminal offences connected to the contractual relationship that they have established with Deutsche Börse. In such case, the External Service Provider must report suspicion to the Deutsche Börse Group Money Laundering Reporting Officer (MLRO) or it's deputy or to the MLROs of the local legal DBG entities.

2.4 Responsibilities

The External Service Provider must ensure that all employees directly or indirectly entrusted with the business relationship with the Deutsche Börse Group understand and apply the anti-money laundering and counter-terrorism financing requirements. They must furthermore ensure that adequate procedures of internal control and communication are established within their unit(s) to notify Deutsche Börse Group about potential risks that have been detected with regards to money laundering or terrorism financing.

Employees of the External Service Provider who suspect money laundering or terrorism financing shall contact the Money Laundering Reporting Office within Group Compliance.

3 Prevention of Other Criminal Offences (Fraud)

3.1 Purpose

This chapter sets out the professional obligations in relation to the prevention of fraud. A breach of these obligations could constitute a criminal offense.

3.2 Definitions

"Fraud" encompasses any intentional deceptive act/legal offense which could directly or indirectly result in a threat to the assets or a substantial damage to the reputation of DBG.

This includes, in particular, any deceptive act or omission

• by a third party (business partner, customer, non-customer)

• by at least one internal party (employees or members of institutional organizations)

This comprises falsifying or concealing any books, records or accounts that relate to the business of DBG, its customers, suppliers or other business partners and thus is prohibited and fall under the definition of "Fraud" within the meaning of this policy.

In case of doubt whether certain conduct or an event may involve fraud, the Money Laundering Reporting Office within Compliance must be contacted for further coordination.

3.3 Obligations

The obligation to implement effective fraud prevention within the group is mainly based on:

- The German Stock Company Act in conjunction with the German, Luxembourg, Singaporean Penal Code and the Swiss Criminal Code.
- The German Commercial Code.

Regarding DBG companies operating in other countries, the respective jurisdictions effectively require similar fraud prevention measures. Where applicable, local legal requirements and regulations should always be considered.

DBG is committed to creating an environment which inhibits fraud. DBG is responsible for securing its own interests as well as those of its customers. It must, therefore, provide for proper internal control systems and effective mechanisms for reporting and acting on reports of misconduct.

3.4 Responsibilities

External Service Providers who suspect that an irregularity has occurred should report this to their respective GDB contact, who will in turn notify the MLRO if the concerns are justified. At each time the irregularity can also be directly reported to the Money Laundering Reporting Function within Compliance or by using the Whistleblower System of DBG, especially in case where the alleged suspicion might affect / involve the above-mentioned contacts. Any concern raised is to be treated with utmost confidentially and fall under the protective rules of the Whistleblower Policy.

4 Financial Sanctions & Embargoes

4.1 Purpose

This chapter summarizes the legal and regulatory requirements that apply with respect to the prevention of the violation of Financial Sanctions & Embargoes. Any breach of these obligations could trigger substantial penalties or constitute a criminal offense.

4.2 Definitions

Financial Sanctions & Embargoes are restrictions on activity with targeted countries, governments, entities, individuals, or industries. Sanctions are in place to make sure that economic support is not provided to targeted regimes (or countries), people or organizations known to be involved in activities which threaten global security or otherwise serious organized illegal activities including terrorism.

4.3 Obligations

Specific procedures, internal controls and means of communication must be put in place to forestall and prevent operations related to sanctioned countries and sanctioned entities / individuals. The main legal requirements are contained in:

- The Sanctions-related resolutions of the United Nations Security Council
- The Sanctions-related regulations or decisions of the European Union.
- The requirements of the US Department of Treasury's Office of Foreign Assets Control.
- National and regional sanctions lists and authorities (including Deutsche Bundesbank, HM Treasury, MAS, CSSF, SECO)
- National Sanctions regulation which will apply to a DBG entity or its relevant agent or correspondent located in that particular country.

No business activity of DBG & External Service Providers shall relate to a sanctioned country or a sanctioned entity, unless it is permissible pursuant to the applicable Sanctions laws. No external service provider who has been sanctioned or which is currently sanctioned shall provide a service to DBG and its entities.

