Data Privacy Notice

Last updated: 29 May 2026

1. Introduction and scope

Nimble Global Ltd ('Nimble Global', 'we', 'our' or 'us') is committed to protecting personal data and to responsible data governance across our global operations. As an international workforce compliance, audit, governance and advisory organisation, we treat privacy as a matter of operational integrity and professional accountability, not merely technical compliance.

This Notice explains how we collect, use, disclose, transfer and protect personal data through our websites and digital platforms (including www.nimbleglobal.com), client audit and compliance portals, workforce compliance engagements, supplier and worker audit programmes, consulting and advisory services, and related communications and operational activities.

It is relevant to anyone whose personal data we process in the course of our work, including individuals connected with the clients, suppliers, workforce providers and technology platforms we serve, and the workers and contractors engaged through their supply chains.

This Notice applies globally and is designed to align with internationally recognised privacy and data-protection principles. Depending on the engagement and the location of the individuals concerned, the laws that may apply include, among others:

- the UK GDPR and the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), and the Privacy and Electronic Communications Regulations ('PECR');
- the EU General Data Protection Regulation ('EU GDPR');
- Australia's Privacy Act 1988 and the Australian Privacy Principles ('APPs');
- Brazil's Lei Geral de Proteção de Dados ('LGPD');
- Canada's Personal Information Protection and Electronic Documents Act ('PIPEDA') and applicable provincial laws, including Québec's Law 25;
- Singapore's Personal Data Protection Act ('PDPA');
- the Swiss Federal Act on Data Protection ('FADP');
- the United States, including state-level comprehensive privacy laws such as California's CCPA/CPRA and the comparable laws now in force across a growing number of other states; and
- other applicable privacy and data-protection laws (such as China's PIPL, India's Digital Personal Data Protection Act, the Kingdom of Saudi Arabia's PDPL, the United Arab Emirates regime and South Africa's POPIA) in jurisdictions where we operate or support clients.

Jurisdiction-specific provisions are set out in Section 22.

2. Key terms

Because this Notice addresses multiple legal regimes that use different terminology, the following terms are used throughout:

- **Personal data / personal information**: any information relating to an identified or identifiable individual. 'Personal data' is used in the UK, EU and many other regimes; 'personal information' is used in the United States and certain others. We use the terms interchangeably.

- **Processing**: any operation performed on personal data, including its collection, recording, storage, use, disclosure, transfer and deletion.
- **Controller / processor**: a controller determines the purposes and means of processing; a processor (a 'service provider' under certain US laws) processes personal data on a controller's behalf and on its instructions.
- **Special category / sensitive data**: categories of data that applicable law treats as requiring heightened protection (see Section 8).

3. Our role in data processing

Our role under data-protection law depends on the nature of each engagement. Identifying it matters, because it determines who is responsible for which obligations. Depending on the engagement, we may act as:

- **Controller**: where we determine the purposes and means of processing, for example in managing our own business relationships, personnel and communications, and in certain independent audit, governance and expert engagements in which we exercise professional judgement over the data we hold;
- **Processor / service provider**: where we process personal data on a client's behalf and on its instructions, for example when conducting a supplier or worker audit of a client's contingent-workforce supply base;
- **Joint controller**: where we and another party jointly determine the purposes and means of processing; or
- **Independent recipient**: where we receive personal data and determine our own purposes for it, distinct from those of the disclosing party.

Where we act as a processor, the relevant controller's own privacy notice governs the processing; affected individuals should exercise their rights through that controller, and we will support the controller in responding. Where we act as a controller or independent recipient, this Notice applies directly.

4. Categories of individuals whose data we process

Depending on the engagement, we may process personal data relating to:

- our own personnel, and individuals at the clients, suppliers, partners and technology platforms we work with (for example, contacts, signatories and authorised representatives);
- candidates and prospective workers;
- contingent workers, contractors and other personnel engaged through our clients' workforce programmes; and
- workers and personnel engaged through lower tiers of a client's supply chain, including end workers from whom, or about whom, we obtain documentation during worker-level audits, who may be several tiers removed from our direct client.

