

unlimit

Unlimit UK Ltd Privacy Notice

Version 1.3

Contents

1. Introduction.	3
2. Scope and General Provisions	4
3. Lawful grounds for the processing of personal data	4
4. Collection and Use of Personal Data	5
5. Retention period	9
6. Who receives your personal data?.....	10
7. Automated decision-making and profiling.....	12
8. Website and Automatic collection— Cookies and IP addresses.....	12
9. Information on Data Security	12
10. Your Rights	13
11. Data Protection Officer Contact details	14
12. Right to file a complaint	14
13. Your Responsibilities	14
14. Changes to our Privacy Notice	14

1. Introduction

Unlimit UK Ltd (“Company” or “we” or “us”) provides payment services (e-money services), acquiring and payment initiation services and other alternative payment methods for customers and merchants through our platforms and applications (“services”).

The Company and its affiliates or businesses are part of a global payments and technology organisation holding various licenses and authorisations as each business is obliged to under the laws and regulations it operates in.

The Company is dedicated to protecting the privacy and confidentiality of information in its possession and is committed to the appropriate use and protection of personal data, with transparency and respect for rights in line with United Kingdom General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by S.3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified from time to time; the UK Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (as amended) and any amending or replacing United Kingdom legislation adopted with regard to the protection of Personal Data (“data protection law”).

This Privacy Notice aims to provide information on how the Company collects and processes your personal data when you correspond, apply or establish relations with us as a customer, partner or merchant, or related services and use our website.

This Privacy Notice outlines our current policies and commitment to data protection and privacy. In line with this, we aim to collect and process only personal data strictly necessary in the context of our relationship with (prospective) customers, (future) partners, users/visitors of our website (s) (collectively referred to as “customers” or “you”) and online resources, to provide services and information for specific and legitimate purposes.

In this Notice:

- “Personal data” refers to information that identifies you or may identify you (e.g., depending on who you are, a merchant, cardholder, supplier or business partner) and how you interact with us, we may process different types of personal data.
- “Processing” of personal data refers to actions such as collecting, gathering, handling, storing, transmitting and combining personal data.
- A “data subject” is a person that can be identified or identifiable from the personal data that is processed by a controller or processor.

When you visit our website, we act as controllers of your personal data. When our services are used, we act as a provider of payment services and payment methods to merchants/providers of services and goods. In this circumstance, we act as a processor of personal data for these businesses, who are the controllers of your personal data and its processing. For example, when the Company performs card or online payment processing on behalf of the merchant in the capacity of processor, we process personal data received from merchants, such as transaction details and personal details in the context of transactions processing (e.g., payment instrument and transaction details, identification details, contact details, email/telephone numbers), so that we can complete payments from you to the merchant. Please read the privacy documentation of the merchant or service provider in this case.

We make our Privacy Notice available on our website’s homepage, www.unlimit.com, in its most recent version.

2. Scope and General Provisions

- 2.1. You should read this Privacy Notice together with the relevant Terms and Conditions of the service/product (as applicable) provided by the Company and also applies to the use of our website and online systems under the relevant Terms.
- 2.2. This Privacy Notice applies to personal data held by the Company and as described in this Privacy Notice. It contains information on the following:
 - The personal data we collect;
 - How we use personal data;
 - Who we share personal data with; and
 - Your rights.
- 2.3. This Notice is addressed to data subjects such as:
 - Directors, signatories, representatives, shareholders, beneficial owners, secretaries, officers, employees of legal entities or individuals who are current or potential/applicant or former customers;
 - Representatives of a legal entity/customer that have applied to the Company for a service/product offered by the Company, users of the Company service/product, website or online system.
 - Are end users that use our payment initiation service through which they can initiate payments from their bank accounts.
- 2.4. Some links on the Company websites may contain links or lead/originate to/from non-the Company websites or areas with their own data protection policies, which may differ from our Privacy Notice. Please ensure that the relevant policies of other entities are acceptable to you before using other sites or web pages. The Company does not accept any responsibility or liability for third-party websites. Additionally, if you are not a data subject to whom this Notice is addressed, please refer to the privacy policy of your personal data's relevant data controller (entity) to learn more about how the entity processes it. The Company may be involved in your data processing as the processor, as in the cases referred to in this Privacy Notice.

