RBS Group Candidate Privacy Notice

The “bank”, “we”, “us”, “our” for the purposes of this notice means The Royal Bank of Scotland Group Plc and its subsidiaries and related companies (“RBS Group”), each of which is a data controller in its own right for the purposes of data protection law. As part of our candidate application and recruitment activities we collect, process and store personal and special categories of data which may directly or indirectly identify you (together “personal information”). We process personal information for a range of purposes relating to general recruitment activities as well as the recruitment process and this may include your application, assessment, pre-employment screening, and your worker permissions. This Candidate Privacy Notice (“Privacy Notice”) sets out:

- why we collect your personal information;
- what information is collected and;
- how it is processed within the recruitment process.

Throughout this Privacy Notice we use the term “processing” to cover all activities involving your personal information, including collecting, handling, storing, sharing, accessing, using, transferring and disposing of the information.

Please refer to section **Poland** or **India** below for specific information about how candidates personal information of is processed in Poland or India respectively.

1) Why do we collect your personal information?

We only process your personal information where we are lawfully permitted for one or more of the purposes set out below. Not all of the purposes set out below will apply to you all of the time.

a) Application: activities carried out in the course of receiving and assessing candidate applications, including reviewing general applications or applications for specific jobs and processing information to enable subscription to our job alerts. This may involve the processing of your CV, name, address, employment history, academic and professional qualifications, age, diversity data including gender, ethnicity, disability, sexual orientation, nationality and previous disciplinary matters;
b) Assessment: activities carried out in the course of assessing candidate suitability for roles at the bank, which may involve the processing of your CV, psychometric tests (such as a situational judgement test, ability or personality test), interview (face to face, telephone or video), behavioural assessments (such as a role play, group exercise or presentation), technical assessments;
c) Pre-employment screening (PES): a pre-employment screening activities carried out for the purposes of financial, credit history and insurance risk assessments; criminal records checks; county court judgements checks, adverse media checks, screening against external databases and sanctions lists to establish connections to politically exposed persons; determining penalties for tax evasion (see sections 7, 8, 9, 10 & 11 for more information on PES screening.)
d) Candidate searches: In the course of our search activities, we use personal information that we have collected concerning candidates to identify professional opportunities that we think may be of interest. We may contact potential candidates from time to time regarding such opportunities. We may also contact individuals from time to time to solicit names of, or other personal information regarding, potential candidates in connection with a search that we are conducting and for purposes of market intelligence;
e) General recruitment activities: market research activities and specific or speculative recruitment-related activities.

2) What personal information might we process and how we collect it?

Generally, we collect personal information directly from you in circumstances where you provide personal information to us by applying directly for a role at the bank, or information that we learn about you through your interactions with us, or with third parties (e.g. recruitment agencies). [5] We may also collect personal information about you from third parties, including, for example, when a referee provides information about you, when a colleague recommends that we consider you for a position or from other sources where you have made your personal information publically available for the purposes of recruitment on jobs boards, LinkedIn (or other publically available social media networks and databases). Here are some examples of the type of information we may process about you. There's a full list in the schedule at the end of this notice.

a) Your Personal Information

- Personal details such as name, address, email address and date and place of birth;
- Work history/job data; previous employers, positions, dates, etc.;
- Compensation; basic salary, benefits, bonuses, etc.;
- Education and work history including professional qualifications and skills;
- Employer feedback / references, to include regulated references where necessary;
- Nationality / visa / right to work permit information; (e.g. passport, driving licence, National Insurance numbers);
- Photographs and images from recorded assessments or from on site CCTV;
- Results of pre-employment screening checks (e.g. credit history, criminal records checks where permitted under local law);
- Assessment results e.g. psychometric assessment results, results from gamification and video or telephone assessment.

b) Your Special Categories of Information

During the process we may also inadvertently capture some special categories of personal information about you (e.g. information relating to your racial or ethnic origin, religious of philosophical beliefs, trade union membership, physical or mental health or condition, sexual orientation), where this has been provided or made publically available by you or can be inferred from your CV. We may also process certain special categories of information about you (e.g. information about a physical or mental health or condition) in order to make reasonable adjustments to enable our candidates to apply for jobs with us, to be able to take online/telephone assessments, to attend interviews/assessment centres, to prepare for starting at the bank (if successful) and to ensure that we comply with regulatory obligations placed on us with regard to our hiring. We may also process information relating to criminal convictions and offences (e.g. as part of pre-employment screening checks). We will only process special categories of information or information about criminal convictions and offences where we have obtained your explicit consent or where permitted by applicable laws (and then only when necessary for the purposes mentioned above). Where we are processing personal information based on your consent, you have the right to withdraw that consent at any time where there is no other legal basis for the processing.

