KTL KREDIETRUST LUXEMBOURG

1. Executive summary

At Quintet Private Bank Europe SA and its affiliates (the "**Group"),** we take privacy and confidentiality matters very seriously and we handle Personal Data in accordance with any applicable data protection laws, regulations, and guidelines ("**Data Protection Regulations**"). This Privacy Notice (*hereinafter* "**B2B**") is a **prior information notice** advising how we will process your Personal Data and providing information on your rights in order to comply with the Group's requirement under the Data Protection Regulations, including the so-called GDPR[1] and other applicable Data Protection laws[2].

Kredietrust Luxembourg S.A. ("KTL"), as a Luxemburg-based management company incorporated under the laws of the Grand Duchy of Luxembourg in the form of a public limited company (Société Anonyme) and registered with the Luxembourg Trade and Companies Register under the number B 65.896 supervised by the Luxembourg regulator ("**CSSF**") is part of the Quintet Group.

	Controller : when onboarding Customers see General terms and conditions Kredietrust Luxembourg S.A. (KTL) 88 Grand rue - L- 1660 Luxembourg - RCS : B65.896 *The firm is approved by the Commission de Surveillance du Secteur Financier (hereinafter the "CSSF"), with offices at: 283, route d'Arlon, L-1150 Luxembourg* **Conducting Officer** : Cyril Thiébaut **Processor** : when acting on behalf of the Management Company or its delegated **Data protection Office** : see Who should I contact & how do I exercise my rights? EU countries : DPOGROUP@QUINTET.COM		Within information technology innovation, we may use some **Artificial Intelligence** tools to support operational activities (*e.g. Microsoft Copilot, Deepl*). Prior to using such a tool, or when high inherent risk has been identified, we will assess the risk according to an individual's fundamental rights and to prevent a security incident (= data breaches). When we are using electronic signature, we collect information for authentication and execution in a secure manner. We have put in place **technical and organisational measures** to manage your Personal Data in a **safe manner** (*e.g. password policy, management of privileges and access rights, prevention of data leakage*).
	We use your Personal Data *(= information about you*) mainly for the following purposes: When we have your consent (*e.g. use of photographs for marketing purposes*) and when there is a legitimate interest, such as		We do not share your Personal Data with third parties, such as the provider of our core banking system, (Lombard Odier T&O Services (Europe) S.A), third party brokers or IT providers (e.g. *Microsoft 365 cloud, HubSpot*) without first performing a risk assessment, due diligence and a contractual review which

[1] EU Regulation 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)" (the "**GDPR"**).

[2] UK General Data Protection Regulation ("**UK GDPR**"), (GDPR is retained in law as the UK GDPR) and explains the data protection regime that applies to UK businesses and organisations. processing of personal data is subject to the UK GDPR and DPA 2018.

	the safety and protection of the workplace, (*e.g. use of CCTV*). We do not retain your Personal Data for longer than is necessary for the business or for legal requirements.		may include additional safeguards (*e.g. appendix to a contract where the duties and obligations of both parties are described in the context of data protection, including an appropriate standard clause, if necessary*). When we transfer your Personal Data outside of your Entity's country, we will make sure that it is protected in the same way as if it is being used in your own country. As we are a cross border business, we may share your personal data with our EU affiliates within the Group but we will be legally bound by an **Intra-Group Agreement** (*e.g. Service Level Agreement*).

2. What is the scope, purpose and target audience of this Privacy Notice?

- **What**: the category of personal data collected and processed and, which method will be used, depend significantly on the services or products[3] you have selected.
- **When**: you are considering entering into a professional / institutional client relationship or you are already a professional / institutional client of The Group or any of its affiliates (the **"Entity"** or **"Entities**), the terms "**we**" or "**our**" or "**us**" used in this Privacy Notice refer to The Group.
- **What for**: you have a **contractual relationship** with us, this Notice is a part of your contract with us, and you are bound by it.

3. Who is responsible for Data processing and how to contact us?

Within the Data Protection framework, "*Personal Data*" means any information which allows direct or indirect identification of an individual, while "*Processing*" means any operation or set of operations which is performed on personal data (e.g., collecting, sending, using, extracting, storing, or sharing personal data).

