Quintet Business to Business Privacy Notice

Table of Contents

Quintet Business to Business Privacy Notice

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

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 Business-to-Business Privacy Notice (*hereinafter* "**B2B**") is a **prior information** to give an overview of how we will process your Personal Data and of your rights in order to comply with The Group's requirement under the Data Protection Regulation, including the so-called GDPR[1] and other applicable Data Protection laws, such as Data Protection Act ("**UK GDPR"**)[2] or any subject matter national laws.

Please note

- The details on what data will be processed and which method will be used depend significantly on the services applied for or agreed upon.
- 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.
- Where you have a contractual relationship with us, this Notice is a part of your contract with us, and you are bound by it.

2. 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 any affiliate may act **as data controller or data processor** with regards to services and products delivered to you:

Data controller when we are performing AML-KYC duties according to legal requirement within	**Data processor** when The Group or its affiliates is delivering services within an agreement for
For administrators & representatives of professional/ institutional client: • Client onboarding including AML - KYC operations according to legal requirement (including administrators and representatives of professional/ institutional client) • Client file review including a review of KYC operations according to legal requirement (including the answer to transfer agent due diligence requirements) • **For shareholders, end client of professional/ Institutional client:** Transaction control including AML check according to legal requirement (	**For administrators & representatives of professional/ institutional client and their end clients or shareholders which data are processed during the following services:** **1- Luxembourg domiciled funds based on open architecture set up by KTL including** : • Manco • Domiciliation • Administrator & Transfer Agent • Depository Bank • Paying Agent Services • Fund Managers

[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.

including shareholders transactions such as subscription/redemption for third party funds)	**2- Global Custody Services** to third party Luxembourg domiciled & regulated funds, Banks & Insurance Companies, External Asset Managers , non-domiciled regulated and un-regulated funds.

Please note any operation or set of operations, including a data processing agreement, 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

Group Data Protection Officer,
Quintet Private Bank (Europe) S.A.
43, Boulevard Royal - L- 2955 Luxembourg
Email: DPOGROUP@QUINTET.COM

3. What types of Personal Data might be processed?

In order to facilitate, enable and/or maintain our business relationship The Group provides a broad range of services including among other:

- For Services for Luxembourg domiciled funds based on open architecture set up by KTL :corporate and domiciliation: *e.g. documentation to shareholders, convening AGM or directorship documentation*
- fund administration, accounting, paying agent & transfer agent: *e.g. subscription, payment to shareholders, register update, transfer of funds*, payment of distribution;
- reporting, tax: *e.g. Fatca, CRS Tax reporting MIFIR transaction report* and AML control & report
- administrative and support services (our "Services") to you and related parties (hereinafter our "Clients") which may involve services performed by suppliers or third-party service providers (*hereinafter the "sub processors"*).

For Global Custody Services to third party Luxembourg domiciled & regulated funds, Banks & Insurance Companies, External Asset Managers , non-domiciled regulated and un-regulated funds, and Quintet's Private Wealth Management Clients.

- asset servicing and financial intermediary: *e.g. onboarding external asset manager, asset portfolio management (lifecycle), transaction order and payment at FIM desk;*
- reporting, tax: *e.g. Fatca, CRS Tax reporting MIFIR transaction report* and AML control & report

When performing the Services, the Group 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, 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 as follows:

- 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*[3] *or anti-money laundering rules*). 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 you are a prospect and/or you introduce a client to the Group and/or are in contact with Quintet and/or are acting as a member of staff of a third-party company in a relationship with the Group.
- When you do not want us to process this information, we recommend that you refrain from providing or making available such sensitive data, e.g. by removing this type of data from any document made available to us.

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

4. What principles 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 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** *(= Quintet Management is accountable for the processing of personal data needed for their business activities and Quintet has put in place a compliance framework and record of processing activities to demonstrate compliance*.)

5. What is the lawful basis for each type of Processing activities?

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 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*).

[3] 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)

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

6. Who do we share your Personal Data with?

To achieve the purposes described above (*see* section 4), we may transfer Personal Data outside of The 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)[4] 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/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*,)
    - Central administration (administrative and transfer agent services) outsourced: European Fund Administration S.A.

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.

7. 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 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 and we transfer Personal Data to a non-EEA country or in the UK and we transfer Personal Data to an EEA or non-EEA country, we will use one of the following safeguards:

- deploy adequate contractual guarantees such as EU Standard Contractual Clauses (SCC)[5] or UK International Data Transfer Agreement (IDTA)[6] 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[7], for example with your consent, establishment, exercise or defence 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*).

[4] 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

[5] 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) 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

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

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

8. 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: 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 use these automated tools to assist in our decision making. **We do not rely on them solely to make any decisions**. Therefore, **final decisions are made by members of our banking and advisory teams**.

