Quintet Privacy notice

Table of Contents

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 Quintet Privacy Notice (the "**Privacy Notice**") has been created 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 national labour laws.

This Privacy Notice (the "**Notice**") is a prior and formal information channel to let you know how we collect and process your Personal Data. when you are considering entering into a client relationship or you are already a 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.

[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.

This Notice applies whether you are a customer of ours (= *private Client*), a potential customer interested in our services (= *prospect*), a shareholder or agent of a corporate client[3] or a third party wanting to do business with us or with which we did or do business with.

Regarding professional clients in Business-to-Business relationship (such as asset servicing, third parties' administration, …) please refer to the Quintet Business to Business (BTB) notice for more details related to personal data processed.

Please note 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. What types of Personal Data might be processed?

The Entity you have a contractual relationship with, or the Entity you are discussing potential services with, is responsible for determining the **purposes** *(= what we do with your personal data*) and **means** *(= how we manage your personal data*). That means this Entity is acting as a **data controller** when collecting or using your Personal Data.

Within the Data protection framework, "**Personal Data**" means any information which allows direct or indirect identification of an individual, while "**Processing**"[4] means any operation or set of operations which is performed on personal data (*e.g., collecting, sending, using, extracting, storing, or sharing personal data*).

Those Personal Data are 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	Such as your first name and family name, address, email address, telephone numbers
Identity	Such as your ID card or passport number, your (electronic) signature
Professional	Such as your professional contact details if any
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

[3] See Quinet Business to Business Privacy Notice for more details.

[4] See art 4, GDPR: "'*processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as* ***collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction***".

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[5]). 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
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 Special data (such as Health data) or personal information of a criminal nature, which will only be collected and used if permitted by applicable law (*e.g., anti-money laundering*) or • with your explicit consent; • 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.

[5]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
Website	Such as cookies management. Please refer to Quintet website data protection cookies policy for more details.

We will collect Personal Data from you *(= direct source*), from other companies within our Group and from others (= *indirect source*) as follows:

Information directly collected from you:

- When you apply for our products or services or complete other forms or documentation.
- When you talk to us either in person or over the phone.
- When you send emails or submit forms from our website or send letters through the post.
- When you take part in any competitions, surveys, or promotions that we may run.

Information from third parties we work with:

- Independent Financial Advisors.
- Organisations that introduce you to us.
- Government, compliance and law enforcement agencies.
- Public information sources and other agencies depending on the product you applied for (*e.g., Anacredit for credit reference and fraud prevention agencies and Transunion (UK)*[6])
- Companies that you work for or hold shares in.

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[7] 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 are in contact with Quintet and/or are acting as a member of staff of a third-party company in relation to the Bank.

3. 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*;)

[6] Transunion International UK Limited (formally Callcredit). The following link provides further details about how each of the three main credit reference agencies use and share personal data they receive about you https://www.transunion.co.uk/legal/privacy-centre

[7] FATCA stands for **F**oreign **Ac**count **T**ax **C**ompliance **Ac**t, "*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)

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*.)

4. 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 suitability for investment (*e.g., MIFID questionnaire*), 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. 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*).

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: • carry out an initial risk profile and needs assessment, • provide investment advice to you, • manage your investments, execute your instructions, • make and manage payments due to you or instructed by you, • deliver other banking or real estate services and investment advice, • 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
	• manage and monitor our properties for crime prevention and prosecution of offenders, for identifying accidents and incidents and emergency situations and for internal training; • 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 for complying with our legal and regulatory obligations 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; • assess affordability and suitability of credit for initial credit applications and throughout the duration of the relationship, including analysing client credit data for regulatory reporting; • 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; • investigate and report on incidents or emergencies on the Quintet's properties and premises; • 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.

Lawful basis	Type of Processing activities
	• 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

5. 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)[8] or the United Kingdom.

a) Data transfers across the Group

In the context of Shared Service Centres (hereinafter "SSC") within the Group, we may share your data amongst Entities of the Group which might be based within or outside the EU such as our subsidiary established in UK:

- Each affiliate and subsidiary is a Group Entity: Quintet Group has implemented a matrix organization, with multiple reporting lines across the Group, which means it is necessary to share some of your Personal Data across the Group.
- The Group has centralised some support services by implementing Service Level Agreements including a Data Processing Agreement if necessary. Some services are provided by the Group, as a Processor, on behalf of other Group Entities
- To ensure compliance with legal obligations and to prevent abuse, the Group conducts internal audits and investigations at Entity level. In the context of such audits or investigations, the auditor or investigator may have access to some of your Personal Data.

b) Data transfers to third parties

We may also share your data with:

- 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, payment and card services providers and payment initiation providers, correspondent banks, transfer agents or custodians);
- third parties providing services:
    - IT/Operations services outsourced to Lombard Odier T&O Services (Europe) S.A.

[8] 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

- IT services and products including telecommunications, IT providers including providers of cloud solutions (*e.g., Microsoft 365 cloud, Pax Familia Wealth platform, Intelliflo wealth platform*)
- Advertising and marketing providers including digital and cloud-based solutions for marketing and offerings (*e.g., HubSpot, Spotler*), printing, market & behavioural analysis/research and benchmarking, consulting (e.g. *KMPG, Deloitte*)

- parties linked directly to you by contract such as a spouse with a joint account.

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.

For more details about our third parties acting as a processor, please contact DPOGROUP@QUINTET.COM/ DPO@brownshipley.co.uk.

6. 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 or 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)[9] or UK International Data Transfer Agreement (IDTA) [10] 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 [11], 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 11*).

7. 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.