Consequently, the Group and KTL may act **as a data controller or a data processor** with regards to services and products delivered to you:

[3] Take a look at our offerings for professionals in Quintet Servicing & Financial Intermediaries, Fund Solutions, Private Label Solutions or custodian network services

Data subject / Quintet roles	Third party or Partner's Representatives	Administrators & Professional / Institutional client representatives	Shareholders, end Clients as Individuals
Data controller who is controlling the onboarding process workflow 	Third party onboarding with standard AML-KYC or due diligence as per legal requirements form Supervisory Authorities.	Client onboarding including AML - KYC operations according to our legal obligation (including administrators and representatives of professional / institutional client) Client file review including a review of KYC operations according to our legal obligation (including the responses to transfer agent's due diligence requirements)	Transaction screening and compliance with AML legal requirements *(including shareholders transactions such as subscription / redemption of third party funds*) regulatory controls and reporting, Tax reporting (FATCA, CRS...)
Data processor when KTL is delivering services (*e.g. Management Company services, Funds managements*) 	Third party legal representative information needed for performing a contract and related to daily business.	Funds and Asset servicing: • Depository Bank • Paying Agent Services • Fund Management Depositary and Global Custody Services to internal and external Luxembourg investment funds, Banks & Insurance Companies, External Asset Managers.	

Please note any operation or set of operations where your personal data is collected is covered by a Data Processing Agreement, in addition to the master service agreement.

For any inquiry related to personal data processing, please contact our Group Data Protection Office : see section 12 Who should I contact & how do I exercise my rights?

4. What types of Personal Data might be processed?

KTL provides portfolio management. When performing such service, the KTL and Group may collects and processes Personal Data relating to you

- **directly** from you: in the context of our business relationship (*e.g. due diligence enquiries, on boarding documentation, correspondence, which may include written, telephone or electronic communications*);

- **indirectly** (*e.g. in your capacity as a director, officer, authorised signatory, employee, investor and/or beneficial owner and any other related person(s) of our clients or third party);*
- from **publicly accessible sources** (*e.g. commercial and association registers, press, internet*), bankruptcy registers, tax authorities, including those that are based in and outside the EEA and UK, governmental and competent regulatory authorities, credit agencies, fraud prevention and detection agencies and organisations and internal lists for prevention and detection of financial crime activities maintained by the Group globally or that is legitimately transferred to us by our affiliates or other third parties (*e.g. third party service providers, investment funds, their management companies and/or general partners and their relevant service providers and delegates such as the portfolio managers, distributors, etc*.).

Please note collecting **some personal data is necessary** in the following cases:

- to offer our services to you or to continue offering a service to you due to our legal obligations (*e.g., tax status such as FATCA*[4]*, CRS*[5] *or anti-money laundering regulations*). What we collect will be explained in the relevant services application form or client profile form. If you do not provide us with the required information, we will not be able to offer certain services to you.
- When we are using electronic signature data to sign documents electronically (*e.g. easy fast legal signature on documents or as a means of authentication and verification, with regard to contractual commitments.*), we collect the surname, first name and professional email address for 2 distinctive purposes:
    - authentication and execution of documents to comply with legal or regulatory requirements, including litigation and the management of complaints;
    - to prevent, detect and investigate fraud (e.g. a user's electronic signature includes the signature itself and the contact data associated with this signature).

For more details about the category of personal data collected, please refer to the table *in the* appendix*.*

5. What principles do we follow when we process your Personal Data?

Personal data processing must comply with the **7 data protection principles**:

1. **Lawfulness** *(= only process personal data if we have a lawful basis*), **Fairness** *(= collect and process your personal data in a way that is not unduly detrimental, unexpected, or*

[4] FATCA stands for **F**oreign **Ac**count **T**ax **C**ompliance **A**ct, "*which was passed as part of the HIRE Act, generally requires that* ***foreign financial Institutions and certain other non-financial foreign entities report on the foreign assets held by their U.S. account holders or be subject to withholding on with holdable payments***". See more details on Internal Revenue Service's website (US public body)