In evaluating sanctions-related risks, the Compliance Function shall consider additionally risks of secondary exposure or reputational and risk considerations for DBG entities and business counterparties.

4.4 Responsibilities

All External Service Providers (including its employees) are prohibited from engaging in any business activity related to sanctioned countries or sanctioned individuals. The External Service Provider must ensure that no sanctioned individuals may be assigned to tasks related to DBG contracts. The Compliance Function is solely authorized to grant exceptions, in cases where the exception is permissible pursuant to the applicable Sanctions laws. Employees of External Service Providers must report every Sanctions-related matter to the Compliance Function including suspicions on violation of sanctions laws and regulations.

5 Prevention of Market Abuse

5.1 Purpose

The purpose of this chapter is to inform all External Service Providers of relevant laws and regulations related to the prevention of Market Abuse, including Insider Dealing, Unlawful Disclosure of Inside Information or Market Manipulation, and to ensure compliance with this legislation.

Insider Dealing, Unlawful Disclosure of Inside Information and Market Manipulation are criminal offences, and so is the Inciting, Aiding and Abetting and the attempt of any of these offences.

5.2 Definitions

Inside Information means any information of a precise nature which has not been made public, relating, directly or indirectly, to one or more issuers / financial instruments / commodity derivatives / emission allowances or auctioned products based thereon / wholesale energy products, and which, if it were made public, would be likely to have a significant effect on the price of those financial instruments or on the price of related derivative financial instruments or on the price of those wholesale energy products. It would be likely to have a significant effect on the prices of financial instruments or on the prices of the wholesale energy products if a reasonable investor would be likely to use it as part of the basis of his or her investment decisions.

Insider Dealing arises where a person:

- Has access to Inside Information and uses that information by acquiring or disposing of, for his or her own account or for the account of a third party, directly or indirectly, financial instruments or wholesale energy products to which that information relates; or
- Uses Inside Information by cancelling or amending an order concerning a financial instrument or wholesale energy products to which the information relates where the order was placed before the person concerned possessed the Inside Information. In relation to auctions of emission allowances or other auctioned products based thereon that are held pursuant to Regulation (EU) No. 1031/2010, the use of Inside Information shall also comprise submitting, modifying, or withdrawing a bid by a person for its own account or for the account of a third party.

Recommending that another person engages in insider dealing, or inducing another person to engage in insider dealing arises where the person possesses Inside Information and recommends, based on that information, that another person

- Acquire or dispose of financial instruments or wholesale energy products to which that information relates, or induces that person to make such an acquisition or disposal; or
- Cancel or amend an order concerning a financial instrument or a wholesale energy product to which that information relates or induces that person to make such a cancellation or amendment.

Unlawful disclosure of Inside Information arises where a person possesses inside information and discloses that information to any other person, except where the disclosure is made in the normal exercise of an employment, a profession, or duties, including where the disclosure qualifies as a market sounding made in compliance with the legal and regulatory requirements.

The onward disclosure of recommendations or inducement to engage in insider dealing amount to U**nlawful Disclosure of Inside Information**, where the person disclosing the recommendation or inducement knows or ought to know that it was based on Inside Information.

Market Manipulation can be defined as any and all actions which could influence unjustifiably the stock exchange or market price of financial instruments or wholesale energy products, or to give false signals regarding the supply of or demand for financial instruments or wholesale energy products. Irrespective of whether or not the action actually affects the demand for, supply of or market price of financial instruments or wholesale energy products, the intention or suitability for manipulation will be the dispositive issue for purposes of determining the existence of manipulation.

5.3 Obligations

The main legal requirements derive from:

- The European Directives and Regulations on Market Abuse
- The German Securities Trading Act and BaFin circulars.
- The Luxembourg law on Insider Dealing.
- The UK Financial Services and Markets Act 2000, Proceeds of Crime Act 2002, Criminal Justice Act 1993 and Financial Services Act 2012
- Singaporean Securities and Futures Act.
- The Swiss Criminal Code, the Swiss Federal Act on Stock Exchanges and Securities Trading.

