Data Protection Compliance

Guidance on Personal Data Processing Principles

Version 1.0

Last revised on 5 December 2023

Table of Contents

1. Objective

The objective of the Guidance on Personal Data Processing Principles (the "Guidance") is to provide guidance on Personal Data Protection Policy Principle 3: The Group must comply with the Personal Data Processing Principles.

2. Definitions

The below definitions apply to the terms used throughout the Guidance.

Appropriate Technical and Organisational Measures	information security measures implemented at a technical and organisational level to ensure a level of security appropriate to the risk presented by the Personal Data Processing activity, in particular from accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. The Appropriate Technical and Organisational Measures must take 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 the Data Subject.
Anonymisation	the process by which Personal Data is rendered irreversibly anonymous in such a way that a Data Subject is no longer identified or identifiable, so far as possible, either from the data set at issue or by combining the data set with other data from sources within the Group or outside the Group.
Automated Decision-Making ("ADM")	the ability to make decisions by solely technological means (e.g. by use of algorithms) without human involvement and which produces legal or similarly significant effects for the Data Subject. Automated decisions can be based on any type of data.
Business Unit ("BU")	a generic term that covers Personal Customers, Business Customers and Large Corporates and Institutions.
Common Law	the body of customary law, based upon judicial decisions and embodied in reports of decided cases.
Data Controller	a natural or legal person, public authority, agency or other body who (either alone or jointly or in common with others) determines the purposes for which, and the manner in which, any Personal Data is processed, or is to be processed.
Data Processor	a naturalor legal person, public authority, agency or other body, which processes Personal Data on behalf of the Data Controller.
Data Protection Authority[1]	an independent public authority that supervises, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against possible violations of the General Data Protection Regulation and relevant national laws. They are also the authority for approving Personal Data Processing if the processing is of such a nature, that their approval is needed. There is one in each EU/EEA Member State and the United Kingdom ("UK").

[1] Definition must be understood in line with the definition of "supervisory authority" in GDPR.

Data Protection By Design and By Default	a legal requirement that obliges Data Controllers and Data Processors to design and by default implement and configure, systems, processes and products with data protection and confidentiality in mind. Data Protection By Design and By Default means that measures are put in place to ensure that Personal Data Processing complies with the Personal Data Processing Principles in the GDPR and that Appropriate Technical and Organisational Measures are applied.
Data Protection Officer ("DPO")	the Data Protection Officer ("DPO") is a regulated role, with tasks defined in the GDPR. The GDPR requires that organisations such as Danske Bank A/S appoint a DPO to monitor compliance, inform and advise, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and Data Protection Authorities. The Group appoints a single DPO, except where a local requirement or regulatory expectation requires the appointment of a local DPO (e.g. Northern Bank Ltd).
Data Subject	any natural person that can be identified, directly or indirectly, whose Personal Data is processed by the Group and its Data Processors, (e.g. an employee, a customer, a guarantor, a person holding a Power of Attorney, a signatory of a company, a sole trader, etc.). For the purposes of GDPR requirements, Data Subjects do not include deceased persons. National data protection rules may apply up to 10 years after the death of the Data Subject depending on the jurisdiction where the Personal Data Processing takes place.
Derogation	a condition set out in GDPR /UK law upon which a one-off/restricted International Transfer can take place where a Transfer Tool does not apply.
Employee	for the purposes of this Guidance only, an Employee is: • a permanent or temporary employee of the Group; • a contingent worker: an individual who is working for the Group but is not directly employed by the Group (including officers, consultants, contractors, agency workers, student workers, etc.).
GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Group	Danske Bank A/S including its branches and Subsidiaries.
Group Functions	a generic term, which covers the Group's non-Business Units and back office functions: CAO Area, CFO Area, Company Secretariat, Group HR, Group Internal Audit, Group Legal, Group Risk Management, Group Sustainability, Stakeholder Relations, Communications & Marketing, Technology & Services.
Input Providers	Stakeholders who have provided input to the governing information.
International Transfer	any Transfer of Personal Data to a Third Country or an international organisation outside the EEA. The term covers any transfer, disclosure, handover, transmission of Personal Data or grant of access (including remote access) to Personal Data. It covers both Intra-Group Transfers as well as Transfers with external parties, such as external vendors and partners of the Group, provided that one of the parties to the Transfer is located in a Third Country, including any onward Transfers of the Personal Data within a Third Country or to another Third Country.
Personal Data	any information concerning an identified or identifiable natural person ("Data Subject"), e.g. customers, employees and their respective representatives. An identifiable Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, address, e-mail, phone number, IP address or by means of other data such as metadata, purchases, location or payment transaction data. Personal Data can also include references to one or more factors specific to the physical, physiological, behavioural, economic, cultural or social identity of a person. the Personal Data includes information concerning Data Subjects connected to a corporate customer or other legal persons. A Data Subject connected to a corporate