3. Lawful grounds for the processing of personal data

The establishment and legality of contractual relations and provision of services between the Company and its customers depend on the provision of the information requested by the Company, including the personal data of data subjects. It is an obligation to provide personal data to us:

- 3.1. Under our legal obligations deriving from AML legislation and other legal acts:** These require us to identify you, verify your identity and perform due diligence and enhanced due diligence if applicable on your person, as well as to fulfil our legal obligations under laws such as fraud prevention and other applicable laws.
- 3.2. For contractual purposes:** Establishment of business relations for the provision of services, execution of transactions and the performance of contractual obligations between both parties (the Company and its customers) requires the provision of certain personal data.
- 3.3. Our legitimate interests:** such as implementing online and physical security measures to properly provide our services, ensuring data and physical and logical security, access control management, and communicating with you to provide the best quality service.

Personal data is requested before establishing and during the contractual relationship. You are required to provide us with the requested data so we can enter into a contract or execute an order with you. Otherwise, we may no longer be able to continue with a contractual relationship or our services to you, and we may have to terminate the business relationship.

4. Collection and Use of Personal Data

4.1. How we collect personal data

Personal Data shared by you

We collect personal data provided or shared by you (or the customer) during account opening and the business relationship via the application forms, email or forms available on our website or other means of communication. In some cases, you may have previously provided your personal data to the Company (e.g., in the context of an existing or former customer relationship).

Personal Data we collect when you use our services

This data may include:

- Personal data relating to payment and transactions data (this may also include incidental sensitive personal data collection due to the nature of the transaction).
- Profile and usage data (such as when you connect to Internet banking and SMS services) may include personal data on how you use the services. We may collect data from devices you use to connect to the services, such as computers and mobile phones, such as your IP address and use cookies (please refer to the [Cookie Notice](#) available on our website).
- Personal data relating to providing e-money payment services, including data associated with IBAN (e-money accounts) and executing payment transactions. We also offer card issuing (linked to IBAN e-money accounts), also known as card accounts or accounts.
- Personal data relating to providing acquiring services, such as (i) card transaction acquiring (under card associations and brands) for merchants, (ii) acquiring of credit transfers resulting from payment initiation service services (PIS) for merchants (known as PIS channels) and (iii) payment initiation services for PIS customers (PIS PSUs).

If you want to learn more about our services, please refer to our [website](#).

Our primary means of collecting personal data is through personal data you share and when we provide our services. However, we may collect third-party or public data described below.

Third-party data

We may lawfully collect your personal data from other entities such as service providers, public authorities, persons that refer you to us with your permission where required, our group companies, and companies processing payments.

Public Data

We may collect your personal data from publicly available databases and publicly accessible sources (e.g., Companies House, commercial registries, screening databases (e.g., sanctions/AML), media, and the Internet).

4.2. What types of personal data do we process?

Various types of personal data are collected and processed in the context of the relationship between you and the Company and according to the service/product used and your capacity. The Company may process the following categories and types of personal data:

Individual personal information	E.g., name, previous names, date and place of birth, language, if you hold a prominent public functional role (such as politically exposed persons), residence permit.
Individual personal contact details	E.g., work address, home address, business email address, business telephone number or other contact details you provide to us.
Identity information	E.g., passport, national ID card, nationality, utility bill, tax residence and tax ID.
Financial information	E.g., income, assets, financial status, source of wealth, personal bank details, professional status, employment field, employer details (including, for example, information such as certificates of directors/shareholders), level of education, property ownership, personal investments and income, loans, copy of payslips, tax returns, credit reference information.
Authentication data	E.g., signature specimens, user logins, facial recognition data for KYC onboarding (a special category of personal data).
Communication data	E.g., personal data that you may provide by filling in forms or by communicating with us (e.g., directed to us in letters, emails, via our electronic channels).
Transactional and other/ documents information	E.g., data arising for the execution of payment transactions (including data such as date, time, amount, currencies, beneficiary details, location information and details of merchant/ATM associated with the transaction), supplementary/supporting documentary evidence related to transactions, details arising from contractual obligations between the Company and customers.
Location and technical information	E.g., location data (for example, at the time of login or a transaction), technical information from/on devices and technology you use, IP addresses and device information, visitor's information and similar information collected automatically.
Publicly available Data	E.g., details about you from public records, media and information available in databases, on the Internet.
Documentary Data	E.g., details about you stored in documents in different formats or copies of them.
Investigations data/results of due diligence and enhanced due diligence	E.g., due diligence checks, sanctions and AML/ABAC checks, and supporting information and documentation to identify and manage fraud, money laundering and bribery. We may also collect results from authorised background screening/checks providers regarding criminal convictions and offences as part of our compliance measures with regulatory obligations.
Media	E.g., closed-circuit television (CCTV) at our offices (which may collect photos or videos of you).
Consents	E.g., any permissions or consent given to us.