[5] CRS - Common Reporting Standard (CRS) is an information-gathering and reporting requirement for financial institutions in participating countries / jurisdictions, to help fight against tax evasion and protect the integrity of tax systems.

misleading to the individuals concerned) and **Transparency** *(= this Notice provides information about how Quintet follows the rules in processing your personal data*);

2. **Specific purpose** *(= process your personal data only if we have clearly identified our purpose or purposes and have documented the purpose(s)*);
3. **Data minimisation** *(= collect the minimum amount of personal data required for that purpose(s));*
4. **Accuracy** *(= personal data shall be correct and up to date);*
5. **Retention** *(= kept for no longer than is necessary, which might be defined by a national law*);
6. **Security** *(= implement technical and organisation measures for protecting against unauthorised access; unlawful processing, and accidental loss or destruction, by activating Confidentiality, Integrity, Availability and Resilience of our Information systems*);
7. **Accountability** *(= KTL Management is accountable for the processing of personal data needed for their business activities and KTL has put in place a compliance framework and record of processing activities to demonstrate compliance*).

6. What is the lawful basis for each type of Processing Activity?

Processing activity is defined as any use or operation(s) involving personal data. Each processing operation must be carried out for a specific purpose or operation *(= purpose, specificity, principle*) and have a defined legal basis *(= lawfulness principle*).

Therefore, the type and purpose of your Personal Data processed by us depends on our relationship. For instance, to assess your identity as the Fund administrator or asset manager (*e.g., AML-KYC*), Personal Data processed for onboarding, reporting, or, depending on shares and portfolios, for the purpose of meeting regulatory requirements.

Further, Personal Data is processed for administrative purposes such as keeping client file records, register of shareholders or for paying agent services (shareholders' subscription/redemption). Personal Data processing might also be carried out if you use IT resources or visit our premises. This may also include any monitoring carried out within The Group (*e.g., voice recording in line with MIFID regulation*).

For more details about the category of personal data collected , please refer to the table *in* appendix

7. Who do we share your Personal Data with?

To achieve the purposes described above (*see* section 4), we may transfer Personal Data outside of KTL and Quintet Group, as described below. We may transfer personal data to meet legal and regulatory obligations or share Personal Data with public organisations,

administrative or legal authorities and supervisory bodies. These transfers may take place within or outside of the European Economic Area (EEA)[6] or the United Kingdom:

- To third parties for the purpose of compliance with regulatory requirements, the fulfilment of our contractual obligations, self-regulation and market practices, conditions of issuers and other requirements in connection with the investments or products you have chosen *(insurance companies, correspondent banks, transfer agents, brokers or custodians*);
- To third parties providing services:
    - Core banking IT systems / Operations services outsourced to Lombard Odier T&O Services (Europe) S.A.
    - IT services and products including telecommunications, IT providers including providers of cloud solutions (*e.g.,* Microsoft 365 cloud*, HubSpot*).
    - Central administration (administrative and transfer agent services) outsourced: European Fund Administration S.A.
    - Third party brokers.

We may also be obliged to disclose data under certain laws or by order of court or other competent regulatory bodies or may be permitted to disclose it under applicable Data Protection Regulations.

8. What are the appropriate safeguards in force regarding data transfers?

When we transfer Personal Data outside of your Entity's country, we will ensure that adequate Data Protection safeguards are in place. This means that when we transfer your Personal Data outside of your Entity's country, we will make sure that it is protected in the same way as if it is being used in your own country. We will use appropriate safeguards in line with the local law of your jurisdiction. When you are in the EEA or UK and we transfer Personal Data to an EEA or non-EEA country, we will use one of the following safeguards:

- Adequacy decisions adopted by the European commission such as the latest Adequacy decision for the EU-US Data Privacy Framework[7] on 10/07/2023 and also extended to the UK by the UK Government (*e.g. only third party or provider recorded in* US Data protection Framework);
- Deploy adequate contractual guarantees such as EU Standard Contractual Clauses (SCC)[8] or

[6] UK is an adequate country until the 27/06/2025. That means Quintet Group may share personal data from any data subject with its subsidiary located in UK without any specific safeguards. See COMMISSION IMPLEMENTING DECISION of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom

[7] See Commission Implementing Decision (EU) of 4 July 2023 within **EU-US data transfers**

[8] See Commission Implementing Decision (EU) 2021/914 of **4 June 2021** on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance)

UK International Data Transfer Agreement (IDTA)[9] and supplementary measures recommended by European Data Protection Authority or the UK Supervisory Authority to ensure effective compliance; or

- Process such transfer under one of the data protection framework derogations [10], for example with your consent, assertion or enforcement of legal claims, overriding public interests or because the transfer is necessary to protect the physical integrity of a data subject.