	customer or other legal person could be an employee, director, board member, member of partnership, a beneficial owner, etc.
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Personal Data Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated/technical 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.
Privacy Notice	notification mechanism by which Data Subjects are notified about the purposes, legal basis and their rights in relation to the use of their Personal Data by Data Controllers and Data Processors
Process Owner	the person accountable for the oversight of the management of a business process and its execution during its lifecycle. This includes the underlying activities of the process as well as the related business procedures and SOPs.
Product Owner	the person who is overall responsible for the product during its lifecycle including the ongoing assessment and monitoring of the product.
Profiling	any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject, in particular to analyse or predict aspects concerning that Data Subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Recipient	a natural or legal person, public authority, agency or other body, to which the Personal Data are disclosed, whether a Third Party or not. Public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with EU, EU/EEA Member State or UK law are not regarded as Recipients.
Record of Processing	a regulatory requirement whereby the Group's use of Personal Data is recorded in accordance with the requirements in Article 30 of the GDPR/UK GDPR.
Rights and Freedoms of the Data Subject	general collective term referring to the fundamental rights and freedoms of the Data Subjects. Data Subject's rights refers in particular to the protection of Personal Data included in the Charter of Fundamental Rights of the European Union and the Data Subject's right to access and control of their Personal Data provided for in the GDPR. Freedoms refers specifically to the absence of necessity, coercion, or constraint in choice or action over how Data Subjects exercise their rights in respect of their Personal Data.
Service Owner	the person accountable for the management of a business service and its execution during its lifecycle.
System Owner	the employee (or tribe lead within the BWOW structure) who is accountable for a system that processes Personal Data.
Third Country	any country other than the EEA countries. For the purposes of UK data protection law, a Third Country is any country outside of the United Kingdom.
Transfer	the transfer, disclosure, handover, transmission of Personal Data or grant of access to a Data Processor or Data Controller (including remote access) to Personal Data.
Transfer Tool	collective term referring to the mechanisms described in Chapter V of the GDPR that can be used as a basis for an International Transfer. This term covers for example Standard Contractual Clauses and Binding Corporate Rules.
Vulnerable Data Subjects	Data Subjects can be vulnerable where they are especially susceptible to detriment due to their personal circumstances, , particularly when a firm is not acting with appropriate levels of care. Data Subjects may be considered vulnerable where there is a significant imbalance between the position of the Data Subject and the Data Controller. Vulnerable Data Subjects may be unable to easily consent to, or oppose, the processing of their data,

	or effectively exercise their rights. Vulnerable Data Subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.), and in some cases employees.

3. Scope

This Instruction applies to all Personal Data Processing performed by the Group.

4. Personal Data Processing Principles

4.1. Overview

The GDPR provides seven principles relating to processing of Personal Data:

Lawfulness, fairness and transparency	Personal Data must be processed lawfully, fairly and in a transparent manner.
Purpose limitation	Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
Accuracy	Personal Data must be accurate and kept up to date.
Storage limitation	Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary to achieve the processing purpose.
Integrity and Confidentiality	Personal Data must be processed in a manner that ensures appropriate security of the Personal Data. This includes the implementation of Appropriate Technical and Organisational Measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage.
Accountability	Appropriate governance and records must be implemented in order to demonstrate compliance with the processing principles (above) and the provisions of the GDPR more generally.