4.3. Purposes for which we use your personal data

We process your personal data for the following purposes:

- Verify your identity (e.g., authentication, AML purposes and fraud prevention purposes);
- To provide the services requested (e.g., conduct customer acceptance procedures to enter into a business relationship, opening an account, opening IBAN accounts, card issuing (link to card accounts) and issuing payment instruments);

- To provide acquiring services which include card acquiring (under card associations and brands) and the acquiring of credit transfers resulting from payment initiation services (PIS) channels for merchants;
- To provide payment initiation services for customers (PIS PSUs);
- To provide delivery channels (e.g., online systems);
- To execute transactions;
- To execute requests, act upon instructions;
- To perform our contractual obligations;
- To perform anti-money laundering checks and evaluations;
- For crime prevention purposes or cooperation with authorities;
- For data analytics to improve research, statistics, products and services that the Company and other third party providers (such as for AML/KYC providers);
- To maintain communication with you and provide you with up-to-date information;
- To provide ongoing support and handle inquiries, complaints and similar issues;
- To provide information about the requested/provided products and services;
- To provide information on products/services (this may be advertising/marketing);
- To enforce internal procedures and protective measures against fraud, risk and financial crime;
- To report to relevant authorities (e.g., the Financial Intelligence Institute — FIU);
- For internal operational support and administrative purposes (e.g., product development, audit, risk management);
- To obtain reports/tickets about an online problem (e.g., with our website or online services);
- For general administrative functions (e.g., maintenance of our internal records necessary for keeping up-to-date information in our systems and general record-keeping);
- To comply with our legal obligations and regulatory framework;
- To enforce or defend the rights of the Company or the Company group/affiliates;
- To ensure security and business continuity;
- For service quality management and product improvement.

4.4. Legal basis — Lawful reasons for processing:

We rely on one of the legal basis' below when processing your personal data. We may process your personal data for more than one legal basis depending on the specific purpose for which we are using your data.

a. Conclusion and performance of a contract

When we need to conclude an application process, service contract (or both) with you, or perform our obligations under a contract to provide services to businesses or customers, we rely on the performance of a contract as the legal basis.

b. Legal obligation or for public interest

We may rely on legal obligation basis when we process your data to comply with various legal obligations, legal and regulatory requirements. For example, this includes laws, regulations, and directives relating to providing payment services, verification controls of identity, money laundering and fraud prevention, compliance with our record reporting obligations, tax obligations, and risk control measures, as well as providing information to competent authority, public body or law enforcement agency.

c. Legitimate interests

Where necessary, we may process personal data where there is a legitimate interest for us or a third party in pursuing commercial and business interests, except where your interests override such interests, fundamental rights and freedoms.

d. Your consent

We will rely on consent as a legal basis and process your personal data only if you provide explicit consent. You may withdraw your consent at any time. The withdrawal of your consent will not affect the legality of the data processed before the withdrawal.

You can view the table below if you want to know more about the purposes and related lawful basis:

Purpose (what we use your information for)	Lawful reason	Our Legitimate Interests
Acceptance processes to establish relationship: To review customer's application	Performance of contract (to establish a contractual relationship) Legal Obligation Legitimate Interests	Compliance with applicable regulations governing the provision of Company's services Record Keeping Legal obligations during the review of an application
AML/TF, fraud prevention activities: - To identify, examine, prosecute and prevent crime or fraud - To verify customer and identify his (continued) eligibility for the requested services and ability for management of the account - To manage risk internally for the Company and externally for the customers - To comply with applicable laws and regulations - To provide information to authorities upon request - To respond and solve complaints	Legal Duty Public Interest Performance of contract Legitimate Interest	To establish and implement an internal fraud and crime identification and reporting mechanism Compliance with applicable regulations governing the provision of Company's services Cooperation with authorities at a national and international level To fulfill our legal and contractual obligations
Conducting of business relationship: - To deliver the requested products and services - To execute and manage customer's payment orders and to perform our obligations arising from customer's transaction - To apply on the customer's account any fees and charges - To collect any due funds - To communicate with the customer and provide information	Performance of contract Legal Obligation Legitimate Interest	Fulfilment of our legal and contractual duties Compliance with applicable regulations governing the provision of Company's services Company's interest in providing the requested services at a satisfactory and anticipated level Record Keeping maintenance