How do we use automated decision-making Processing?

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

- MIFID (= *Directive on markets in financial instruments and amending Directive 2002/92/EC*) profile score with a "questionnaire investor "in order to provide you suitable products and services
- AML (= **A**nti-**M**oney **L**aundering or *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 relationship to detect any fraudulent or illicit activity, in relation with financial crimes or terrorism financing.

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.

9. How do we protect your Personal Data?

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

10. 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 Client, third party and any Customer of Client (as the case may be) for a maximum period of **10 years upon termination of the business relationship[8].**

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.

11. What are your rights regarding your Personal Data?

Under the GDPR you have several important rights, although these rights have exceptions. In summary, those include rights to:

1. Access to your Personal Data. This includes obtaining a copy of the Personal Data we are processing ;
2. Rectify any inaccurate Personal Data or complete any incomplete Personal Data;

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

3. Erasure of your Personal Data (= *"Right to be forgotten")*
4. 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.
5. 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)
6. 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 on your consent (= Portability)
7. 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 Luxembourg : CNPD
- For UK : ICO
- For other countries, please check the EDPB list

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

The Group 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 affiliates	When you are a Client of Brown Shipley & Co
Group Data Protection Officer, Quintet Private Bank (Europe) S.A. 43, Boulevard Royal - L- 2955 Luxembourg Email: DPOGROUP@QUINTET.COM	**Brown Shipley Data Protection Officer,** No. 1 Spinningfields 1 Hardman Square Manchester M3 3EB Email: DPO@brownshipley.co.uk

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

13. Professional secrecy obligation of the Quintet Private Bank (Europe) S.A. (the Head Office) and related exemptions

If you have a contractual relationship with Quintet Private Bank (Europe) S.A. (the "**Head Office**"), we refer you to the general terms and conditions of the Head Office for all relevant information concerning the professional secrecy obligation of the Head Office in connection with Confidential Information (as defined below) that concerns you.

If you are a prospect and you are in contact with the Head Office, the Head Office takes the following measures:

The Head Office, including its staff (the members of the management body, the directors, the employees and the other persons who work for the Head Office) are subject to professional secrecy obligations in accordance with Luxembourg laws, pursuant to which the Head Office must maintain secrecy about your information of which it may have knowledge or that you have entrusted it with (the "**Confidential Information**").

Confidential Information will only be released by the Head Office, in circumstances where the Head Office may be so obliged (e.g. when ordered by a competent court) or authorised by Luxembourg laws or, under certain circumstances and conditions, where the Head Office has obtained your consent or instructions to that effect.

In this context, we draw your attention to the fact that, in order to improve the efficiency and quality of the operational tasks relating to the services it provides and activities it performs, Quintet may outsource, in whole or in part, business, control or operational functions (or any other relevant function as the case may be) to other Entities or to third party service providers including using cloud based and digital solutions (such as other Entities and/or third party service providers, together the "**Service Providers**").

In this context, the Service Providers may have access to and process certain Confidential Information of prospects that have been created or collected by, or communicated to (whether provided in person, by mail, email, fax, telephone or any other means) the Head Office, such as personal identification data and details (name, address, place of incorporation, identity of representatives, tax domicile, KYC documentation, etc.), as well as data relating to your business affairs (data generated by the Head Office in the context of the services provided or to be provided to you, business contacts, information on you or your beneficial owner, etc.).

In cases of Services Providers which are not regulated in Luxembourg, the description and purposes of the outsourced functions, the Confidential Information of prospects that may be transferred and/or disclosed to such Service Providers as well as the country where they are located are detailed in the table below:

Confidential Information of Prospects likely to be transmitted	**Country of establishment of the Service Provider**	**Nature of the outsourced activities**
Administrative data: Academic career, ID Number, Passport Number, Passport document, Qualifications / certifications, Tax Identification Number, Utility bills, Photographs, Criminal offences or convictions (e.g., Copy of criminal records) Financial data: Inheritance, Portfolio / Shares, Salary / wage, Transaction, Wealth / Estate Identification data: Date of Birth, First Name, Full Name, Home Address, Last Name, Nationality, Personal Email, Place of birth, Signature	Switzerland with a storage in Luxembourg	Core banking activities
First Name, Full Name, Gender, Last Name, Personal Email, Private contact details (phone number, fax, address), professional email, body of any correspondences	USA with a storage in Germany, Ireland and France	Office and correspondence (file and servers management)
Administrative data: Academic career, ID Number, Passport Number, Passport document, Qualifications / certifications, Tax Identification Number, Utility bills, Photographs, Criminal offences or convictions (e.g., Copy of criminal records) Environmental data: Information about family members, including children	United Kingdom with a storage in Luxembourg	Anti-money laundering prerequisite for onboarding Client and prospect

