Ulster Bank Ireland DAC

Privacy Notice – Long form

Contents

1. Who we are

1.1 This privacy notice (the "Privacy Notice") applies to all personal information processing activities carried out by Ulster Bank Ireland DAC.

1.2 Ulster Bank Ireland DAC is a private company limited by shares, trading as Ulster Bank, Ulster Bank Group and Banc Uladh. Ulster Bank Ireland DAC is a data controller in respect of personal information that we process in connection with our business (including the products and services that we provide). In this notice, references to "we", "us" or "our" "the bank" are references to Ulster Bank Ireland DAC.

1.3 Our principal address is Ulster Bank, Ulster Bank Head Office, Block B, Central Park, Leopardstown, Dublin 18, D18 N153 and our contact details can be located at www.ulsterbank.ie

1.4 We are a member of NatWest Group plc ("the NatWest Group" or "NWG"). More information about the NatWest Group can be found at www.natwest.com by clicking on 'About Us'.

1.5 We respect individuals' rights to privacy and to the protection of personal information. The purpose of this Privacy Notice is to explain how we collect and use personal information in connection with our business. "Personal information" means information about a living individual who can be identified from that information (either by itself or when it is combined with other information). We may update our Privacy Notice from time to time, by communicating such changes to you and publishing the updated Privacy Notice on our website www.ulsterbank.ie/privacy. We would encourage you to visit our website regularly to stay informed of the purposes for which we process your information and your rights to control how we process it.

2. The information we process

2.1 We collect and process various categories of personal information at the start of and for the duration of your relationship with us. We will limit the collection and processing of information to information necessary to achieve one or more legitimate purposes as identified in this notice. Personal information may include:

a. basic personal information, including name and address, date of birth and contact details;
b. your Personal Public Service Number (PPSN) or Tax Reference Number (TRN);
c. financial information, including account and transactional information and history;
d. information about your family, lifestyle and social circumstances (such as dependents, marital status, next of kin and contact details);
e. information about your financial circumstances, including personal wealth, assets and liabilities, proof of income and expenditure, credit and borrowing history and needs and goals;
f. education and employment information;
g. goods and services provided;

h. visual images and personal appearance (such as copies of passports or CCTV images); and

i. online profile and social media information and activity, based on your interaction with us and our websites and applications, including for example, your banking profile and login information, Internet Protocol (IP) address, smart device information, location coordinates, online and mobile banking security authentication, mobile phone network information, searches, site visits and spending patterns.

2.2 We may also process certain special categories of information for specific and limited purposes, such as detecting and preventing financial crime or to make our services accessible to customers. We will only process special categories of information, such as medical or biometric data, where we've obtained your explicit consent or are otherwise lawfully permitted to do so (and then only for the particular purposes and activities set out at Schedule A for which the information is provided). This may include:

a. information about racial or ethnic origin,

b. religious or philosophical beliefs;

c. trade union membership;

d. physical or psychological health details or medical conditions; and

e. biometric information, relating to the physical, physiological or behavioural characteristics of a person, including for example where we may use voice recognition or similar technologies to help us confirm your identity and prevent fraud and money laundering.

2.3 Where you have provided your consent for us to process your special category data, such as biometric data, you can change it any time by contacting us.

2.4 Where permitted by law, we may process information about criminal convictions or offences and alleged offences for specific and limited activities and purposes, such as to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and sharing data between banks and with law enforcement and regulatory bodies.

2.5 We can make very limited use of information that you provide to us in relation to a third party, for example an additional authorised account user. If you provide such information to us, we will:

a) contact the third party to advise them that we have received their data, the circumstances under which we have received it and the purposes for which we will use the data;

b) ask for confirmation that we may process that data;

c) provide the third party with access to our privacy notice; and

d) request that the third party ensures that their information is accurate, up-to-date and that they promptly notify us if they become aware that it is incorrect.