Purpose (what we use your information for)	Lawful reason	Our Legitimate Interests
- To provide information in relation to the (requested) products and services available - To communicate with customers and provide support to meet customer's needs - To manage relations of the Company with counterparties, partners, and service providers	Performance of contract Legal Obligation Legitimate interests	To ensure products and services are suitable for customers To develop and improve products and services and to define applicable charges To identify the target market To fulfill our legal and contractual obligations
- To improve services and products - To manage our cooperation with other service providers - To analyze customers, and efficiency of operation of products and services - To launch and test new products - To develop new products and expand its business - For Marketing activities	Performance of contract Legal Obligation Legitimate Interest	To develop and improve products and services and to define applicable charges To fulfill legal and contractual obligations
To manage the Company's operations, financial and business ability, communication channels and organizational planning	Legal Obligation Legitimate interests	Compliance with applicable regulations governing the provision of Company's services To fulfill its legal and contractual obligations
For proper execution and performance of the agreement between the customer and the Company: - To exercise rights set out in agreements - To inform the customer in relation to any changes to the Terms and Conditions of the services provided	Legal Obligation Performance of contract Legitimate interests	Compliance with applicable regulations governing the provision of Company's services To fulfill its legal and contractual obligations

5. Retention period

- 5.1. Our retention period is primarily determined by our obligations under applicable legislation to retain data for a specific time. Destruction will only be possible after the lapse of this period.
- 5.2. We are obliged to keep customer data (including personal data) during the business relationship and for a minimum period of 5 years after business relationship termination, or after customer application rejection/withdrawal, under AML legislation and other requirements applicable to our business.
- 5.3. We may retain your personal data for longer than the minimum retention period above if there are other lawful reasons justifying an extended retention period (such as for complaints handling, legal proceedings, investigations, regulatory, tax, money laundering and crime and fraud prevention purposes).

6. Who receives your personal data?

6.1. Internal

We receive your personal data in the context of the Company's operations. The Company's functions or departments receive specific categories and types of personal data depending on their organisational roles and responsibilities.

6.2. External

The following types of external parties may receive your personal data:

6.2.1. Service providers, auditors and consultants

We will disclose personal data to third-party partners and service providers (processors) so they can process it on our behalf where required. These service providers are required to provide sufficient assurances under data protection law. (e.g., being bound contractually to confidentiality and data protection obligations). We will only share personal data necessary for them to provide their services.

In addition, as a heavily regulated organisation, we may disclose personal data for purposes and in the context of audits (e.g., external audits, security audits, compliance audits) to legal and other advisors or to investigate security issues, risks, and complaints.

As such, personal data may be transferred and disclosed to:

- Money laundering and fraud prevention aggregation/agencies, compliance/verification services and risk prevention services. This is required to verify your identity, ensure protection against fraud, and confirm eligibility for our services/products;
- Banks (other credit and financial service institutions) and similar institutions. These enable us to provide our services, including correspondent and intermediary banks;
- Payment systems (SWIFT, SEPA, Visa, MasterCard), payment service providers and card processing companies since these enable us to provide our services;
- Card manufacturing/personalisation and delivery companies for us to create a personalised payment card and deliver it to the requested address;
- Data management, storage, archiving, and cloud storage service providers;
- Companies assisting us with the provision of our services (e.g., technological services, solutions, support such as support/maintenance/development of IT applications, technology, website management, telephony/SMS services);
- Customer support service providers and marketing service providers;
- Administrative service providers;
- Auditing and accounting services and consultants;
- External legal advisors;

6.2.2. Entities which are affiliated/related to us provided that they are subject to being bound to equivalent data protection obligations as us. We may disclose your personal data to those companies to:

- provide support services and technical services to these internal third parties and receive some of these services from them;
- contribute to the research, data analytics and studies to improve the products and services that the Company and other internal third parties provide.