We recognise that worker-level audit activity reaches individuals at the base of complex supply chains. The transparency and indirect-collection considerations that apply to those individuals are addressed in Section 7.

5. Our commitment to responsible data governance

We are committed to:

- collecting only data reasonably necessary for legitimate business, compliance, contractual, legal or operational purposes;
- maintaining appropriate technical and organisational safeguards;
- supporting transparency and accountability in how data is handled;
- embedding privacy and security considerations into our operational workflows and technology decisions;
- limiting access to personal data on a need-to-know basis; and
- continuously reviewing and improving our data-governance practices.

6. Information we collect

Depending on the interaction or engagement, we may collect and process:

- name and contact information;
- company, role and professional details;
- employment or contractor-related information;
- supplier and vendor information;
- identification and verification information;
- immigration, visa or work-authorisation information where relevant;
- insurance and compliance documentation;
- communications and correspondence;
- website usage and technical information;
- audit and compliance submission records;
- billing and payment-related information;
- training, certification and credential information; and
- security, access and system-log information.

Some of this information may include special category or criminal-offence data, which we handle as described in Section 8.

7. How we collect personal data

We collect personal data both directly and indirectly. We collect it directly from individuals when they interact with us, our websites or our platforms, or provide documentation in the course of an engagement. We collect it indirectly from our clients, suppliers, workforce and technology providers, publicly available sources and other authorised third parties.

Where we obtain personal data about an individual from someone other than the individual (for example, where documentation about a worker is provided to us by a supplier or managed-service provider during an audit), additional transparency obligations apply under laws such as Articles 13 and 14 of the UK and EU GDPR. In those circumstances, we, or the controller on whose behalf we act, will provide affected individuals with the information required by applicable law (including the categories of data obtained and their source) within the required timeframes, except where a recognised exemption (such as where provision would involve disproportionate effort) applies and has been appropriately assessed and documented. Where we act as a processor, we support the relevant controller in meeting these obligations.

8. Special category and criminal-offence data

Some engagements require us to process special category personal data (such as data revealing health, or racial or ethnic origin) and data relating to criminal convictions and offences. This may arise, for example, through identity and right-to-work verification, immigration and visa documentation, and background-screening records obtained during workforce and supplier audits.

We process such data only where a lawful basis and an additional condition for processing are satisfied under applicable law. In the UK and EU, this includes the conditions in Article 9 (and, for criminal-offence data, Article 10) of the GDPR and the corresponding conditions in Schedule 1 to the Data Protection Act 2018, and we maintain the appropriate-policy documentation and safeguards those conditions require. Certain US state laws separately treat defined ‘sensitive personal information’ as requiring additional protection and, in some cases, confer a right to limit its use; we honour those rights where they apply (see Section 22).

9. Why we process personal data

We process personal data for legitimate operational, commercial, compliance and legal purposes, including to:

- deliver audit, governance and compliance services;
- manage workforce compliance engagements;
- conduct supplier and worker assessments and operational reviews;
- support onboarding and contractual processes;
- verify compliance with legal, regulatory and client requirements;
- manage business relationships and communications;
- protect our systems, networks and information assets;
- detect, prevent and investigate fraud, misconduct and security incidents;
- comply with legal obligations and regulatory requests;
- improve our services, platforms and operational processes; and
- support business continuity, governance and risk management.

10. Legal bases for processing

Where required by applicable law, we process personal data on one or more of the following bases:

- consent;
- contractual necessity;
- compliance with legal obligations;
- legitimate interests (and, in the UK, the ‘recognised legitimate interests’ introduced by the Data (Use and Access) Act 2025);
- the establishment, exercise or defence of legal claims; and
- other lawful bases permitted under applicable law.

Our legitimate interests may include operational management, client-service delivery, fraud prevention, information security, business administration, governance oversight and risk management. Where we rely on legitimate interests, we have assessed that they are not

overridden by individuals' interests, rights or freedoms, and individuals may request further information about that assessment.