3. How we obtain information

3.1 Your information is made up of all the financial and personal information we collect and hold about you/your business and the proprietors, officers and beneficial owners of that business and your transactions. It includes:

a) information you give to us;

b) information that we receive from third parties (including other NWG companies, third parties who provide services to you or us, the Central Credit Register, credit reference, fraud prevention or government agencies), and other banks (where permitted by law);

c) information that we learn about you through our relationship with you and the way you operate your accounts and/or services, such as the payments made to and from your accounts;

d) information that we gather from the technology which you use to access our services (for example location data from your mobile phone, or an IP address or telephone number) and how you use it (for example pattern recognition); and

e) information that we gather through cookies or similar tracking tools (e.g. pixels) when you use our websites, internet banking, mobile banking app or web chat services. Advertising or targeting cookies or similar technologies may also be used to track your responses to particular adverts, messages or forms, which helps us to ensure we present you with the most relevant content in the future. When running email campaigns, we also track delivery and log when emails are opened and when the links within them are clicked (we do not track an individual's activity after clicking a link). These tracking logs are created by recording URLs as they are automatically downloaded to the email, for example, when images in the email are activated. We track delivery and analyse the overall open and click rates of bulk emails in order to:

   a. Identify delivery problems with Internet Service Providers.
   b. Provide evidence that regulatory messages are being opened.
   c. Ensure subject lines and email content are clear and helpful.
   d. Measure the overall performance of communication campaigns.
   e. We do not use this technology to target individuals with follow on messages or online content. By default, tracking logs are deleted after 6 months.

f) Information that we gather from publicly available sources, such as the press, the electoral register, company registers and online search engines and information that you make public on social media (e.g. Facebook, Twitter.).

4. Your rights

4.1 We want to make sure you are aware of your rights in relation to the personal information we process about you. We have described those rights and the circumstances in which they apply in the table below.

4.2 If you wish to exercise any of these rights, or if you have any queries about how we use your personal information which are not answered here, please contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.

Please note that in some cases, if you do not agree to the way we process your information, it may not be possible for us to continue to operate your account and/or provide certain products and services to you.

4.3 If you wish to contact our Data Protection Officer please contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.

Table A – Your Rights

Rights	Description
Access - You have a right to get access to the personal information we hold about you. You have a right to get access to the personal information we hold about you.	If you would like a copy of the personal information we hold about you, please follow this link https://digital.ulsterbank.ie/personal/gdpr-triage-page.html or write to: Subject Access Requests Mailroom Manager - North England 1 Hardman Boulevard, Manchester, M3 3AQ, Depot 049 or contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475 Or email us at SARCustomerQueries@ulsterbank.com For more information on how to get access to your information and the documents we need you to submit, please visit our website at www.ulsterbank.ie or contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.
Rectification – You have a right to rectification of inaccurate personal information and to update incomplete personal information.	If you believe that any of the information that we hold about you is inaccurate, you have a right to request that we restrict the processing of that information and to rectify the inaccurate personal information. Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Erasure - You have a right to request that we delete your personal information.	You may request that we delete your personal information if you believe that: - we no longer need to process your information for the purposes for which it was provided; - we have requested your permission to process your personal information and you wish to withdraw your consent; or - we are not using your information in a lawful manner. Please note that the right to erasure is subject to certain exemptions, and if you request us to delete your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Restriction – You have a right to request us to restrict the processing of your personal information.	You may request us to restrict processing your personal information if you believe that: - any of the information that we hold about you is inaccurate; - we no longer need to process your information for the purposes for which it was provided, but you require the information to establish, exercise or defend legal claims; or - we are not using your information in a lawful manner. Please note that right to restriction is subject to certain exemptions, and if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.

Portability – You have a right to data portability.	Where we have requested your permission to process your personal information or you have provided us with information for the purposes of entering into a contract with us, you have a right to receive the personal information you provided to us in a portable format (subject to certain exemptions). You may also request us to provide it directly to a third party, if technically feasible. We're not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you. If you would like to request the personal information you provided to us in a portable format, please write to or contact us at: Subject Access Requests Mailroom Manager - North England 1 Hardman Boulevard, Manchester, M3 3AQ, Depot 049 or contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475 or email us at SARCustomerQueries@ulsterbank.com For more information on how to get access to your information and the documents we need you to submit, please visit our website at www.ulsterbank.ie or contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.
Objection – You have a right to object to the processing of your personal information.	You have a right to object to us processing your personal information (and to request us to restrict processing) for the purposes described in table C (Legitimate Interests of the Bank) of Schedule A (Schedule of Purposes of Processing), unless we can demonstrate compelling and legitimate grounds for the processing, which may override your own interests or where we need to process your information to investigate and protect us or others from legal claims. Depending on the circumstances, we may need to restrict or cease processing your personal information altogether, or, where requested, delete your information. Please note that your right to object to our processing is subject to certain exemptions, and if you object to us processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Marketing – You have a right to object to direct marketing	You have a right to object at any time to processing of your personal information for direct marketing purposes, including profiling you for the purposes of direct marketing. For more information see Marketing Information – Section 9.
Withdraw consent – You have a right to withdraw your consent.	Where we rely on your permission to process your personal information, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities.