6.2.3. Regulatory authorities, law enforcement, courts

We may disclose personal data to comply with applicable legislation and regulatory obligations, to respond to requests of regulatory authorities, government and law enforcement agencies, courts and court orders in the United Kingdom, such as:

- Supervisory Authorities, including the Financial Conduct Authority (“FCA”);
 - FIU and the Police;
 - Tax Authorities;
 - Information Exchange Mechanisms;
 - Other regulators, authorities and public bodies, wherever obligations exist.
- 6.2.4. Other recipients may be any person/legal entity/organisation for which you ask your personal data to be transferred (e.g., for reference purposes) or give your consent to transfer personal data.
- 6.2.5. We may also disclose your data in circumstances such as the following:
- If we are under a duty to disclose or share your personal data to comply with any legal or regulatory obligation or request;
 - To apply or enforce the Terms and Conditions or any other agreement in place in the context of our relationship and to investigate potential breaches;
 - To protect the Company’s rights, safety or property, or that of our customers or third parties/the public. This includes exchanging information with other companies and organisations for money laundering, fraud prevention and equivalent risks;
 - If the Company or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.
- 6.2.6. We may also disclose your data in circumstances such as the following:
- If we are under a duty to disclose or share your personal data to comply with any legal or regulatory obligation or request;
 - To apply or enforce the Terms and Conditions or any other agreement in place in the context of our relationship and to investigate potential breaches;
 - To protect the Company’s rights, safety or property, or that of our customers or third parties/the public. This includes exchanging information with other companies and organisations for anti-money laundering, fraud prevention and equivalent risks;
 - Organisations or companies that we plan to merge with or entities that we may be acquired by, in which situation we will require that the new combined entity or the acquiring entity follow this Privacy Notice concerning your personal data.

6.2.7. Transfers outside the UK, EEA or to international organisations

The Company and its businesses consist of several local affiliates in different markets worldwide. Your personal data may be processed locally in the country where you work or reside (the United Kingdom) or in any other country where we or our approved third-party service providers operate as permitted by law.

Should your personal data move outside the United Kingdom, we use either adequacy decisions as amended from time to time, including the provisional UK adequacy arrangements covered by European Commission adequacy decisions valid as of 31 December 2020, or by the Secretary of State as approved by Parliament or shall have appropriate safeguards with the level of data protection in the United Kingdom or as afforded in the country of origin.

We may also use the standard contractual clauses for restricted transfers or other locally compliant mechanisms (such as local transfer agreements or consent) to ensure that an adequate or equivalent level of protection applies to your personal data as the one in the country of origin.

Such transfers take place, for example:

- When necessary to carry out and in the context of transactions (e.g., card transactions, payment orders to third countries, through a correspondent bank in a third country);

- Under applicable law (e.g., tax legislation);
- Based on your explicit instructions or consent;
- In the context of data processing undertaken by third parties on our behalf (e.g., the data may also be processed by staff outside of the United Kingdom who work for the Company or one of our third-party service providers or our Group. Such staff may be performing technical duties and support, duties related to processing your requests, or providing support services).

7. Automated decision-making and profiling

Automated decision-making means the process of making decisions through automated means of processing personal data without human intervention. We do not generally use automated decision-making in establishing and carrying out a business relationship.

We may process specific data automatically by using systems to make automated suggestions or decisions, including profiling, based on information we have or collect from other authorised sources to help us react quickly and efficiently, aiming to protect our customers.

Automated decisions we may make include anti-money laundering and anti-fraud measures. We may use your personal data to help us decide if an account/payment instrument is potentially being used for fraud, money laundering/terrorist financing or sanctions contraventions. Such assessments are carried out to help us detect if an account/payment instrument is being used in ways fraudsters work or in a way unusual for you or our customer's business. If we determine a risk of fraud, unauthorised use, or unusual activity, then in such a case, we may stop activity on the account/block the payment instrument, or refuse access to them.

8. Website and Automatic collection — Cookies and IP addresses

The Company's website contains forms which website visitors may use. When website visitors send us information online via forms on the website, in the context of the provision of services, we will use the information as set out in this Privacy Notice.

In some instances, the Company and other entities (such as service providers) may use cookies and other technologies to automatically collect certain types of data when you visit our websites and online platforms. The collection of this data enables us to improve the security and usability of our websites and online resources and to measure the effectiveness of marketing activities.

For detailed information on cookies and their purposes, please refer to our [Cookie Notice](#) on our website.