3) Legal basis for the processing

The bank's entitlement to process your personal information is governed by a number of processing conditions. This means that we may rely on more than one of these conditions in order to process elements of your personal information throughout the recruitment process.

- It is in the legitimate interests of the bank to process your personal information in the administration of your application and for general recruitment purposes;

- The bank will also process your personal information where it is required by law or regulation. This processing will always be fair and lawful and will at all times comply with the principles of applicable privacy laws in the country where you have applied to be employed;
- During the course of your application it may also be necessary for the bank or its suppliers to process special categories of information about you (as per the detail in section 2(b) and Schedule 1 of this notice) where we have obtained your explicit consent or where permitted by applicable laws.

4) Who do we share your personal information with?

The bank will need to share your personal information internally (both in the country where you may work and in other countries in which we have central operations) and may require to share it with some external parties or associates of the bank. Some of these third parties and associates will be located outside the European Economic Area ("EEA"). Where we transfer your personal information outside the EEA, we will ensure that it is protected in a manner that is consistent with how your personal information will be protected by us in the EEA. This can be done in a number of ways, for instance the country that we send the information to might be approved by the European Commission; or the recipient may have signed up to a contract based on "Standard Contractual Clauses" approved by the European Commission, obliging them to protect your personal information. In other circumstances the law may permit us to otherwise transfer your personal information outside the EEA. In all cases, however, we will ensure that any transfer of your personal information is compliant with applicable data protection law. Your information will only be shared if it is necessary or required (for example in order to carry out pre-employment screening).

The recruitment process will involve:

- Assessing and progressing your application;
- Assessing your suitability (skills, strengths, behaviours for the role);
- Activities needed to complete the on-boarding and screening process should your application be successful.

To enable these processes your personal information may be shared internally, but the information shared is limited to what is required by each individual to perform their role in the recruitment process.

Your personal information may be shared internally within the bank (including with other RBS Group companies) with the following people:

- Those employees who would have managerial responsibility for you or are acting on their behalf;
- Employees in HR who have responsibility for certain HR processes (for example, recruitment, assessment, pre-employment screening);
- Employees with responsibility for investigating issues of non-compliance with laws and regulations, internal policies and contractual requirements;
- Employees in IT and system owners who manage user access;
- Audit and Investigations employees in relation to specific audits/investigations; and
- Security managers for facilities / premises.

The bank may also need to share your information with certain external third parties including:

- Companies who provide recruitment and candidate interview and assessment services to the bank;
- Suppliers who undertake background screening on behalf of the bank (credit checking agencies, criminal checking bureaus, etc.);
- Academic institutions (Universities, colleges, etc.) in validating information you've provided;

- Individuals and companies that you have previously worked for who may provide references/recommendations to the bank ;
- Other third-party suppliers (or potential suppliers), who provide services on our behalf.

5) How do we protect your information?

Our HR and Recruitment systems are protected to ensure that unauthorised or unlawful processing of personal information, accidental loss or destruction of, or damage to, personal information does not occur. This is done in accordance with the RBS Security Policy.

Where we share information with other parties located outside your country, as a minimum, the bank will require that such personal information is protected as required by the laws of the country where you work. The bank also requires its third party suppliers or recipients of personal information to guarantee the same level of protection as provided by the bank. In addition to using your personal information for the position for which you have applied, we may retain and use your personal information to consider you for other positions. We typically retain your personal information for up to two years, but retention periods may vary and will be determined by various criteria including the type of record in which your information is included, the purpose for which we are using it and our legal obligations (laws or regulation may set a minimum period for which we have to keep information). We may on exception retain your information for longer periods, particularly where we need to withhold destruction or disposal based on an order from the courts or an investigation by law enforcement agencies or our regulators. This is intended to make sure that the bank will be able to produce records as evidence, if they're needed. If you do not want to be considered for other positions or would like to have your personal information removed, you may contact us as specified under Inquiries, Complaints and Objections below. Unless required for tax or other legal purposes or in connection with employment as specified above, your personal information will be retained in accordance with our with our Managing Records Policy (which means that we may hold some information after your application to the bank is complete).