Process, Product, System and Service Owners (hereafter referred to as "Personal Data Processing Owners") must ensure that products, processes and systems/applications that include Personal Data Processing comply with the Personal Data Processing Principles.

4.2. Lawfulness, Fairness and Transparency

4.2.1. Lawfulness

Personal Data Processing is lawful only when a legal basis under data protection law applies.

Personal Data Processing Owners must identify a legal basis for Personal Data Processing and document it prior to commencing Personal Data Processing.

Further information on identifying appropriate legal bases for processing can be found in the relevant Guidance on Legal Basis for Personal Data Processing.

If no legal basis applies to the processing activity, it is likely that the Personal Data Processing is unlawful and in breach of the lawfulness principle and should not commence. Where this is the case, the Process Owner must seek advice from Group Legal and/or Data Protection Compliance.

In addition to identifying a legal basis under data protection law, Personal Data must not be used for activities which are unlawful in a more general sense. Personal Data Processing must comply with EU and national legislation, including legislative, statutory and Common Law obligations, whether criminal or civil. When designing a new product or process which uses Personal Data, Personal Data Processing Owners should seek local legal advice in the country (or countries) where the processing will take place to consider local legal implications of the proposed activities, for example implications according to local employment law, social security law, marketing, tax and bookkeeping laws, etc.

If processing involves committing a criminal offence or breaking a civil or administrative law, it will obviously be unlawful. Processing may also be unlawful if it results in, for example:

- a breach of a duty of confidence
- exceeding legal powers or exercising those powers improperly
- an infringement of copyright
- a breach of an enforceable contractual agreement
- a breach of industry-specific legislation or regulations

This is a non-exhaustive list. Local legal requirements must always be taken into account. Personal Data Processing Owners must ensure that Personal Data Processing is in accordance with local legal requirements and should consult local Legal teams in relevant market areas as necessary.

If Personal Data is processed unlawfully, Data Subjects have the right to erasure of that data or restriction of the Group's use of it.

4.2.2. Fairness

Personal Data must not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected, deceptive or misleading to the Data Subject. Personal Data Processing must take place within the reasonable expectations of the Data Subjects. It also requires consideration of any possible negative consequences Personal Data Processing may have on the Data Subject.

Consideration must be given to the specific circumstances of the Data Subject. A process that is acceptable for many Data Subjects, but unfairly discriminates or would have unjustified negative effects on one Data Subject, would be a breach of this principle. The Group must implement specific safeguards and protections in order to guarantee that all Data Subjects do not suffer unjustified negative consequences and can effectively exercise their Rights and Freedoms regardless of their capacity or circumstance. For example, the needs of Vulnerable Data Subjects must be taken into consideration in process or product design.

Personal Data Processing must not take place in a secret or hidden way. See further section, 4.2.3 Transparency.

4.2.3. Transparency

Data Subjects must be informed about how and why their Personal Data is used. This is achieved through the provision of privacy information to Data Subjects, for example:

- Privacy Notices
- in cases where consent for Personal Data Processing is collected (special requirements apply in addition to the provision of Privacy Notices[2])
- tailored notification measures (for example, where automated decision making and profiling is used)

[2] For requirements in relation to Personal Data Processing on the basis of consent, see the Instruction on Legal Basis for Processing Personal Data.

Privacy information must be accessible and easy to understand. For example, a signposted link to a webpage and/or an explicit Privacy Notice document that uses clear and plain language (in the local language).

Information must be provided to the Data Subjects on the identity of the Data Controller, the purposes of the Personal Data Processing and further information to ensure fair and transparent processing. Information must be provided about their rights to obtain information about and access to the Personal Data about them that is being processed.

