QUINTET
LUXEMBOURG
PRIVATE BANK

Candidate Privacy Notice

1. What is the purpose 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 candidates Personal Data in accordance with any applicable data protection laws, regulations, and guidelines ("**Data Protection Regulations**"). This Candidate 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 2018 ("**UK GDPR"**)[2] or any national labour laws.

This Privacy Notice is provided to job applicants and prospective candidates ("**You**") as prior notice of how we collect and process your Personal Data when you are either considering applying or actively applying for a position within the Group and any of its affiliates (the **"Entity"** or **"Entities**). The terms "**we**" or "**our**" or "**us**" used in this Privacy Notice refer to the Group.

2. What types of Personal Data might be processed?

1.1. Definitions

Within 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 are performed on personal data (*e.g., collecting, storing, and transferring data*).

Personal Data collected and stored by us may include the following categories

1.2. Categories of Personal Data

Categories of Personal data	Examples of type of Personal Data
Contact details	Such as your name and family name, address, email address, telephone numbers
Identity information	Such as your ID number, social security number and tax number for preparing the contractual relationship in compliance with applicable laws
Professional and educational backgrounds	Such as your skills, qualifications, and educational courses (*e.g., degree or any certifications*) Employment history and educational history for background checks before entering into a contract
Sociodemographic	Such as your gender, date and place of birth and nationality

[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**"), tailored by the Data Protection Act 2018 explains the general data protection regime that applies to most UK businesses and organisations : a lot of processing of personal data are subject to the GDPR however some parts DPA 2018 supplements GDPR when it does not apply.

Categories of Personal data	Examples of type of Personal Data
Open data and public records	Such as data available in public records or social Network (e.g. LinkedIn)
Documentary data	Which are stored in paper/electronic documents or copies of them (*e.g., your passport or ID card*)
Work relationships	Such as your business references for background checks or any business associates and other relationships, where required by law, including for conflict-of-interest purposes or family members for emergency
Special categories of data	We do not process any special data. However, under certain circumstances, you might provide us with special personal data such as **health data**, which is only collected and used with your consent. (*e.g., disabilities*) or personal information of a criminal nature (that you may declare to us), which will only be collected and used if permitted by applicable law (*e.g. employment laws and anti-money laundering*)
CCTV recording	Such as video surveillance recording, set up for your personal safety, prevention and detection of crime and for physical security of our premises, according to local legal requirements.

Personal Data we process is information that is provided to us by you. However, in some instances, and with your consent, we may process Personal Data relating to you received from a third party (see next chapter What is the legal basis of each type of processing activities?).

3. What is the legal basis of 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 the role/types of roles you are applying for. For instance, to assess your suitability for employment, experience or certifications may be collected within the recruitment process, based on the job profile, to comply with regulatory requirements for specific regulated professions. However, your personal contact details, like email address, might also be needed to use some of our IT tools (*e.g., our onboarding module in SuccessFactors*) or to invite you to come to our office premises for a face-to-face interview.

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

Lawful ground	Type of Processing activities
Contractual agreement	The Processing is necessary for preparing the future contractual agreement and obligations with you prior to any hiring.
Legitimate interest	Processing your Personal Data is based on the legitimate interest because it is necessary to safeguard our own legitimate interests, insofar as your interests or fundamental rights and freedoms do not prevail. We will balance this processing on a case-by-case basis and will consistently monitor this; Legitimate interest covers our talent acquisition process to decide whether we want to enter into a contract of employment with you and may include; • receiving your CV and covering letter, or your application form and your test results (if applicable), to decide whether you meet the basic requirements to be longlisted / shortlisted for the role; • recording your Personal Data in our candidate database; • assessing your skills, qualifications, and suitability for the role (*i.e. various professional or personality tests*); • carrying out reference checks and any background checks, including employment and educational history, where applicable; • communicating with you about the recruitment process and (where you have expressly consented) about new opportunities / other suitable vacancies; • determining the terms and conditions of a job offer.
Legal or regulatory requirement	The Processing is necessary to comply with our legal and regulatory obligations such as: • pre-employment screening (= background checks); • obligations to ensure fair treatment, protection of candidates' rights and anti-discrimination policies; • investigate and resolve complaints concerning unfair treatment; • obligations under labour laws and regulations for regulated professions; • compliance with requests from, or requirements of, regulatory and enforcement authorities; • manage contentious regulatory matters, investigations, and litigation.
Consent	Your consent will be needed when: • The background check is carried out by a trusted third party; • We use a pre-screening tool to perform a partial profiling of your application. However, a recruiter will always have the opportunity to review these results.

Please note when you fail to provide any requested information, which is necessary for us to consider your application (such as evidence of qualifications, work history or your work permit), we will not be able to

process your application successfully. For example, if we require references for this role, and you fail to provide us with relevant details, we will not be able to take your application further.

4. Automated decision-making

You will not be subject to decisions, based solely on automated decision-making that will have a significant impact on you.

There may be instances where you will be required to fill out mandatory fields directly linked to the objective requirements of the job you are applying for (*e.g., specific qualification required to apply for certain banking positions*). You understand that your application will automatically be disregarded for the relevant role if you do not satisfy this mandatory requirement.

Within information technology innovation, we may use some Artificial Intelligence tool to support operational activities (*like Microsoft Copilot or LinkedIn)* prior to using AI system (*e.g data mining*) , we will perform a risk assessment.