6) Your Rights

a) Access, correction and deletion

You are entitled to see the personal information the bank holds about you. You can also request changes to be made to incorrect personal information and can ask for your personal information to be deleted or blocked if you legitimately think that the bank shouldn't be processing that information or is processing it incorrectly, except where retention of that personal information is required in the context of a legal dispute, or as otherwise required by law. If access, correction or deletion is denied, the reason for doing so will be communicated to you.

b) Inquiries, objections and complaints

If you have any queries about this notice or your personal information generally, including questions about accessing your personal information or correcting it, you should contact the **RBS Recruitment Support Team** at rbs.jobs.query@rbs.co.uk in the first instance. You may also withdraw consent to the processing of your personal information or submit complaints and/or objections to the processing of your personal information by sending a request in writing to: **RBS Recruitment Support Team** at rbs.jobs.query@rbs.co.uk. Alternatively, there is information available on our internet about accessing your personal information, please search for "subject access requests".

It is your responsibility to keep your personal information up to date so that accurate application records can be maintained. You can manage all of your applicant data by accessing and updating your profile on

the banks applicant tracking system or by contacting **RBS Recruitment Support Team** at rbs.jobs.query@rbs.co.uk.

When asked to remove a record from our database, RBS Executive Search will retain minimal personal information in order to prevent future contact and where required in accordance with legal / regulatory requirements.

c) Automated processing

We do not generally make recruiting or hiring decisions based solely on automated decision-making. In the event that the bank relies solely on automated decision-making that could have a significant impact on you (e.g. automated psychometric and behavioural testing), we will provide you an opportunity to express your views and will provide any other safeguards required by law.

d) Direct Marketing

The bank will not use personal information collected about you for the purposes of recruitment to offer you any products or services for personal or family consumption ("direct marketing") or provide your personal information to third parties for their direct marketing. We will ask for your consent prior to sending you communications about future events and opportunities that are relevant to you.

e) Changes to this Privacy Notice

As this Privacy Notice is updated, the current version will be posted on this site.

7) Screening checks

As part of the Selection process, the RBS Group Plc performs a number of screening checks, where permitted by local law. These checks are only performed on candidates who have been selected for a role. Your consent will be requested before screening checks are performed.

For United Kingdom and Republic of Ireland candidates only:
The personal information we have collected from you will be shared with Cifas who will use it to prevent fraud, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct. If any of these are detected you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by us and Cifas, and your data protection rights, can be found by contacting the bank's Internal Controls Team at HRPeopleServicesUK&EMEAInternalControlsTeam@rbs.co.uk.

8) Criminal records checks

Given the nature of our business, we have legal and regulatory obligations to ensure that the people we employ can be relied upon to handle client money and information responsibly. We therefore ask questions about any prior civil or criminal proceedings you may have been subject to and may also conduct criminal record checks.

9) Credit reference agencies

We will undertake searches about you at credit reference agencies who will supply us with information, including information from the electoral register, in support of our recruitment decision. The agencies will

record details of the search but will not make them available for use by lenders to assess your ability to obtain credit. We may use scoring methods to assess this application and to verify your identity.

You have the right of access to your personal records held by credit reference agencies. We will supply their names and addresses upon request.

10) Fraud prevention agencies

To prevent or detect fraud, or assist in verifying your identity, we may now and periodically make searches of Group records and at fraud prevention agencies. Should our investigations identify fraud or the commission of any other criminal offence by you (on your part) when applying for, or during the course of your employment with us, we will record details on this on fraud prevention databases. This information may be accessed from the UK and other countries and used by law enforcement agencies and by us and other employers (and potential employers) to prevent fraud. Please contact us if you want to receive details of the relevant fraud prevention databases through which we share information.