Data Subjects must be made aware of the risks, rules, safeguards and all Data Subject rights in relation to the Personal Data Processing and how to exercise those rights.

Transparency about the processing of Personal Data also applies where there is no direct relationship with the Data Subject and where Personal Data is collected from another source, for example from public registers or credit reference agencies. This may have implications for complying with the Fairness principle as Data Subjects may not be aware that their Personal Data is being processed. When Personal Data is collected indirectly from another source, privacy information must be provided to Data Subjects at an appropriate time.

Further information on notification requirements to Data Subjects, can be found in the Instruction on Data Subject Rights.

4.3. Purpose Limitation

4.3.1. Purpose for processing

The "purpose" of Personal Data Processing means the reason and intentions for why the Personal Data is used and the objective that is being pursued.

The Group must collect Personal Data only for specified, explicit and legitimate purposes, and not further process the Personal Data in a manner that is incompatible with the purposes for which it was collected. The Personal Data collected and the metho for Personal Data Processing must be proportionate to achieve the intended purpose.

The Group must ensure that the purposes for processing Personal Data are identified and clearly documented before the Personal Data is collected or used (see further section 4.8.1).

The purpose of the processing must be clearly communicated to the Data Subject as part of the privacy information provided (see section 4.2.3).

4.3.2. Using Personal Data for new purposes

The Group must ensure that Personal Data is only used for the purpose for which it was originally collected and within the reasonable expectations of the Data Subject.

i. Compatible purposes

If the Group wishes to use Personal Data collected for a specific purpose for a new purpose, this is allowed if the new purpose is compatible with the original purpose. To consider whether the new purpose is compatible with the original purpose, the Group must take into account:

- any link with the original purpose
- the context in which the Personal Data has been collected
- the nature of the Personal Data
- the possible consequences of the intended further processing for Data Subjects, and
- the existence of appropriate safeguards (e.g. security measures)

Where the purpose is compatible, it is likely the same GDPR legal basis will apply.

ii. Non-compatible purposes

To assess compatibility, consideration must be made to whether the new purpose is very different from the original purpose, would be unexpected, or would have an unjustified impact on the Data Subject. In practice, where this is the case, specific consent may be required to use or disclose data for this type of purpose.

4.4. Data Minimisation

The Group must only collect, use and store Personal Data that is adequate, relevant and limited to what is strictly necessary to achieve its processing purposes. The Group must not collect Personal Data because it 'may' be useful in the future or retaining data 'just in case'. It is important to assess exactly what data and level of identification of the Data Subject is required when designing the processing activity.

The Data Minimisation Principle also applies to the method of processing, which must be necessary and proportionate to the purpose for the Personal Data Processing. Where there is a choice of processing methods, the Group must choose the least privacy intrusive method.

Where excessive data is collected, Data Subjects have the right to request erasure of their Personal Data.

The Group must not collect insufficient or incomplete Personal Data. Collecting insufficient data can cause harm to the Data Subject if decisions are based on insufficient or incomplete information which may negatively affect the Data Subject. This requirement is closely linked to the Data Accuracy Principle (see section 4.5).

4.5. Accuracy

Personal Data must be accurate and where necessary, kept up to date. The Group must ensure inaccurate, insufficient/incomplete, or outdated data is deleted or amended. To comply with this principle, the Group must:

- take reasonable steps to ensure the accuracy of any Personal Data collected/used
- ensure that the source of any Personal Data is clear and properly documented
- carefully consider any challenges to the accuracy of information and
- regularly review Personal Data and determine whether it is necessary to update the information.

The above list is non-exhaustive and there may be other actions required to ensure the accuracy of data depending on the context and nature of the Personal Data Processing

4.5.1. Rectification of inaccurate data

Data Subjects have an absolute right to have incorrect Personal Data rectified (for more information see the Instruction on Data Subject Rights (Right to Rectification)).