For more details about this topic, do not hesitate to contact us or (*see* Section 12).

9. How do we use automated tools and profiling?

How do we manage the profiling?

"Profiling" uses aspects of an individual's personality, behaviour, interest, and habits to make predictions or decisions about them, such as to control and detect money laundering, terrorism, fraud and assess risk of offence according to regulatory and legal requirements (*e.g., analyse transactional data amongst other activities to identify potential suspicious patterns).*

How do we use automated decision-making processing?

We do not use any automated decision-making tools, but we do use the results of some automated tools to get a preliminary analysis of your situation:

- AML (= **A**nti-**M**oney **L**aundering *Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*) scoring for Investment management and Wealth planning: we monitor your personal data from the entry into a relationship to detect any fraudulent or illegal activity, in relation to financial crimes or terrorism financing.
- Within information technology innovation, we may use some Artificial Intelligence tools to support operational activities (*e.g. Microsoft Copilot, Deepl*). Prior to using such a tool, or if a high inherent risk has been identified with a potential profiling output, we will assess the risk according to an individual's fundamental rights and to prevent a security incident (= data breaches) according to the relevant legal requirement[11].

We use these automated tools to assist in our decision making. **We do not solely rely on them to make any decisions**. Therefore, **final decisions are made by members of our Asset Servicing, Funds Management and Advisory teams**.

---

and Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of Personal Data Version 2.0 , EDPB , 18 June 2021, p. 9 § 4

[9] See International data transfer agreement and guidance, ICO

[10] See art 49.1.a, GDPR and UK GDPR

[11] See Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial intelligence Act)

Please note that you may object to such processing at any time (see 11. What are your rights regarding your Personal Data?)

How to manage cookies?

For more details, please see our Cookie Policy.

10. How do we protect your Personal Data?

For more details please go to our Client Privacy Notice available on our website.

11. How long will we retain your Personal Data?

We will store your Personal Data only for as long as is necessary for the relevant Processing activity to be completed and/or in accordance with the Personal Data retention period permitted under applicable law.

According to Luxembourg Commercial Code and Law of 5 April 1993 on the financial sector, we retain any personal information relating to a Client, third party and any Customer of a Client (as the case may be) for a maximum period of **10 years upon termination of the business relationship[12].**

As a financial services firm we can face legal holds which might require us to keep records for a longer period of time.

Other organisations that we provide information to, such as law enforcement and fraud prevention, will operate different retention periods over which we have limited, if any, control.

12. What are your rights regarding your Personal Data?

1. Under the GDPR you have several important rights, although these rights have exceptions. In summary, those include rights to:
2. Access your Personal Data. This includes obtaining a copy of the Personal Data we are processing;
3. Rectify any inaccurate Personal Data or complete any incomplete Personal Data;
4. Erasure of your Personal Data (= "Right to be forgotten");
5. Object to any Processing based on the Entity's legitimate interest. We will then cease the processing unless we have a compelling legitimate ground for the processing;
6. Ask us to restrict the Processing, for instance, when you contest the accuracy of the data or when the processing is not or no longer compliant with applicable law. This means that, except for storage, your Personal Data is only processed in specific cases (e.g., for the establishment, exercise or defence of the Entity's legal claims);
7. Receive the Personal Data you have provided to us in a structured, commonly used and machine-readable format and transmit those to another controller insofar as we process them in an automated way based on a contract with you or with your consent

[12] UK retain information relating to clients and third parties for a maximum of 15 years after termination of the client relationship.