11) Regulatory screening

In order to comply with our legal and regulatory obligations in relation to anti-money laundering and sanctions restrictions, we will screen your name against global sanctions lists. The screening will simply involve searching our internal and third party databases to ensure you are not on a sanctioned list. We are not able to employ anyone on a sanctions list. In addition, in order to comply with our legal obligations relating to anti-bribery and corruption, we will also perform searches and ask questions to assess whether there is a potential bribery or corruption risk to the role based on your personal and political associations. If there is a risk we will look to assess what additional internal controls we need to put in place to reduce that risk.

Poland: The following specifically relate to Poland:

Data controller

NatWest Markets plc Spółka Akcyjna Oddział w Polsce (KRS No. 0000235983, 1 Sierpnia 8A, Warsaw) or National Westminster Bank plc Spółka Akcyjna Oddział w Polsce (KRS No. 0000677815, 1 Sierpnia 8A, Warsaw) is the Data Controller of personal information collected during the recruitment process in Poland. This means we are responsible for deciding how we process your personal information. You can contact us by **RBS Recruitment Support Team** at rbs.jobs.query@rbs.co.uk.

Purpose and lawful basis

The following chart describes the categories of personal data we may collect or obtain from you if you are a candidate in Poland, as well as the business purpose for which we use or process it and the lawful basis for that processing:

Purpose of processing	Categories of personal data	Lawful basis for processing
Your application and recruitment for a current role with us	Information contained in your application and CV, which is permitted to be collected by an employer under art. 22 (1) § 1 of Polish Labour Code, such as your name, surname, date of birth, contact details, education,	Article 6 (1)(b) of the GDPR - processing which is necessary for the performance of the employment contract as well as to take steps prior to entering into the employment contract.

	professional qualifications and employment history.	The submission of your application and CV will be taken as a request by you to process this information in order for you to participate in the recruitment process and be considered for a role with us.
	Any other personal information included in your application and CV not covered in art. 22 (1) § 1 of Polish Labour Code.	Article 6 (1)(f) of the GDPR - processing is necessary for the purposes of the legitimate interests pursued by the Bank as a prospective or current employer. Provision of this information in your job application or CV is voluntary.
Contacting you about future opportunities	Your contact information as supplied in your application and CV for a previous role with us or provided by you on your candidate profile.	Article 6 (1)(f) of the GDPR - processing is necessary for the purposes of the legitimate interests pursued by the Bank as a prospective or current employer. Should you not wish to be contacted about these opportunities you can let us know contacting the RBS Recruitment Support Team at rbs.jobs.query@rbs.co.uk.
Processing of special category information included voluntarily in your application and CV.	Information such as ethnicity or nationality, health or disability and sexual orientation.	Please note that we do not actively ask you to provide any special category data in your CV or application. Where you decide to provide this to us on your own initiative we will take your active submission of that information to us as confirmation of your explicit consent under Art. 9 (2)(a) of the GDPR. This consent can be withdrawn at any time by contacting the NatWest Recruitment Support Team at rbs.jobs.query@rbs.co.uk.
Carrying out of criminal record checks for pre-employment screening (PES) activities.	Information related to criminal background checks.	Art 6(1)(f) and Article 10 of the GDPR - criminal background checks which are necessary for the Bank's legitimate interest to mitigate the inherent risks associated with allowing anyone unaccompanied access to RBS Group (RBS) premises, systems and/or data and permitted under amendments to the Polish Labor Code on Amending Financial Sector Legislation enacted on October 24, 2017.

Your rights

In addition to the rights set out in section **6) Your Rights** above you have the right to submit a complaint directly to the President of the Personal Data Protection Office (address: Stawki 2, 00-193 Warsaw).