Lodge complaints – You have a right to lodge a complaint with us or with the Data Protection Commissioner	If you wish to raise a complaint in relation to how we handled your personal information, please contact us in any of the following ways: In person – Visit any of our branches and speak to one of our staff. In Writing – address your letter to Customer Care Ulster Bank PO Box 145 FREEPOST Dublin 2 Online at www.ulsterbank.ie – submit a complaint using our Online Complaint Submission form. By telephone - To help us understand what has gone wrong and how we can help, some customers find it easier to talk through their issues. To talk to a member of staff, you can call us on 1800 200162, or from abroad: 00353 1 709 2042. We hope to address your concerns through our normal complaints process, however, we may escalate your complaint to our Data Protection Officer for further investigation. You have the right to complain to the Data Protection Commissioner. You can contact; the Data Protection Commissioner, Canal House, Station Road, Portarlington, County Laois, R32 AP23, Ireland. Phone +353 (0761) 104 800; LoCall 1890 25 22 31 ; email info@dataprotection.ie. For more information, visit www.dataprotection.ie

5. Changes to the way we use your information

5.1 From time to time we may change the way we use your information. Where we believe you may not reasonably expect such a change we will notify you and will allow a period of at least 30 days for you to raise any objections before the change is made. However, please note that in some cases, if you do not agree to such changes it may not be possible for us to continue to operate your account and/or provide certain products and services to you.

6. How we use and share your information within NatWest Group

6.1 We will only use and share your information where it is necessary for us to lawfully carry out our business activities. Your information may be shared with and processed by other NWG companies. We want to ensure that you fully understand how your information may be used. We have described the purposes for which your information may be used in detail in a table in Schedule A – Schedule of Purposes of Processing.

7. Sharing with third parties

7.1 We will not share your information with anyone outside NWG except:

a) where we have your permission;

b) where required for your product or service;

c) where we are required by law and by law enforcement agencies, judicial bodies, government entities, tax authorities or regulatory bodies around the world;

d) where we are required in order to comply with the United States FATCA (Foreign Account Tax Compliance Act) and/or the CRS (Common Reporting Standard). The following information will be reported to Revenue (to comply with the above); name, address, tax identification number (TIN), date of birth, place of birth (where present in our records), the account number, the account balance or value at year end, and payments made with respect to the account during the calendar year. This data may be exchanged by Revenue with other tax authorities; further information is available on the Automatic Exchange of Information portal on the Irish Revenue website;

e) with other banks and third parties where required by law to help recover funds that have entered your account as a result of a misdirected payment by such a third party;

f) with third parties providing services to us, such as market analysis and benchmarking, correspondent banking, and agents and sub-contractors acting on our behalf, such as the companies which print our account statements

g) with third parties that we appoint to help us manage arrears resolution, loan servicing or asset management

h) with social media companies (in a secure format) or other 3rd party advertisers so they can display relevant messages to you and others about our products and services on our behalf. Third party advertisers may also use information about your previous web activity to tailor adverts which are displayed to you.

i) with other banks to help trace funds where you are a victim of suspected financial crime and you have agreed for us to do so, or where we suspect funds have entered your account as a result of a financial crime;

j) with debt collection agencies;
k) with market research companies to help us assess and improve your experiences with us;
l) with the Central Credit Register, credit reference and fraud prevention agencies;
m) with third party guarantors or other companies that provide you with benefits or services (such as insurance cover) associated with your product or service;
n) where required for a proposed or actual sale, reorganisation, transfer, financial arrangement, sub-participation, asset disposal, including, without limitation, loan portfolio sales, securitisations or other transaction relating to our business and/or assets held by our business where information may be shared with any relevant third party; where such data is shared with a third party it is done so under strict duties of confidentiality;
o) in anonymised form as part of statistics or other aggregated data shared with third parties; or
p) where permitted by law, it is necessary for our legitimate interests or those of a third party, and it is not inconsistent with the purposes listed above.