In some cases, it is reasonable to rely on the Data Subject to make contact and inform when their Personal Data has changed, such as when they change address or other contact details. However, due to the nature of Personal Data Processing that takes place in the Group, the Group must periodically ask Data Subjects to update their Personal Data.

When Personal Data Processing involves a decision as to whether the Data Subject will be eligible for a product or service, Personal Data must be proactively checked and updated. The more important it is that the Personal Data is accurate, the greater the effort required to ensure its accuracy.

4.5.2. Historic data

There may be circumstances where it is not necessary or appropriate to delete out-dated Personal Data because it is necessary to keep a record of historic data. For example, when addresses are changed it may be necessary to keep a record of the old address and the date the new address was added for audit or regulatory compliance purposes.

4.6. Storage Limitation

4.6.1. Retention and deletion

The Storage Limitation principle requires that Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed. In practice, this means that Personal Data cannot be kept in an identifiable form for longer than it is needed.

Once the Group no longer needs Personal Data for the purpose for which it was processed it must be deleted unless there is another legal basis for retaining it. The Storage Limitation Principle is closely linked to the Data Minimisation Principle (see section 4.3).

The Group must ensure that all Personal Data has appropriate retention rules and that these are clearly documented and justifiable.

When determining the duration of retention periods such considerations may include:

- legal or regulatory requirements
- relevant industry standards
- statutory limitation and the need to defend legal claims
- sensitivity of Personal Data held
- longevity of the data (how relevant is the data over time)
- purpose for continued processing
- data sharing arrangements (e.g. any contractual conditions attached to the retention/use of Personal Data)

Further information on retention and deletion can be found in the Business Procedure on Retention and Deletion of Personal Data.

4.6.2. Anonymisation

Where Personal Data is correctly anonymised, it can no longer identify a Data Subject and is no longer classified as Personal Data. Anonymised data is not subject to the GDPR/national data protection rules and can therefore be used and retained with less restrictions.

Relevant guidance on Anonymisation, can be found in the Business Procedure on Retention and Deletion of Personal Data.

4.6.3. Data preservation

In exceptional circumstances, the Group may be required to keep data, including Personal Data beyond normal retention periods for the purposes of an ongoing investigation and/or litigation. This is often referred to as “data preservation” or “subject to disposal hold”.

Such preservation of Personal Data will only be authorised where there is a legal requirement (recognised in EU, EU/EEA Member State or UK law) to preserve that data or where the Group’s legitimate interest to use a specific data set for an investigation is not overridden by the interests or fundamental Rights and Freedoms of the Data Subject to whom the Personal Data refers.

In cases related to the preservation of Personal Data, Group Legal and Data Protection Compliance must be consulted. For Danske Bank UK, the initial contact should be with the local Regulatory Compliance function.

Further information on preservation of Personal Data can be found in the Business Procedure on Retention and Deletion of Personal Data.

4.7. Integrity and Confidentiality

Personal Data must be processed in a manner that ensures appropriate security of Personal Data, including protection against unauthorised or unlawful Personal Data Processing and against accidental loss, destruction, or damage.

The Group must implement Appropriate Technical and Organisational Measures that take into account the state of the art (e.g. the state of technical advancements) and costs of implementation, as well as the nature, scope, context and purposes of the Personal Data Processing.

Appropriate Technical and Organisational Measures must include physical and estates security measures as well as information security measures. The Integrity and Confidentiality Principle goes beyond requirements for the storage and transit of Personal Data. Every aspect of Personal Data Processing is included in this processing principle (such as governing documents, day-to-day document handling and information management, physical data security, and access management (for documents, systems and estates), physical and electronic mail management and clear desk etiquette, etc.), not just cybersecurity (system, online, data and device security).

The Technical and Organisational Measures must be 'appropriate', which means they must consider varying likelihood of the identified risks materialising, and the severity of the risks posed to the Rights and Freedoms of the Data Subject. The security measures adopted must be proportionate to the risk to the Data Subject and should meet any legal/regulatory requirements.