11. Automated processing and AI-assisted analysis

We use analytical tools, automation and AI-assisted processes to support audit workflows, data analysis and operational efficiency. We do so within a governance framework designed to keep such tools accountable and subject to human judgement. In particular:

- we do not make decisions producing legal or similarly significant effects on individuals based solely on automated processing without meaningful human involvement. Where our work informs significant determinations about individuals (such as assessments relevant to worker classification or status), those determinations are subject to qualified human review and professional judgement;
- where applicable law permits automated decision-making on a given basis (including the recalibrated rules introduced in the UK by the Data (Use and Access) Act 2025), we apply the safeguards that law requires, including providing information about the decision, enabling individuals to make representations, and providing for human intervention; and
- we assess the privacy, fairness and governance implications of analytical and AI technologies before and during their use, consistent with emerging regulatory expectations for the responsible use of such tools.

If our position on solely automated decision-making materially changes, we will update this Notice where required.

12. Marketing communications

Where you have subscribed to our communications (including The Compliance Edge newsletter) or where we are otherwise permitted to contact you, we may send you updates, insights and information about our services and activities.

We send marketing communications only where we have a lawful basis to do so, which, depending on your location, may be your consent or a 'soft opt-in' relationship under PECR, and in accordance with equivalent rules elsewhere (such as Canada's CASL, the United States' CAN-SPAM Act and Singapore's Do Not Call provisions). You may withdraw consent or opt out of marketing at any time using the unsubscribe mechanism in our communications or by contacting us, and we will action your request promptly.

13. How we share personal data

We may share personal data:

- internally within Nimble Global on a need-to-know basis;
- with trusted service providers, subprocessors, technology vendors and professional advisers operating under contractual confidentiality and security obligations;
- with clients, suppliers or workforce partners where operationally or contractually necessary;
- where required by law, regulation, court order or governmental authority;
- to protect the rights, safety, property, systems or operations of Nimble Global, our clients or others;
- in connection with a merger, acquisition, restructuring, financing or other business transaction; or
- with your consent or at your direction.

We do not sell personal data.

14. International data transfers

As a global organisation, we may transfer personal data internationally, including outside the United Kingdom, the European Economic Area, Switzerland or an individual's country of residence. Where we do, we implement appropriate safeguards, which may include:

- Standard Contractual Clauses and the UK International Data Transfer Addendum;
- transfers to jurisdictions recognised as providing an adequate level of protection, assessed in the UK under the 'data bridge' framework introduced by the Data (Use and Access) Act 2025, which considers whether protection in the destination is not materially lower than under the UK regime;
- recognised certification or equivalent transfer mechanisms;
- transfer risk assessments; and
- contractual, technical and organisational security measures.

Where relevant, we also assess the privacy and security practices of the vendors, subprocessors and operational partners involved in cross-border processing.

15. Data retention

We retain personal data only for as long as necessary for the purposes for which it was collected and to meet our contractual, legal, regulatory, tax, accounting, audit and governance obligations, to resolve disputes and to enforce our agreements.

We determine retention periods by reference to the nature and sensitivity of the data, the purpose of processing, applicable legal and limitation periods, and the requirements of the relevant engagement. We maintain a retention schedule that sets out indicative periods by data category, available to individuals and clients on request. Where data is no longer required, we securely delete or anonymise it.

16. Data security

We maintain technical, administrative and organisational safeguards designed to protect personal data against unauthorised access, disclosure, alteration, loss, misuse or destruction. These may include:

- encryption and secure transmission protocols;
- role-based access controls and least-privilege principles;
- authentication and identity-management controls;
- monitoring and logging mechanisms;
- secure collaboration environments;
- confidentiality obligations for personnel and vendors;
- vulnerability assessments and security reviews; and
- incident-response and escalation procedures.

While no system can guarantee absolute security, we continually review and improve our safeguards in light of evolving risks and industry practice.

17. Personal data breaches

We maintain procedures to detect, assess, manage and respond to personal data breaches. Where a breach is likely to result in a risk to individuals, we will notify the relevant supervisory authorities and, where required, affected individuals, within the timeframes set by applicable law. Where we act on a client's behalf, we will support that client in meeting its own notification obligations.