Further local regulations and requirements may also need to be considered, where applicable.

DBG is committed to creating an environment which promotes transparency and inhibits Market Abuse. DBG is responsible for securing its own interests as well as providing a fair playing field for market participants. It must therefore provide for proper internal control systems and effective mechanisms for reporting and acting on reports of attempted or actual Insider Dealing or Market Manipulation.

While working for DBG, compliance-relevant information – meaning sensitive or inside information - may become known to External Service Providers. The misuse of such information is strictly prohibited. It can damage the trusting relationship which DBG has with its market participants, issuers, investors, the financial sector, and the general public.

Thus, care should be taken, and appropriate measures be implemented, such as through Zones of Confidentiality, information barriers and other practices with respect to sharing Compliance-Relevant Information on an authorized and need-to-know basis within and across DBG entities, between DBG and External Service Providers or among the employees of External Service Providers to avoid even the appearance of unauthorized use of information.

No External Service Provider shall acquire or dispose of or try to acquire or dispose of financial instruments on the basis of Inside Information in relation to these instruments.

5.4 Responsibilities

It is strictly forbidden for any External Service Provider or employee of an External Service Provider to attempt or engage in Insider Dealing, Recommending, or Inducing to Engage in Insider Dealing, Unlawful Disclosure of Inside Information and Market Manipulation. External Service Providers must furthermore adhere to local rules on the prevention of Market Abuse, where provided. External Service Providers or employees of External Service Providers who are not sure about legal circumstances shall consult the Compliance Function at compliance-ecp@deutsche-boerse.com.

To prevent Market Abuse, all external persons who are responsible for or who handle the group's external communication, or assist in doing so, must ensure that no false or misleading information is published.

If an External Service Provider gains access to inside information regarding financial instruments issued by DBAG or any of its affiliates due to acting on behalf or on account of DBG they must establish and maintain an insider list in accordance with Art. 18 (1) of Regulation (EU) No 596/2014 (Market Abuse Regulation). A contact person of the External Service Provider responsible for the maintenance of the insider list must be notified to the Compliance Function at compliance-ecp@deutsche-boerse.com. Additionally, the personal information in accordance with Template 1 of Annex I of Commission Implementing Regulation (EU) 2016/347 must be provided to the Compliance Function using the same email address to be entered into DBG's insider list.

Furthermore, External Service Providers must take all reasonable steps to ensure that any person on the insider list acknowledges in writing the legal and regulatory duties entailed and is aware of the sanctions applicable to insider dealing and unlawful disclosure of inside information.

In addition, External Service Providers must establish and maintain appropriate and effective systems and procedures aimed at the prevention of (attempted) insider dealing and market manipulation.

Employees of External Service Providers who suspect that an irregularity has occurred should report this directly to the Compliance Function at compliance-ecp@deutsche-boerse.com. Notified concerns must be treated confidentially and must only be shared on an absolute need-to-know basis.

6 Conflicts of Interest

6.1 Purpose

This chapter summarizes the requirements in relation to the management of conflicts of interest.

6.2 Definitions

A conflict of interest is not, in itself, evidence of wrongdoing. However, a conflict of interest can become a serious legal, regulatory, or reputational issue, if not identified and managed effectively.

Conflicts of interest may arise in situations in which the interests of one party interfere with (or appear to interfere with) the interests of another party. This may impair the ability of one or both parties to act fairly and ethically, i.e., its objectivity to take a decision to be taken during its professional obligations.

6.3 Obligations

The main legal requirements in relation to conflicts of interest are contained in:

- Regulatory requirements on European level deriving e.g., from the directive on markets in financial instruments (MiFID), the regulation on OTC derivatives, central counterparties, and trade repositories (EMIR), the regulation on improving securities settlement in the European Union and on central securities depositories (CSDR), the benchmark regulation, and provisions related to these requirements,
- Local regulatory requirements deriving from e.g., the German Securities Trading Act, the Luxembourg law on the financial sector, the Swiss Federal Law on Unfair Competition

Where applicable, other local legal requirements and regulations might also be considered.