Appropriate Technical and Organisational measures will include:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems via physical means (e.g. lockable cabinets, access barriers to buildings, etc.) and digital means, (e.g. encryption, pseudonymisation measures, etc.)
- measures to ensure compliance with any wider legislative or industry specific security requirements
- clear definition of roles and responsibilities for ensuring information security
- appropriate continuity and resilience measures to restore Personal Data in a timely manner in the event of a physical or technical incident
- appropriate processes to test, assess and evaluate the effectiveness of security and access measures and to demonstrate the Group's compliance with these principles on an ongoing basis.

4.8. Accountability

The accountability principle requires the Group to be able to demonstrate how it complies with the Personal Data Processing Principles.

4.8.1. Evidencing Compliance

The Group must implement appropriate and effective measures, including relevant evidence and records to be able to demonstrate the compliance of its Personal Data Processing. The Group must also be able to demonstrate the effectiveness of the implemented measures.

The Group's accountability for its Personal Data Processing and for decisions made in connection with those activities also applies to Personal Data Processing carried out by Third Parties on behalf of Data Controllers in the Group, including Data Processors. Data Controller's in the Group are also responsible and accountable for ensuring that Transfers of Personal Data to other Data controllers is carried out in accordance with the Personal Data Processing Principles.

Accountability measures include, but are not limited to:

- a Personal Data protection governance framework, documented in Group-wide Policy, Instructions, local governance and Standard Operating Procedures (SOPs) at BU/Function level
- allocation of clear roles, responsibilities and accountabilities defined in accordance with the three lines of defence model, including risk ownership, risk oversight and risk assurance

- Application of a 'Data Protection by Design and By Default' approach to system, process and product development, including
    - implementation of a robust control framework (see further, Instruction on Data Privacy Risk Assessments)
    - execution and documentation of appropriate risk assessments (see further, Instruction on Data Privacy Risk Assessments)
- execution and documentation of relevant monitoring activities on a continuous basis including reporting of activities and risk findings/outcomes
- documented adherence to relevant codes of conduct and membership of certification schemes where appropriate
- documented due diligence/checks and written contracts with Third Parties, including Data Processors that process Personal Data on the Group's behalf or with other Data Controllers with whom the Group shares Personal Data (see further, Instruction on the Use of Data Processors and Instruction on International Transfers of Personal Data)
- recording and, where necessary, reporting Personal Data Breaches to the relevant Data Protection Authority
- provision of ongoing mandatory and specialised training for Employees with associated record-keeping

4.8.2. Records of Processing

The Group must establish a process for recording Personal Data Processing in a Record of Processing. Each Data Controller in the Group must record the Personal Data Processing carried out under their responsibility.

Each Data Processor in the Group must record the Personal Data Processing carried out on behalf of a Controller. This requirement applies to Personal Data Processing carried out for Data Controllers inside the Group as well as external Data Controllers.

The Record of Processing must include:

- the name and contact details of the Data Controller (and, where applicable, the joint controller, the controller's representative) and the Group Data Protection Officer[3]
- the purposes of the Personal Data Processing
- a description of the categories of Data Subjects and of the categories of Personal Data;
- the categories of Recipients to whom the Personal Data have been or will be disclosed including Recipients in Third Countries or international organisations[4]
- where the processing includes an International Transfer(s), identification of any Third Country or international organisation
- where the processing includes an International Transfer(s) based on a Derogation, a description of the safeguards applied (see Instruction on International Transfers of Personal Data
- where possible, a description of the retention rules to be applied to the different categories of Personal Data
- where possible, a general description of the Appropriate Technical and Organisational Measures

Personal Data Processing Owners must ensure that information related to the Personal Data Processing under their responsibility is recorded in the Group's Records of Processing.

[3] Data Processors must record the names and contact details of the Data Processor as well as the Data Controller

[4] Requirement applies to Data Controllers only.

5. Change log

Date	Version number	Comments/changes
5 December 2023	1.0	Following the retirement of the Instruction on Data Processing Principles under GDPR, part of the content moved to the Guidance.