(= Portability);

8. Withdraw your consent at any time when it has been collected.

In addition, if you feel that we did not act in line with data protection legislation, you may lodge a complaint with the supervisory authority of your country of residence, of your place of work or of the place of the alleged infringement:

- For EU residents where Quintet have offices: CNPD
- For other countries, please check the EDPB list

13. Who should I contact & how do I exercise my rights?

The Group and KTL has appointed a Group Data Protection Officer to manage and monitor our compliance with its data protection obligations.

When you are a Client of the Group or any FIM desk affiliates
Group Data Protection Officer, Quintet Private Bank (Europe) S.A. 43, Boulevard Royal - L- 2955 Luxembourg Email: DPOGROUP@QUINTET.COM

For more details please go to our Client Privacy Notice available on our website.

14.Appendix

14.1Table of the category of personal data

The Personal Data collected, used, stored or extracted from IT tools by us, and depending on your relationship with, or position within the Entity, may include the categories as follows:

Personal Data Category	Examples of Personal Data
Contact Details	(Customers legal representatives within Customer Due diligence and onboarding) Contact details: Name, surname, gender, physical and electronic address data, phone numbers
Identity	(Customers legal representatives within Customer Due diligence and onboarding) identification data (e.g. name, e-mail, postal address, telephone number, country of residence, passport, identity card, driving licence, tax identification number, source of wealth and invested amount of each Investor, identification) and authentication Data (e.g. sample signature) and your signature (electronic signature within DocuSign) or signature when you are a legal representative with a delegation of authority.
Professional	(Customers legal representatives within Customer Due diligence and onboarding) Regulatory or financial situation (e.g. for due diligence purposes), PEP status, professional contact details.
Sociodemographic	(Customers legal representatives within Customer Due diligence and onboarding) Such as your gender, date and place of birth and nationality.
Documentary Data	(Customers legal representatives within Customer Due diligence and onboarding) Which are stored in documents or copies of them (for example your passport or ID card).
Open Data and Public Records	(Customers legal representatives within Customer Due diligence and onboarding) Such as data available in public records.
Log data & other security data	credentials to connect to internet service Such as logical access control logs and systems audit trails.
Locational	Such as information on your physical location which may come from the place where you use our online services .

Personal Data Category	Examples of Personal Data
Financial	Such as your financial position, status and history, account number(s), personal assets and liabilities (*e.g., portfolios and shares*).
Behavioural	Such as your attitude to risk in investment (*e.g., MIFID questionnaire before entering a contract*).
Contractual	Such as information we collect or learn about you to provide our products or services.
Communications	Such as call recordings required under relevant law (e.g., MIFID[13]). Please note that any communications between you and staff in our front office, dealing room or asset management roles, which is required to transmit security orders, will be recorded
Special categories of Personal Data	In principle, we do not process Special Categories of Personal Data or Personal Data regarding criminal convictions and offences. However, in specific circumstances, you might communicate to us Special data or **personal information of a criminal nature (e.g. criminal record)** , which will only be collected and used if permitted by applicable law (*e.g., anti-money laundering*) or • with your explicit consent (e.g. such as placing markers on the account which tell us a client is hard of hearing or has poor eyesight); • where you have made the information public e.g. if you have been profiled in a newspaper or magazine. • where it is necessary for us to establish, exercise or defend legal claims. • when we have your permission for any optional use of biometrics e.g. facial recognition technology systems used to identify you.(*e.g IDNow*)

[13]See art 16.7, DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MIFID):" Records *shall include* ***the recording of telephone conversations or electronic communications*** *relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission, and execution of client orders. […] For those purposes, an* investment *firm shall take all reasonable steps to record relevant telephone conversations and electronic communications, made with,* ***sent from or received by equipment provided by the investment firm to an employee*** *or contractor* ***or the use of which by an employee*** *or contractor has been accepted or permitted by the investment firm."*

Personal Data Category	Examples of Personal Data
Transactional	(Customers legal representatives within Customer Due diligence and onboarding) Such as details about your investments, shares and securities portfolios
Marketing	Such as your preference to receive newsletters (*e.g., Counterpoint*) or event invitations. Please note a disclaimer and a consent informs you when pictures or videos of you are taken during conferences, social or business events.
CCTV Recording	Such as video surveillance recording when installed for physical security of our premises and according to local legal requirement.
Website	Such as cookies management. Please refer to Cookies Policy for more details.