DBG makes necessary efforts to avoid and, where necessary, mitigate conflicts of interest which may arise among customers or providers, between customers or providers and DBG itself, between customers or providers and employees of DBG, and within DBG and its entities or divisions.

6.3.1 Potential Sources of Conflicts of Interest

Conflicts of interest may arise – on a personal or on a corporate level – between

on the one hand		on the other hand
DBG in its different roles, including through different affiliates with multiple responsibilities	**and**	one or more third parties (e.g., past, current or prospective) customers, service providers or competitors
members of management bodies or employees of DBG entities or persons closely associated (linked)with them	**and**	one or more third parties (e.g., past, current or prospective) customers, service providers or competitors
members of management bodies or employees of DBG entities or persons closely associated (linked) with them	**and**	DBG
a DBG entity	**and**	another DBG entity
a third party	**and**	another third party
in the context of services provided by DBG to them (conflict of interest between two DBG customers)		

Personal conflicts of interest may originate from personal, professional, or economic relationships with other persons such as:

- Secondary employment/external mandates (remunerated or not),
- Further internal mandates and role(s) within DBG,
- Financial interests (deriving from e.g., participation of at least 5% in a third party, for example a shareholder or competitor of DBG or a Group entity, from loans or investment club memberships),
- Interests of persons closely associated, e.g., family members.

Personal interests may also be the source of corporate conflicts of interest, e.g., by an individual holding several mandates in two different entities, thus creating conflict potential for this person, and also on a corporate level for one or even both of these entities, e.g., in the context of services provided by one entity to the other.

Furthermore, corporate conflicts of interest may arise e.g., in the context of fee arrangements, or of commissioning different (past or present) assignments to the same provider.

6.3.2 Management of Conflicts of Interest

When identifying a situation, where a (potential) conflict of interest cannot be avoided, appropriate actions to manage, document and, as applicable, report this situation shall be taken, such as

- Notification to the Compliance Function at compliance-ecp@deutsche-boerse.com, ensuring transparency
- Segregation of duties and business functions
- Recusal by or exclusion of the conflicted person or termination of the constellation, e.g., by terminating a contract
- Controls and monitoring
- As a measure of last resort, disclosure to customers

6.4 Responsibilities

External Service Providers shall contribute to identify, manage and document (potential) conflicts of interest.

Furthermore, they shall in particular abstain from activities that may be to the detriment of DBG, as well as from any kind of misuse of inside information or other sensitive, non-public information obtained in the course of their professional responsibilities, or of misuse of their professional position for personal gain.

7 Corruption

7.1 Purpose

This chapter summarizes the requirements in relation to the prevention of bribery, and corruption in general. Any breach of these obligations could constitute a criminal offense.

7.2 Definitions

Corruption means the abuse of entrusted power in business dealings for private gain for oneself or a third party, i.e., by offering, promising, or giving a benefit, or authorizing someone to do so (active corruption), or by accepting, soliciting a benefit, or allowing oneself to be promised a benefit (passive corruption).

This includes a benefit in return for an unfair preference in the purchase of goods or services in (domestic or foreign) competition, or (failing to) act without the consent of the company (of the donor or recipient) and thereby breaching obligations towards the company.

Bribery is a type of Corruption meaning offering, promising, giving, or authorizing someone to offer, promise, accept or solicit [active Bribery], or accepting, soliciting, or allowing oneself to be promised [passive Bribery] an improper benefit, directly or indirectly, to or from a third party with the intention of influencing or rewarding the behavior of this or another third party to obtain or retain a commercial advantage.

Benefit means gift, business entertainment or other benefits, i.e., any privileges, rights, assets, items, or activities / events of Value. It is something that comes at a cost or foregone revenue to the giving party and is expected to be valued by the recipient, beyond what is made available to the public generally. In addition to a tangible transfer of direct Benefits to the recipient, the granting of a Benefit might include the granting of Value or opportunities for others that do not stand on their own merits, but rather have a purpose of inappropriately influencing a recipient.