Financial data: Inheritance, Portfolio / Shares, Salary / wage, Transaction, Wealth / Estate Identification data: Date of Birth, First Name, Full Name, Home Address, Last Name, Nationality, Personal Email, Place of birth, Signature Professional data: Business career, CV, Occupation, Professional contact details (phone number, fax), Professional email address		
Mobile phone number	Luxembourg	Telecommunication operator
Phone recording (Mifid)	Luxembourg	Telecommunication operator
Information likely to enable the identification of the Clients, which would encompass personal identification data and details (e.g. full name, address, correspondence, email address, emails, place of incorporation, identity of representatives, beneficial owners, tax domicile, KYC documentation, date and place of birth, passport numbers, national and international tax identification numbers, account information)	Germany, Netherlands, France	Information likely to enable the identification of the Clients, which would encompass personal identification data and details (e.g. full name, address, correspondence, email address, emails, place of incorporation, identity of representatives, beneficial owners, tax domicile, KYC documentation, date and place of birth, passport numbers, national and international tax identification numbers, account information)

The Head Office has taken reasonable technical and organisational measures to ensure the security of the Confidential Information transmitted and to protect the Confidential Information against any unauthorised processing, taking into account that the level of protection for personal data, and confidential information in general, in third countries may not be the same as in Luxembourg. The Service Providers are either subject by law to a professional secrecy obligation or will be contractually bound to comply with strict confidentiality rules. Confidential Information that will be transferred in accordance with the purposes described above will only be accessible to a limited number of persons within the relevant Service Providers, on a need-to-know basis. Unless otherwise authorised by law or in order to comply with requests from or requirements of, national or foreign regulatory or law enforcement authorities, the Confidential Information will not be transferred to entities other than the Service Providers. You hereby acknowledge and accept that the Service Providers may not be subject to Luxembourg professional secrecy rules and that professional secrecy obligations applicable to them may be less stringent than Luxembourg professional secrecy legislation.

Against this background, for those recipients of the Privacy Notice who are prospects of the Head Office, we will deem that you consent, authorise and empower us to transfer the Confidential Information to Service Providers, if and where necessary, in the context of the outsourcing arrangements described in the table above if we receive no written objection from you from the provision of this Privacy Notice and its future updates.

14.How can we change this Privacy Notice?

The Group reserves the right to change, supplement and/or amend this Privacy Notice at any time. We will reach out to you to inform you of any change. Check your emails or our internet**.**

15.Appendix

15.1 Table of 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	Contact details Name, surname, gender, physical and electronic address data, phone numbers
Identity	identification information and documentation *(e.g. ID card details*), taxpayer identification number (TIN), Bank account number, Client number (LEI) and authentication Data (e.g. sample signature)
Professional	regulatory or financial situation (e.g. for due diligence purposes), PEP status, professional contact details
Sociodemographic	Such as your gender, date and place of birth and nationality
Documentary Data	Which are stored in documents or copies of them (for example your passport or ID card).
Open Data and Public Records	Such as data available in public records
Log data & other security data	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 your bank card
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[9]). 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

[9]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	Such as details about your investments, shares and securities portfolios, real estate, donations or inheritance and loans
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 personal information of a criminal nature, which will only be collected and used if permitted by applicable law (*e.g., anti-money laundering*) or • 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. • for reasons of substantial public interest e.g. carrying out fraud prevention activities or obtaining insurance cover for you (UK only).
Marketing	Such as your preference to receive newsletters (*e.g., Counterpoint*) or event invitations.
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 Quintet website data protection cookies policy for more details.

15.2 Table 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 <u>before entering into a contractual relationship or to carry out the performance of a contract</u>: • carry out an initial risk profile and needs assessment, • manage your investments, execute your instructions, • make and manage payments due to you or instructed by you, • manage fees, interest and charges on your accounts or exercise rights set out in contractual agreements.
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: • monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services.

Lawful basis	Type of Processing activities
	• perform assessments and analyse client data for the purposes of managing, improving and fixing data quality. • protect our legal rights and interests; • 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.
Legal or regulatory requirements	The Processing is necessary <u>for complying 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 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; • 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

16. Version control and metadata

Group Policy Document Metadata

Writer	Head of Group DPO
Owner	Group legal? Group GPS?
Policy document category	Policy (Level 1)
Group affiliates and population in scope	All staff of all group affiliates and locations
Annual certification process	no
Last approval date and Body	Group DPO forum
Effective date	01 December, 2022
Expected review date	01 December, 2024
Related documents	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) UK GDPR & Data Protection Act 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 UK DPO Group DPO Head Stakeholders: Asset servicing & FIM Group legal	07/10/2022 11/10/2022 26/10/2022 14/11/2022 28/11/2022	Drafting B2B English version Minor changes and updates Reviewed Minor changes and updates n/a