Global Data Protection Notice

Introduction

Your privacy is very important to us. This Global Data Protection Notice explains how we collect, use, store, share, transmit, transfer, delete, or otherwise process (collectively "Process") your Personal Data. It describes the measures we take to protect your Personal Data and provides information on how you can contact us with any questions regarding data protection.

Scope

This notice applies to the Processing of Personal Data collected by Nimble Global Ltd and/or its affiliates, directly or indirectly, from all individuals including, but not limited to, Nimble's current, past, or prospective job applicants, employees, clients, consumers, suppliers/vendors, contractors/subcontractors, shareholders, or any third parties. "Personal Data" refers to any data that relates to an identified or identifiable individual or a person who may be identified by means reasonably likely to be used.

As a global organisation headquartered in London, UK, we are committed to compliance with data protection laws worldwide. This notice is designed to comply with the UK General Data Protection Regulation (UK GDPR) as retained in UK law following Brexit, and the Data Protection Act 2018. We also respect and comply with applicable data protection laws in all jurisdictions where we operate, including but not limited to the EU GDPR, the California Consumer Privacy Act (CCPA), the Australian Privacy Principles, and other applicable regional and national data protection regulations.

Compliance and Audits

As a global provider of compliance audit services, we maintain rigorous internal standards that often exceed minimum legal requirements. We regularly:

- Conduct internal data protection audits and assessments
- Maintain records of processing activities as required by applicable laws
- Perform Data Protection Impact Assessments (DPIAs) for high-risk processing activities
- Train our staff on data protection requirements and best practices
- Review and update our policies and procedures
- Monitor regulatory developments worldwide to ensure ongoing compliance

Our commitment to data protection is integral to our business operations and services.

Consent Collection

Before users submit data through our platform, we obtain explicit consent via a mandatory checkbox with the following language:

✅ *Data Protection and Privacy: By completing this form, I consent to the collection, processing, and secure deletion of my signature and personal information for audit purposes only. My data will be handled in accordance with Nimble Global's Data Protection Notice, which outlines data protection practices and my rights under applicable data protection laws. I understand this information will only be used to verify submission compliance.*

This consent mechanism:

- Is clearly presented and requires affirmative action (ticking the box)
- Is separate from other terms and conditions
- Uses clear and plain language
- Explains the purpose of data processing (audit purposes only)
- References this notice for more detailed information
- Is documented as evidence of consent

In jurisdictions where legal bases other than consent may be more appropriate (such as contractual necessity or legitimate interests), we may rely on those alternative legal bases while still providing the above notice for transparency purposes.

Legal Basis for Processing

We only process your Personal Data when we have a valid legal basis to do so. While the specific legal bases may vary by jurisdiction, our processing generally relies on one or more of the following:

- **Consent**: You have given clear consent for us to process your Personal Data for a specific purpose. Where we rely on consent, you have the right to withdraw this consent at any time.
- **Contract**: Processing is necessary for the performance of a contract with you or to take steps at your request before entering into a contract.
- **Legal obligation**: Processing is necessary for us to comply with legal obligations to which we are subject in the relevant jurisdiction.
- **Legitimate interests**: Processing is necessary for our legitimate interests or the legitimate interests of a third party, provided your fundamental rights and freedoms do not override those interests. Where we rely on legitimate interests, we conduct appropriate assessments to ensure we balance our interests with your rights.

For certain types of data or specific jurisdictions, additional legal bases may apply. We will always ensure that our processing complies with the applicable laws of the jurisdiction relevant to the processing activity and the individual concerned.

Collection and Processing of Your Personal Data

We are committed to complying with applicable data protection laws worldwide. As a UK-headquartered organisation, we primarily adhere to the UK GDPR and Data Protection Act 2018. We also comply with applicable data protection laws in each jurisdiction where we operate or process data of individuals, including but not limited to:

- The EU General Data Protection Regulation (GDPR)
- The California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- The Personal Data Protection Act in Singapore
- The Privacy Act in Australia
- The Protection of Personal Information Act (POPIA) in South Africa
- The Lei Geral de Proteção de Dados (LGPD) in Brazil
- Other applicable national and regional privacy and data protection laws

We ensure that Personal Data is collected and processed lawfully, fairly, and transparently in accordance with these regulations.