7.3 Obligations

The main legal requirements in relation to conflicts of interest are contained in:

- Regulatory requirements on international level, e.g., deriving from the Convention on Combating Bribery of Foreign Officials in International Business Transactions
- Regulatory requirements on European level deriving e.g., from the directive on markets in financial instruments (MiFID), and provisions related to these requirements
- Local regulatory requirements deriving from e.g., the UK Bribery Act, the US Foreign Corrupt Practices Act, the German Criminal Code and the German Securities Trading Act, the Luxembourg law on the financial sector, the Singaporean Penal Code, Prevention of Corruption Act and Corruption, Drug Trafficking, and other Serious Offenses (Confiscation of Benefits) Act, the Swiss Criminal Code and the Swiss Federal Law on Unfair Competition

Where applicable, other local legal requirements and regulations might also be considered.

Bribery, and corruption in general, active or passive, are prohibited by all means. If an action merely appears to or actually does result in corruption, they must refrain from proceeding in any way.

DBG has committed itself to the highest standards in preventing active and passive corruption and bribery. It follows a stringent zero tolerance policy in this regard.

7.3.1 Offering or receiving Benefits

No benefit should be offered or accepted, if it: (1) is inconsistent with customary business practice, (2) is excessive in value or frequency, (3) can be construed as an inducement, bribe or payoff, (4) may improperly influence an employee's judgement, or (5) violates any laws or regulations.

7.4 Responsibilities

External Service Providers must not offer, promise, give, or authorize someone to offer, promise, accept or solicit any gift, business entertainment or other benefit, if it appears excessive, frequent, non-customary, intended to improperly influence employee judgment, or is illegal. Granting or accepting benefits should be aimed at promoting, maintaining, and strengthening the overall business relationship. Such business purpose should clearly outweigh the personal aspects. Granting or acceptance of Benefits requires a responsible attitude of all involved persons.

The frequency, type and value of the benefit must be appropriate and must not risk reputational damages.

8 Data Protection

8.1 Purpose

The purpose of this chapter is to inform External Service Providers of the relevant legislation related to personal data protection for Deutsche Börse Group and the necessity to ensure compliance with this legislation.

8.2 Definitions

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Data 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

8.3 Obligations

The main legal requirements for Deutsche Börse Group entities may result from:

- The Regulation (EU) 2016/679 (General Data Protection Regulation).
- The German Data Protection Law.
- The Luxembourg law on the Protection of Persons regarding the Processing of Personal Data.
- The Singaporean Personal Data Protection Act.
- The Swiss Federal Act on Data Protection.

Due to the principle of territoriality for permanent establishments inside the European Union and European Economic Area (EEA), the applicable law besides the General Data Protection Regulation is in addition the law of the country where the personal data processing takes place.

Personal data must be kept confidential and only be transferred to third parties in accordance with the relevant laws and regulations. Data subjects must be informed (i) that their personal data is being collected and (ii) the reason why it is being collected and processed and (iii) if a transfer to a non-EU/EEA country is intended.

8.4 Responsibilities

External Service Providers must bind their employees to act in accordance with the data protection requirements.

Furthermore:

- EU External Service Providers potentially having access to personal data of employees, customers or third persons in responsibility of a DBG entity during the performance of its tasks must
  - engage into a data processing agreement and
  - provide transfer impact assessments in case of intended involvement of non-EU sub-processors.

- Non-EU External Service Provider having potentially access to personal data must
  - engage into a valid and effective transfer tool, e.g., the most recent version of the EU Standard contractual clauses (SCC),
  - provide a written statement on its local applicable surveillance law and its potential conflicts with agreed data protection responsibilities on a case-by-case basis to support a transfer impact assessment,
  - provide effective supplementary technical, contractual, or organizational measures to ensure that provider's contractual commitment to data subjects rights (e.g., access, correction and deletion) can be effectively applied in practice and are not thwarted by law in the 3rd country,
  - proactively inform about changes in such 3rd country law and being responsive in cases of DBG entity transfer impact assessment iterations.

9 Overview of material changes

This document is owned by Group Compliance. It is subject to annual review. The following section provides an overview of all material changes to reflect the evolution of the document.

Version	Date	Remark
1.0	November 2020	Initial version was created.
1.1	November 2021	Annual review