7.2 If you ask us to, we will share information with any third party that provides you with account information or payment services. If you ask a third-party provider to provide you with account information or payment services, you're allowing that third party to access information relating to your account. We're not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you.

7.3 In the event that any additional authorised users are added to your account, we may share information about the use of the account by any authorised user with all other authorised users.

7.4 NWG will not share your information with third parties for their own marketing purposes without your permission.

8. Transferring information overseas

8.1 We may transfer your information to organisations in other countries (including to other NWG companies) on the basis that anyone to whom we pass it protects it in the same way we would and in accordance with applicable laws.

8.2 In the event that we transfer information to countries outside of the European Economic Area (which includes countries in the European Union as well as Iceland, Liechtenstein and Norway), we will only do so where:

a) the European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately;
b) the transfer has been authorised by the relevant data protection authority; and/or
c) we have entered into a contract with the organisation with which we are sharing your information (on terms approved by the European Commission) to ensure you information is adequately protected. If you wish to obtain a copy of the relevant data protection clauses, please contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.

9. Marketing information

9.1 Subject to the marketing preferences you have indicated to us, we will send you relevant marketing information (including details of other products or services provided by us or other NWG companies which we believe may be of interest to you), by mail, phone, email, text and other forms of electronic communication. If you change your mind about how you would like us to contact you or you no longer wish to receive this information, you can tell us at any time by contacting your local branch or by contacting us at, Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.

10. Communications about your account

10.1 We will contact you with information relevant to the operation and maintenance of your account (including updated information about how we process your personal information) or in relation to your account opening or loan application, by a variety of means including via online banking, mobile banking, email, text message, post and/or telephone. If at any point in the future you change your contact details you should tell us promptly about those changes.

10.2 We may monitor or record calls, emails, text messages or other communications in accordance with applicable laws for the purposes outlined in Schedule A – Schedule of Purposes of Processing.

11. Central Credit Register, credit reference and fraud prevention agencies

11.1 We may access and use information from the Central Credit Register, credit reference and fraud prevention agencies when you open your account and periodically:

a) to manage and take decisions about your accounts, including assessing your creditworthiness and checks to avoid customers becoming over-indebted;
b) when you apply to have your existing loan restructured;
c) if you have arrears on your account or have exceeded the limit on your overdraft or credit card;
d) if an amendment is required to the records held on the Central Credit Register;
e) to prevent criminal activity, fraud and money laundering; and
f) trace debtors and recover debts.

11.2 We require you to provide us with certain information in order for us to undertake credit reference and fraud prevention processing. The basis for our processing of such personal data for such purposes and the consequences of not providing such personal data is set out in Schedule A.

11.3 Application decisions may be taken based solely on automated checks of information from the Central Credit Register, credit reference and fraud prevention agencies and internal NWG records. To help us make decisions on when to give you credit, we use a system called credit scoring to assess your application. To work out your credit score, we look at information you give us when you apply; information from credit reference agencies or the Central Credit Register that will show us whether you've kept up to date with payments on any credit accounts (that could be any mortgages, loans, credit cards or overdrafts), or if you've had any court

action such as judgments or bankruptcy; your history with us such as maximum level of borrowing; and affordability, by looking at your available net income and existing debts. You have rights in relation to automated decision making, including a right to appeal if your application is refused.

11.4 We will continue to share information with the Central Credit Register and credit reference agencies about how you manage your account including your account balance, payments into your account, the term of the loan, the regularity of payments being made, credit limits and any arrears or default in making payments, while you have a relationship with us. This information will be made available to other organisations (including fraud prevention agencies and other financial institutions) so that they can take decisions about you.

11.5 If false or inaccurate information is provided and/or fraud is identified or suspected, details will be passed to fraud prevention agencies. Law enforcement agencies and other organisations may access and use this information.

11.6 If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services and financing you have requested, or we may stop providing existing services to you.

11.7 A record of any fraud or money laundering risk may be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you.

11.8 When the Central Credit Register, credit reference and fraud prevention agencies process your information, they do so on the basis that they have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect their business and to comply with laws that apply to them.