5. With who do We share your personal Data?

5.1. Third parties

We may collect Personal Data about You from third party sources including:

- Previous employers, in the case of background checks,
- Head-hunters and recruitment agencies,
- Credit reference agencies, as part of backgrounds checks,
- Job boards, social media, and other publicly available sources.

We may share your personal data, depending on the position you are applying for, with:

- Personality tests providers,
- Other third-party providers generally used in the context of recruitment (*e.g., background checks with Vero Screening Ltd at Group level or Validata Group B.V. in the Netherlands*).

5.2. Within the Group

When you apply, via one of our "Careers" sites, and with your consent, we will retain your profile and we may contact you if further opportunities for which we believe you might be suitable become available. Your profile will be visible by all recruiters within the Group. Please note in Germany, applications are also seen by the local WC[3]

When we receive your application via an agency or a colleague, we register it in our applicant tracking system and notify you, so that you can access and update your data. By default, your profile is visible to 'any company recruiter worldwide'. You can change this any time.

6. What are the appropriate safeguards in force regarding your Personal Data transfers?

When we transfer Personal Data outside of your country of application, we will ensure that the adequate Data Protection Regulation safeguards are in place. This means that when we transfer your Personal Data outside of your country, we will make sure that it is protected in the same way as it is being used in your

[3] See the § 99 BetrVG

country. We will use the appropriate safeguard in line with the local law of your jurisdiction. When you are in the EEA 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)[4] or UK International Data Transfer Agreement (IDTA)[5] and supplementary measures recommended by European Data Protection Authority to ensure effective compliance; or
- process such transfer under one of the data protection frameworks derogations[6], 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.

If you want to know more about these types of transfers, you can contact Us using the contact details below (see Section 10.).

7. How do we protect your Personal Data?

Our priority is to use your personal data in a safe manner **and** to ensure that Personal Data is appropriately protected from any security incident such as data breaches. The Group implements adequate **t**echnical and **o**rganisational security **m**easures (=TOM), such as, depending on the systems used, password protection, encryption, physical locks...etc. That aims to ensure an appropriate level of security to prevent the risks represented by the Processing and the nature of the Personal Data to be protected.

Within the recruitment process, we don't collect any Special Category Personal Data. If the case arises and you voluntarily provide information to us e.g. you have special needs related to a disability, we are committed to keeping this information safe according to strict security rules.

Within the Group, our employees are only given access to Personal Data they need to perform their role and these employees are also subject to a duty of confidentiality, including employees working in the human resources department. For example, access to Personal Data related to human resources management is granted on a need-to-know basis.

8. How do we retain your Personal Data?

We will retain your Personal Data for a period required to comply with local regulation; after we have communicated to you our decision about whether to appoint you to the role.

We retain your Personal Data so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent manner, but also on the basis that further opportunities may arise in the future and we may wish to consider you for those roles. After this period, we will securely delete your Personal Data in accordance with applicable laws and regulations and we will not retain it for longer than 2 years from the creation date (= date when you applied for the role).

---

[4] 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

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

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

Regarding CCTV surveillance installed for your personal safety, prevention and detection of crime and for physical security of our premises, the retention period will not exceed maximum legal requirements (max.30 days according to affiliates local requirements).

9. What are your rights in relation to your Personal Data?

You have the right to:

- access your Personal Data and receive additional information about how it is processed.
- rectify any inaccurate Personal Data or complete any incomplete Personal Data.
- request the erasure of your Personal Data.
- object, on grounds relating to your situation, to any Processing based on the Entity's legitimate interest.
- Request the restriction of Processing of your Personal Data. This enables you to ask us to suspend the Processing of Personal Data about you, for example, if you want us to establish its accuracy or the reason for Processing it.
- Request the transfer of your Personal Data to another party.
- Withdraw your consent for Processing activities for purposes related to the recruitment exercise.

If you want to review, verify, correct or request erasure of your Personal Data, object to the Processing of your personal data, or request that we transfer a copy of your Personal Data to another party, please contact DPOGroup@quintet.com in writing for your request to be considered.

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

The Group has appointed a Data Protection Officer to manage and monitor our compliance with its data protection obligations. Depending on your work location, you can contact this officer or the UK Data Protection Officer if you have any questions or concerns about this Privacy Notice:

When you are applying to the Group	When you are applying to 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

Please note you may also lodge a complaint with the data protection authority of the EU country in which you live, or 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 of the country you are resident.

11. 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
Candidate recruitment	Yes
Annual certification process	no
Last approval date and Body	30/06/2022
Effective date	01/09/2024
Expected review date	01/09/2026
Related documents	Group HR policies
Policy replacements	GDPD 640 - HR notice for candidates
Laws, regulations, and standards	General Data Protection Regulation 2016/679 (24/04/2016 – into force on 25/05/2018) 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	WC (all)	2021-03-26	Updated English linguistic version
4.0	EWC (consultation) 	2022-05-20 2022-05-20 2022-06-01 2022-06-13 2022-06-21	NL approval DE: German reference added UK approval BE approval EWC approval
4.0	LWC	2022-06-21	Updated English linguistic version
5.0	Local UK DPO DE WC LWC BEWC NLWC	2024-03-12 2024-07-22 2024-08-23 2024-08-08 ?	Updated English linguistic version: Health personal data , UK situation, Artificial intelligence , careers website and recruitment office company