Categories of Personal Data We Collect

Depending on your relationship with us, we may collect:

- **Identification information**: Name, email address, postal address, etc.
- **Professional information**: Job title, employer, professional qualifications, etc.
- **Financial information**: Payment details, bank account information, etc.
- **Technical information**: IP address, cookie data, device information, etc.
- **Special category data**: In limited circumstances and only as permitted by UK law, we may collect information about your health, biometric data, etc. We apply additional safeguards to such data as required by law.

Lawfulness, Fairness, and Transparency

We collect and process Personal Data only with a lawful reason, such as for the performance of a contract, compliance with a legal obligation, or with your prior consent. We provide clear information about the processing of your Personal Data, including the responsible entity, purposes, recipients, and your rights.

Legitimate Purpose, Limitation, and Data Minimisation

Your Personal Data is collected for specified, explicit, and legitimate purposes. Nimble processes Personal Data for various purposes, including:

- Compliance with legal and regulatory obligations
- Recruitment and applicant management
- Human resources and employee management

- Financial management and accounting
- IT support and security
- Client relationship management
- Marketing and business development (subject to your preferences)
- Business analytics and improvement of our services

We limit our collection to what is necessary for these purposes and do not use your data for incompatible purposes without providing notice and, where required, obtaining consent.

Data Accuracy and Storage Limitation

Nimble ensures that Personal Data is accurate and up-to-date. We retain Personal Data only as long as necessary for the purposes for which it was collected, including legal, accounting, and reporting requirements. After the applicable retention period, we securely destroy your Personal Data in accordance with applicable laws and regulations.

Security of Your Personal Data

We implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful alteration, loss, unauthorised use, disclosure, or access. These measures include:

- Encryption of personal data where appropriate
- Regular testing and evaluation of security measures
- Access controls and authentication procedures
- Staff training on data protection and security
- Incident response procedures in line with our obligations under UK GDPR
- Data Protection Impact Assessments for high-risk processing activities

We apply privacy by design and by default principles and provide additional safeguards for Special Categories of Personal Data (Sensitive Personal Data).

Disclosure of Your Personal Data

We share your Personal Data under the following circumstances:

- With your consent or as otherwise permitted by law
- With Nimble entities for the purposes described in this notice
- With third-party service providers who perform services on our behalf
- With financial institutions, regulatory bodies, and law enforcement authorities, as necessary
- In connection with the sale, merger, acquisition, or reorganisation of our business or assets

We ensure that third parties who access your data are bound by appropriate confidentiality and data protection obligations.

International Personal Data Transfers

As a global organisation, we may transfer your Personal Data across international borders to countries outside your country of residence, including to countries that may not provide the same level of data protection. When we transfer Personal Data internationally, we implement appropriate safeguards in accordance with applicable laws.

For transfers from the UK:

- International Data Transfer Agreement (IDTA)
- International Data Transfer Addendum to the EU SCCs
- UK adequacy regulations

For transfers from the EEA:

- Standard Contractual Clauses approved by the European Commission
- EU adequacy decisions

For transfers to and from other jurisdictions:

- Binding Corporate Rules
- Regional or country-specific approved transfer mechanisms
- Derogations for specific situations as permitted by applicable law, such as your explicit consent

Where transfers occur to processors in the United States, we ensure compliance with all applicable data protection requirements.

We maintain a record of all data transfers and the safeguards implemented. Details about these transfers and the safeguards we implement are available in our specific privacy notices or upon request.