11.9 If you would like a copy of your information held by the Central Credit Register, credit reference and fraud prevention agencies we use, or if you want further details of how your information will be used by the Central Credit Register and credit reference agencies please visit their websites or contact them using the details below. You can request your own credit report at any time from the Central Credit Register free of charge (subject to fair usage).

	Contact details
The Central Credit Register	**Web Address:** www.centralcreditregister.ie **Email:** consumerinfo@centralcreditregister.ie **Phone:** +353 (0)1 224 5500

12. How long we keep your information

12.1 By providing you with products or services, we create records that contain your information, such as customer account records, activity records, tax records and lending and credit account records. Records can be held on a variety of media (physical or electronic) and formats.

12.2 We manage our records to help us to serve our customers well (for example for operational reasons, such as dealing with any queries relating to your account) and to comply with legal

and regulatory requirements. Records help us demonstrate that we are meeting our responsibilities and to keep as evidence of our business activities.

12.3 Retention periods for records are determined based on the type of record, the nature of the activity, product or service, the country in which the relevant NWG company is located and the applicable local legal or regulatory requirements. We (and other NWG companies) normally keep customer account records for up to seven years after your relationship with the us ends, whilst other records are retained for shorter periods, for example ninety days for CCTV records. Retention periods may be changed from time to time based on business or legal and regulatory requirements.

12.4 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 we will be able to produce records as evidence, if they're needed.

12.5 If you would like more information about how long we keep your information, please contact us at Republic of Ireland 1800 283062 – Opening hours are Mon to Sun 08.00 – 22.00, from abroad 00353 1 804 7475.

13. Security

13.1 We are committed to ensuring that your information is secure with us and with the third parties who act on our behalf. For more information about the steps we are taking to protect your information please visit www.ulsterbank.com/roi/personal/safe-secure.ashx

Schedule A - Schedule of Purposes of Processing

We will only use and share your information where it is necessary for us to carry out our lawful business activities. Your information may be shared with and processed by other NWG companies. We want to ensure that you fully understand how your information may be used. We have described the purposes for which your information may be used in detail in a table below:

A. Contractual necessity
We may process your information where it is necessary to enter into a contract with you for the provision of our products or services or to perform our obligations under that contract. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you. This may include processing to: a) assess and process applications for products or services; b) provide and administer those products and services throughout your relationship with us, including opening, setting up or closing your accounts or products, collecting and issuing all necessary documentation, executing your instructions, processing transactions, including transferring money between accounts, making payments to third parties, resolving any queries or discrepancies and administering any changes. Calls to our service centre and communications to our mobile and online helplines may be recorded and monitored for these purposes. c) manage and maintain our relationships with you and for ongoing customer service. This may involve sharing your information with other NWG companies to improve the availability of our services, for example enabling customers to visit branches of other NWG companies; d) administer any credit facilities or debts, including agreeing repayment options; and e) communicate with you about your account(s) or the products and services you receive from us.

B. Legal obligation

When you apply for a product or service (and throughout your relationship with us), we are required by law to collect and process certain personal information about you. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you. This may include processing to:

a) confirm your identity, including using biometric information and voice-recognition technology and other identification procedures, for example fingerprint verification where we have your consent;
b) validate your Personal Public Service Number (PPSN) and Individual Tax Reference Number (TRN);
c) perform checks and monitor transactions and location data for the purpose of preventing and detecting crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. This may require us to process information about criminal convictions and offences, to investigate and gather intelligence on suspected financial crimes, fraud and threats and to share data with law enforcement and regulatory bodies;
d) share data with the Central Credit Register to comply with legal obligations under the Credit Reporting Act 2013;
e) assess affordability and suitability of credit for initial credit applications and throughout the duration of the relationship, including analysing customer credit data for regulatory reporting;
f) share data with other banks and third parties to help recover funds that have entered your account as a result of a misdirected payment by such a third party;
g) share data with police, law enforcement, tax authorities or other government and fraud prevention agencies where we have a legal obligation, including reporting suspicious activity and complying with production and court orders;
h) deliver mandatory communications to customers or communicating updates to product and service terms and conditions;
i) investigate and resolve complaints;
j) investigate and remediate errors occurring on your account or service;
k) conduct investigations into breaches of conduct and corporate policies by our employees;
l) manage contentious regulatory matters, investigations, appeals and litigation;
m) perform assessments and analyse customer data for the purposes of managing, improving and fixing data quality;
n) provide assurance that we have effective processes to identify, manage, monitor and report the risks it is or might be exposed to;
o) investigate and report on incidents or emergencies on the bank's properties and premises; and
p) coordinate responses to business disrupting incidents and to ensure facilities, systems and people are available to continue providing services.