As operator in banking and financial industry sector, we use profiling to:

- Manage your preferences to deliver best in class service: you might provide your consent and/or might object to such processing activity where related to direct marketing purposes (*e.g., newsletters, invitation to seminar or Events, etc…)*
- Deliver tailored products and services:

[9] 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

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

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

- we assess your suitability for products before providing portfolio management or advisory mandate. (*e.g., When we provide wealth planning services, we use internal and external profiling tools to help us ascertain your risk profile.*)
- We may also place you in groups with similar clients, known as customer segmentation. (*e.g., customer segmentation to learn about our clients' needs and guide us when designing products and services for different customer segments, and to manage our client relationships*.)

- Assess credit worthiness: system tool, credit scoring, to assess how you are likely to act while paying back any money you borrow and decide whether to lend money to you or your business.
- 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 decision - making automated tool, but we do use the results of some automated tools to get a preliminary analysis of your situation:

- Credit scoring : we assess creditworthiness and your risk rating based on statistical model, then we submit it to the approval to our internal Credit Committee
- 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 10. What are your rights regarding your Personal Data?)

How to manage cookies?

For more details, please see our Cookie Policy.

8. How do we protect your Personal Data?

Technical and Organisational Measures the priority for the Group is ensuring that Personal Data is appropriately protected from data breaches. Therefore, the Group implements adequate technical and organisational security measures, such as, depending on the equipment, password protection, encryption, physical locks...etc. to ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected:

- Any special categories of Personal Data that are processed will be stored with enhanced and specific security measures.
- Employees are permitted to access Personal Data for the sole purpose of performing their professional duties and such employees are subject to confidentiality obligations.
- Access rights to Client/Prospect Personal Data are assigned on a need-to-know basis. Generally, access to Client Personal Data is limited to Client Advisors and Client administration services.

Training and Communication: We believe that the protection of Personal Data is also the responsibility of individuals. As such, all employees of the Group and all individuals having access to Personal Data stored on the Group's IT systems are provided with training and documentation to improve their practical skills and knowledge on Data Protection issues. The relevant guidelines, procedures or policies related to the protection of Personal Data will generally be uploaded on the Group's intranet and accessible to all employees of the Group.

9. 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.

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.

10. What are your rights regarding your Personal Data?

Under the GDPR you have a number of 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;
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.

In order to exercise your rights referred to above, you can refer to the contact details in 11. Who should I contact and how do I exercise my rights?

11. 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. Depending on your location, please contact the officers, detailed below, if you have any questions or concerns about this Privacy Notice:

Group Data Protection Officer,

Quintet Private Bank (Europe) S.A.

43, Boulevard Royal - L- 2955 Luxembourg

Email: DPOGROUP@QUINTET.COM

If you are Client of Brown Shipley & Co, you can also email or write using the details below:

Brown Shipley Data Protection Officer,

No. 1 Spinningfields

1 Hardman Square

Manchester M3 3EB

Email: DPO@brownshipley.co.uk

We will respond to your requests within one month of receipt of your request, unless we need to extend this period due to the complexity and number of requests.

For us to help you with your request, we will need the following from you:

- enough information to identify you (e.g., account number, username, registration details)
- proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill)[12], and
- a clear description of the Personal Data to which your request relates, including any account or reference numbers, if you have them.

Please note

You may also lodge a complaint with the data protection authority of the EU country or UK, in which you live, of your place of work or of the place of the alleged infringement.

When you are **resident in the EEA,** please contact either the **Commission Nationale pour la Protection des données** based in Luxembourg: https://cnpd.public.lu/en.html or your local authority which you can find: https://edpb.europa.eu/about-edpb/board/members_en

When you are **resident in the United Kingdom,** please contact the **Information Commissioner's Office**: https://ico.org.uk/global/contact-us/

Your rights can also be exercised in accordance with the governing law and before the competent courts related to the country of your domicile.

12. 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,

[12] See art 12.6 , GDPR : "*where the controller has **reasonable doubts concerning the identity of the natural person** making the request referred to in Articles 15 to 21, the controller may **request the provision of additional information necessary to confirm the identity of the data subject**.*"

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, the Bank 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 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 likely to be transmitted in relation to clients	**Country of establishment of the Service Provider and/or its sub-contractors**	**Nature of the outsourced activities**
Full name, address, Id card, passport numbers, legal entity identifiers, emails, transactions, account reference and positions.	Luxembourg and Switzerland	Provision of the core banking system, performance of some operational services (maintenance of the securities master file, brokerage and custody activities, production of client advice and statement)
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)	Netherlands, Ireland and France	Cloud solutions and services including applications and functionalities in relation to email communication and exchanges, office tools, communication tools (audio conferencing, phone, chats, webinars), tools for storage of information and data

Full name, gender, personal Email, private contact details (phone number, fax, address)	Ireland, Netherlands	Support with mass mailing for marketing activities
Full name, address, Id card, passport numbers, email addresses and phone numbers.	Germany	Identity verification for clients who would like to use the service
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	Digital signature of documents

The Head Office has taken reasonable technical and organisational measures to ensure the confidentiality 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 recipient 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.

13.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**.**

14.Version control and metadata

Group Policy Document Metadata

Writer	Head of Group DPO
Owner	Group Data protection Office
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	September, 2022
Expected review date	September, 2023
Related documents	Group Privacy notices
Policy replacements	LON_LIB1-#24651977-v3-Quintet_Privacy_Notice_English
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 - 3.0	Group DPO	23/11/2020	Regulatory changes – minor changes
4.0	Group DPO Group legal UK DPO	20/07/2022 21/07/2022 19/07/2022	Regulatory updates, check with current active RPA, third party (cloud applications) Banking secrecy updates - list of outsourcers Minor changes
5.0	Outsourcing	28/10/2022	Update related to the table of section 12
6.0	Control monitoring programme	10/11/2022	Update on automated tool and profiling (section7)