Automated Decision-Making and Profiling

We may use automated decision-making, including profiling, that produces legal or similarly significant effects concerning you, we will:

- Notify you that we are engaging in such activity
- Provide meaningful information about the logic involved
- Explain the significance and potential consequences
- Implement suitable safeguards as required by UK GDPR
- Allow you to request human intervention, express your point of view, and contest the decision

In accordance with UK data protection law, we will not make decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects unless:

- The decision is necessary for entering into or performing a contract between you and us
- The decision is authorised by UK law, which applies to us and which contains suitable safeguards
- You have given your explicit consent

Cookies and Similar Technologies

Our websites may use cookies and similar technologies to enhance your online experience. We use:

- **Essential cookies**: Necessary for the website to function properly
- **Performance cookies**: Help us understand how visitors interact with our website
- **Functionality cookies**: Remember your preferences and settings
- **Targeting/advertising cookies**: Deliver relevant advertisements

In accordance with UK regulations, we will obtain your consent before placing non-essential cookies on your device. You can manage your cookie preferences through our cookie banner, adjust your browser settings to refuse cookies, or delete cookies that have already been set. Please note that if you choose to disable certain cookies, some parts of our website may not function properly.

For more detailed information, please refer to our separate Cookie Policy available on our website.

Your Rights

Depending on your location, you may have various rights regarding your Personal Data. We are committed to respecting these rights in accordance with applicable laws in your jurisdiction. These rights may include:

For individuals in the UK and EU:

- **Right to be informed**: Receive clear information about how we use your Personal Data
- **Right of access**: Obtain confirmation that we process your data and request a copy of your Personal Data
- **Right to rectification**: Correct inaccurate data or complete incomplete data
- **Right to erasure** (sometimes called 'the right to be forgotten'): Request deletion of your data in certain circumstances
- **Right to restrict processing**: Request that we limit the way we use your Personal Data in certain circumstances
- **Right to data portability**: Receive your data in a structured, commonly used, machine-readable format and transmit it to another controller
- **Right to object**: Object to processing based on legitimate interests (including profiling) and for direct marketing

- **Rights related to automated decision-making and profiling**: Not be subject to decisions based solely on automated processing that produce legal or similarly significant effects

For California residents:

- Right to know what personal information is collected, used, shared, or sold
- Right to delete personal information held by businesses
- Right to opt-out of the sale of personal information
- Right to non-discrimination for exercising consumer rights

For individuals in other jurisdictions:

Additional rights may apply based on local laws. Please contact us for specific information regarding your rights in your jurisdiction.

We will respond to requests to exercise these rights within the timeframe required by applicable law (generally one month for UK/EU requests, 45 days for California requests, which may be extended in certain circumstances). In most cases, there is no fee for exercising these rights, but we may charge a reasonable fee or refuse to act on requests that are manifestly unfounded or excessive.

To exercise these rights or contact us with data protection-related queries, please submit the dedicated Subject Access Request web form available on our website or contact us using the details provided below.

Updates to This Notice

We may update this notice as our business or legal requirements change. Significant changes will be posted on our website with a new effective date, and where appropriate, communicated directly to you. We encourage you to review this notice periodically.

Data Protection Officer and Contact Information

For questions, comments, or requests regarding this notice, please contact our Data Protection Officer at:

- Email: dataprotection@nimbleglobal.com
- Postal address: Nimble Global Ltd, Data Protection Officer, 74-75 Shelton Street, London WC2H 9JQ, United Kingdom

Supervisory Authorities

If you believe that we have not adequately addressed your data protection concerns, you have the right to lodge a complaint with the appropriate supervisory authority:

- UK residents: Information Commissioner's Office (ICO) - https://ico.org.uk/make-a-complaint/ or by calling 0303 123 1113
- EU residents: Your local data protection authority (DPA)
- US residents: Federal Trade Commission (FTC) or your state Attorney General's office
- Other jurisdictions: The relevant data protection or privacy regulator in your country

As a UK-headquartered company, our lead supervisory authority is the UK Information Commissioner's Office.

Last update: 9 May 2025

End of Notice