An IP address is a number assigned to your computer when you access the Internet, which allows computers and servers to recognise and communicate with one another. IP addresses of website visitors may be recorded for IT security and diagnostic purposes. This information may also be used in the aggregate for website trends and performance analysis. IP addresses may also be used for the purposes and in ways set out in this Privacy Notice, including fraud prevention.

9. Information on Data Security

We have taken adequate safeguards to ensure the confidentiality and security of your personal data. We have implemented appropriate technical, physical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, damage, alteration, unau-

thorised disclosure or access, as well as all other forms of unlawful processing (including, but not limited to, unnecessary collection) or further processing.

Where the Company processes card data, we adhere to the highest level of protection available by the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is a global standard for securely accepting and processing credit card payments. Launched in 2006 by an alliance of major credit card companies, PCI DSS encompasses 12 key requirements as well as more than 400 sub-requirements and test procedures which are audited for compliance annually by an external auditor. Being PCI-compliant requires not just meeting these requirements but continually identifying, documenting, and (if necessary) remediating business-level systems and processes that involve the handing of user credit card data.

Where you have access to our resources via user authentication means (e.g., user credentials), you are responsible for keeping your user credentials secure and confidential and not disclosing them to anyone.

10. Your Rights

10.1. Data Subject Rights.

Under applicable data protection and privacy laws, you may have the right to:

- **Access your personal data:** You may ask us whether we process any personal data related to you. If this is the case, we may ask for your limited personal data to authenticate you insofar as required by applicable data protection laws.
- **Correct and erase your personal data:** Please request us to correct any inaccurate personal data we process about you. Also, you may ask us to erase the personal data related to you if it is no longer necessary for the purposes we processed it or if you have withdrawn your consent, provided we do not have another legal basis for processing your personal data.
- **Object to processing your personal data:** You may object to our processing of your personal data based on our legitimate interest. We will then only process your personal data if we have an overriding legitimate interest.
- **Data portability:** In certain circumstances, you may request receipt or transmission to another organisation, in a machine-readable and structured form, of the personal data you provided to us or if you provided it to us with your consent.
- **Lodge a complaint:** If you think we did not comply with the applicable data protection and privacy laws, we ask you to please get in touch with us and our data protection function will investigate and respond to you.

10.2. Exercising your rights.

- 10.2.1. Please get in touch with our Data Protection Function directly at the contact details indicated below to exercise your rights or if you have questions about the use of your personal data.
- 10.2.2. You may be subject to identification procedures and measures to ensure that no personal data is disclosed to unauthorised persons. We may also request additional information/clarifications to process your request as rapidly and efficiently as possible.
- 10.2.3. Please submit requests in English and clearly describe the reason for the request.
- 10.2.4. We will not normally charge a fee to access your personal data (or exercise other rights). We may charge a fee where your request is unfounded, excessive or repetitive. Alternatively, we may reject such a request as manifestly or excessively burdensome, unfounded and not submitted in good faith.
- 10.2.5. Depending on the complexity of your request and the volume of data associated with it, we will aim to respond to your request within one month of receipt or within an extended period of up to three months (if we require an extension, we will notify you appropriately).

11. Data Protection Officer Contact details

You can address questions and concerns to the Data Protection Function as follows:

Unlimit UK Ltd.

2 Seething Lane 7th Floor London, EC3N 4AT

Email: dpo@unlimit.com

12. Right to file a complaint

If you believe we have not resolved your complaint, you have the right to submit a complaint to the Information Commissioner's Office (ICO) by visiting <https://ico.org.uk/make-a-complaint/>.

13. Your Responsibilities

You are responsible for ensuring that the information provided to us by you or about you or on your behalf is accurate and up to date, and you must inform us if anything changes as soon as possible.

If you provide information about another person, you must direct them to this Privacy Notice and ensure they agree to us using their information as described.

14. Changes to our Privacy Notice

We may revise or update our Privacy Notice from time to time. In such a case, we make the most recent version of the Privacy Notice available on our website, informing you accordingly by displaying in the updated version and relevant date of update.

You are advised to visit our website frequently to consult our Privacy Notice in its most recent version.

Please see the PDF versions below if you wish to see the earlier versions of our Privacy Notice.

Privacy Notice UNL.UK_DP_PN_CUST-01/2022	Updated on 17.07.2026
---	--------------------------