14.2Table of lawfulness and processing type

The table below provides further details on the type of Personal Data Processing we may carry out.

Lawful basis	Type of Processing activities
Contractual agreement	The Processing activities are necessary before entering into a contractual relationship or to carry out the performance of a contract: (= Customers legal representatives within Customer Due diligence and onboarding) • Manage your investments, execute your instructions; • make and manage payments due to you or instructed by you;
Legitimate interest	Processing your Personal Information is based on the legitimate interest when it is necessary to safeguard our own legitimate interests, and your interests do not override our legitimate interest. We will balance both interests (= performance of a Legitimate Interest Assessment or LIA) before starting such a processing. This is performed on a case-by-case basis, and we will consistently monitor this. Processing based on legitimate Interests include:

Lawful basis	Type of Processing activities
	• monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services. • perform assessments and analyse client data for the purposes of managing, improving and fixing data quality. • protect our legal rights and interests; • manage and monitor our properties for crime prevention and prosecution of offenders, for identifying accidents and incidents and emergency situations and for internal training; • enable a sale, reorganisation, transfer or other transaction relating to our business. • use your Personal Data to tell you about products which we believe may be of interest to you or for the purposes of advertising, inviting you to social events, market research or surveys, unless you have expressly opted out. • Electronic signature to simplify and speed up the contractual commitment and authentication process and, in particular, to prevent fraud.
Legal or regulatory requirements	The Processing is necessary <u>to comply with our legal and regulatory obligations</u> such as: • perform checks and monitor transactions for preventing and detecting crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption and international sanctions (may require us to process information about criminal convictions and offences); • deliver mandatory communications to clients or communicating updates to product and service's terms and conditions; • investigating and resolving complaints and manage litigation; • conduct investigations into breaches of conduct and corporate policies by our employees. • provide assurance that Quintet has effective processes to identify, manage, monitor and report the risks it is or might be exposed to; • coordinate responses to business disrupting incidents and to ensure facilities, systems and people are available to continue providing services;

Lawful basis	Type of Processing activities
	• monitor dealings to prevent market abuse; • provide assurance on Quintet's material risks and reporting to internal management and supervisory authorities on whether the bank is managing them effectively; • perform general financial and regulatory accounting and reporting; • ensure business continuity and disaster recovery and responding to information technology and business incidents and emergencies; • ensure network and information security, including monitoring authorised users' access; • calls to our offices, to mobile phones, emails, text messages or other communications may be recorded and monitored to check your instructions to us; for preventing or detecting crime; to help us investigate any complaint you may make and as evidence in any dispute or anticipated dispute between you and us. • share data with police, law enforcement, tax regulators or other government and fraud prevention agencies where we have a legal obligation;
Consent	When you give consent to us to process your data for one or more specific purposes • confirm your identity for authentication when using online services. • processing activities which include Special Category of Personal Data, not based on legal or regulatory requirements. • sending you direct marketing where you have provided your consent to receive such marketing. • use of your picture if taken individually during some business or Social Events and are published on our corporate Website or social Networks. • any optional use of biometrics e.g. facial recognition technology systems used to identify you.(e.g IDNow).

15.Version control and metadata

Group Policy Document Metadata

Writer	Head of Quintet Group DPO
Owner	KTL
Policy document category	Policy (Level 1)
Group affiliates and population in scope	KTL stakeholders in Quintet Group
Annual certification process	no
Last approval date and Body	Quintet Group DPO
Effective date	01 December 2024
Expected review date	01 December 2026
Related documents	Quintet Group Privacy Notices
Policy replacements	n/a
Laws, regulations, and standards	General Data Protection Regulation 2016/679 (24/04/2016 – into force on 25/05/2018)
Risk taxonomy	Legal and Compliance risk type, Cross-Border risk sub-type

Group Policy Document version control

Version	Approval Body	Approval date	Changes
1.0	Group DPO	07/10/2024	• Format review based on new Privacy notices template • Minor changes and updates
1.1	Stakeholders: KTL	11/10/2024	• Review contact details of entity and list of processing of personal data • Minor changes about Artificial intelligence