C. Legitimate interests of the bank

We may process your information where it is in our legitimate interests do so as an organisation and without prejudicing your interests or fundamental rights and freedoms.

a) We may process your information in the day to day running of our business, to manage our business and financial affairs and to protect our customers, employees and property. It is in our interests to ensure that our processes and systems operate effectively and that we can continue operating as a business. This may include processing your information to:

(i) monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services;

(ii) ensure business continuity and disaster recovery and responding to information technology and business incidents and emergencies;

(iii) ensure network and information security, including monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our telecommunications systems and websites, prevention or detection of crime and protection of your personal data;

(iv) provide assurance on the bank's material risks and reporting to internal management and supervisory authorities on whether the bank is managing them effectively;

(v) perform general, financial and regulatory accounting and reporting;

(vi) protect our legal rights and interests;

(vii) manage and monitor our properties and branches (for example through CCTV) for the purpose of crime prevention and prosecution of offenders, for identifying accidents and incidents and emergency situations and for internal training; and

(viii) enable a proposed or actual sale, reorganisation, transfer, financial arrangement, sub participation, asset disposal, asset management including, without limitation loan portfolio sales, securitisations or other transaction relating to our business and/or assets held by our business where information may be shared with any relevant third party;

b) It is in our interest as a business to ensure that we provide you with the most appropriate products and services and that we continually develop and improve as an organisation. This may require processing your information to enable us to:

(i) identify new business opportunities and to develop enquiries and leads into applications or proposals for new business and to develop our relationship with you;

(ii) send you relevant marketing information (including details of other products or services provided by us or other NWG companies which we believe may be of interest to you). We may show or send you marketing material online (on our own and other websites including social media platforms), in our app, or by email, text or post. We may show or send you marketing material online (on our own and other websites including social media platforms), in our app, or by email, text or post.

(iii) understand our customers' actions, behaviour, preferences, expectations, feedback and financial history in order to improve our products and services, develop new products and services, and to improve the relevance of offers of products and services by NWG;

(iv) research your experiences with us and to monitor the performance and effectiveness of products and services;

(v) assess the quality of our customer services and to provide staff training. Calls to our service centres and communications to our mobile and online helplines may be recorded and monitored for these purposes;

(vi) perform analysis on customer complaints for the purposes of preventing errors and process failures and rectifying negative impacts on customers;

(vii) investigate and compensate customers for loss, inconvenience or distress as a result of services, process or regulatory failures, which may include engaging trace agents for the purposes of locating customers;

(viii) identify our customers' use of third-party products and services in order to facilitate the uses of customer information detailed above; and

(ix) combine your information with third party data, such as economic data in order to understand customers' needs better and improve our services.

We may perform data analysis, data matching and profiling to support decision making with regards to the activities mentioned above. It may also involve sharing information with third parties who provide a service to us.

c) It is in our interest as a business to manage our risk and to determine what products and services we can offer and the terms of those products and services. It is also in our interest to protect our business by preventing financial crime. This may include processing your information to:

(i) carry out financial, credit and insurance risk assessments;

(ii) manage and take decisions about your accounts;

(iii) carry out checks (in addition to statutory requirements) on customers and potential customers, business partners and associated persons, including performing adverse media checks, screening against external databases and sanctions lists and establishing connections to politically exposed persons;

(iv) share data with the Central Credit Register, credit reference, fraud prevention agencies and law enforcement agencies;

(v) trace debtors and recovering outstanding debt;

(vi) for risk reporting and risk management.

Application decisions may be taken based on solely automated checks of information from the Central Credit Register, credit reference agencies and internal NWG records. For more information on how we access and use information from the Central Credit Register, credit reference and fraud prevention agencies see Section 11 Central Credit Register, credit reference and fraud prevention agencies within this document.