India: The following specifically relate to India:

- County court judgements, credit history, penalties for tax evasion are not collected in India, but court room checks for last 2 years at the residential address are conducted.
- in addition Permanent Account Number (PAN), Aadhar Card, Universal account number (UAN), National Insurance numbers are recorded and also the previous organisation where you may have worked in past.
- In India our third party vendor will check details against the 'Credit and Reputational risk' database for India and 'Serious and Organised crime' global database, 'Regulatory authorities database' global database, 'Compliance authorities database' global check
- Military service is not checked or processed in India
- References may be obtained as part of the recruitment process in India

Schedule 1: Full list of information we may process

- Name, work and home contact details
- Date and place of birth
- Education and work history
- *Individual demographic information in compliance with legal requirements (such as marital status, national identifier, passport/visa information, nationality, citizenship, military service, disability, work permit, date and place of birth or gender)
- *Health issues requiring adaptations to working environment
- Job title, grade and job history
- Employment contract related information (including compensation, location, hours of work and so on)
- Reporting and managerial relationships
- *Leaves of absence (such as maternity leave, sickness absence)
- Photograph(s)
- Disciplinary / grievance records
- Time and attendance details
- *Bank account details for salary payment purposes
- Expenses such as travel and expenses claimed from the bank
- Personal information contained in CVs (e.g. name, address, telephone number, e-mail address, employment history, degree(s) and other qualifications, languages and other skills). These may also include, without limitation: age, nationality and race (only to the extent allowed by law), compensation details, a record of our contact history with you and comments from third parties
- Skills and qualifications
- Personal information which you have made available for the purposes of recruitment on jobs boards, LinkedIn (or other publically available social media networks) and to third parties such as recruitment agencies that we work closely with
- Training history and plans
- Results of original and ongoing employee screening, where relevant (see section 7)
- Details provided in relation to Conduct policies (such as conflicts of interest, personal account dealing, trade body membership and so on)
- *Health & safety incidents, accidents at work and associated records
- Building CCTV images

- Audio recordings of telephone interviews
- Video recordings of interviews
- Notes from face to face interviews
- Psychometric test results and associated reports
- Results from behavioural assessments (e.g. Assessment Centre exercises)
- Results from technical assessments
- References and recommendations

*These categories of information might potentially include some special categories of information. Special categories of information are not routinely collected about all applicants, but may be collected where the bank has a legal obligation to do so, or if you choose to disclose it to us during the course of your relationship with the bank.

Schedule 2: EU Data Protection Regulator Websites

France

- https://www.cnil.fr/en/home

Germany

- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: https://www.bfdi.bund.de/DE/Home/home_node.html
- Der Landesbeauftragte für den Datenschutz Baden-Württemberg: https://www.baden-wuerttemberg.datenschutz.de/
- Der Bayerische Landesbeauftragte für den Datenschutz: https://www.datenschutz-bayern.de/
- Berliner Beauftragte für Datenschutz und Informationsfreiheit: https://www.datenschutz-berlin.de/
- Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg: http://www.lda.brandenburg.de/
- Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen: https://www.datenschutz.bremen.de/
- Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: https://www.datenschutz-hamburg.de/
- Der Hessische Datenschutzbeauftragte: https://datenschutz.hessen.de/
- Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern: https://www.datenschutz-mv.de/
- Die Landesbeauftragte für den Datenschutz Niedersachsen: http://www.lfd.niedersachsen.de/startseite/
- Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz: https://www.datenschutz.rlp.de/de/startseite/
- Unabhängiges Datenschutzzentrum Saarland: https://datenschutz.saarland.de/
- Der Sächsische Datenschutzbeauftragte: https://www.saechsdsb.de/
- Landesbeauftragter für den Datenschutz Sachsen-Anhalt: https://datenschutz.sachsen-anhalt.de/nc/datenschutz-sachsen-anhalt/
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/
- Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit: https://www.tlfdi.de/tlfdi/

Greece

- http://www.dpa.gr/

Italy

- http://www.garanteprivacy.it/home_en

Luxembourg

- https://cnpd.public.lu/en.html

The Netherlands

- https://autoriteitpersoonsgegevens.nl/en

Nordics

- Norway: https://www.datatilsynet.no/
- Sweden: https://www.datainspektionen.se/in-english/
- Finland: http://oikeusministerio.fi/en/the-finnish-data-protection-board

Poland

https://uodo.gov.pl/

Spain

- https://www.agpd.es/portalwebAGPD/index-iden-idphp.php

Switzerland

- https://www.edoeb.admin.ch