18. Privacy by design and data governance

We integrate privacy, confidentiality and data-governance considerations into the design and operation of our services, workflows and technology environments. This includes:

- limiting data collection to what is reasonably necessary;
- assessing higher-risk processing activities, including through Data Protection Impact Assessments ('DPIAs') or equivalent risk assessments where appropriate;
- implementing governance and accountability measures;
- supporting transparency and appropriate oversight; and
- considering security and privacy impacts during operational and technology changes.

19. Cookies and similar technologies

Our websites use cookies and similar technologies to support functionality, security, performance and user experience. The categories we use are essential, analytics, preference and functionality cookies.

Essential cookies are necessary for our websites to operate. Where consent is required by law (including under PECR and the EU ePrivacy rules), we obtain it through our cookie-consent tools before setting non-essential cookies, and you may review or change your preferences at any time through those tools. Further detail is set out in our Cookie Policy. Disabling certain cookies may affect website functionality.

20. Children's privacy

Our services are intended for business and professional use and are not directed at individuals under the age of 18. We do not knowingly collect personal data from children. If we become aware that such information has been collected unintentionally, we will take appropriate steps to delete it.

21. Your privacy rights

Depending on applicable law and your location, you may have rights in relation to your personal data, including the rights to:

- access your personal data;
- request correction of inaccurate information;
- request deletion;
- restrict or object to processing;
- data portability;
- withdraw consent where processing is based on consent;

- rights relating to automated decision-making; and
- lodge a complaint with a supervisory authority.

To exercise your rights, please contact dataprotection@nimbleglobal.com. In handling requests:

- we will verify your identity before acting on a request, and may ask for information to do so;
- we recognise authorised agents acting on an individual's behalf where applicable law provides for this;
- we respond within the timeframes required by applicable law (for example, one month under the UK and EU GDPR, and 45 days under many US state laws), and will tell you if we need an extension;
- we do not charge a fee for most requests; and
- where we decline a request, we will explain why and, where applicable law provides for it (as several US state laws do), you may appeal our decision using the process we will provide.

Certain rights may be subject to legal limitations, exemptions or verification requirements. Where we process your data as a processor on a client's behalf, we will direct your request to, or support, the relevant controller.

22. Jurisdiction-specific provisions

The following provisions supplement the rest of this Notice for individuals in the jurisdictions identified. Where they conflict with the general provisions, these provisions prevail for the relevant individuals.

United Kingdom and European Economic Area

Our processing is governed by the UK GDPR and the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025) and, in the EEA, by the EU GDPR. You have the rights described in Section 21 and may complain to your supervisory authority, which in the UK is the Information Commissioner's Office. You may also raise a complaint directly with us in the first instance, and we will acknowledge and respond to it.

Australia

We handle personal information in accordance with the Privacy Act 1988 and the Australian Privacy Principles, including in relation to cross-border disclosure and the Notifiable Data Breaches scheme. The authority is the Office of the Australian Information Commissioner.

Brazil

Processing of data relating to individuals in Brazil is subject to the LGPD. You have rights including confirmation of processing, access, correction, anonymisation, and information about the sharing of your data. We have appointed a data protection officer (encarregado), and the authority is the Autoridade Nacional de Proteção de Dados ('ANPD').

Canada

We handle personal information in accordance with PIPEDA and applicable provincial laws, including Québec's Law 25, which imposes additional requirements. The federal authority is the Office of the Privacy Commissioner of Canada.

Singapore

We comply with the PDPA, including its consent, purpose-limitation and notification obligations and the Do Not Call provisions. We have designated a Data Protection Officer as the PDPA

requires; contact details are in Section 26. The authority is the Personal Data Protection Commission.

Switzerland

Processing of data relating to individuals in Switzerland is subject to the revised FADP. The competent authority is the Federal Data Protection and Information Commissioner ('FDPIC'). Where required, we maintain a representative in Switzerland.

United States

A growing number of US states have enacted comprehensive privacy laws, and we treat the United States as a set of distinct state jurisdictions rather than a single regime. Depending on the state in which you reside, you may have rights to access, delete and correct personal information; to opt out of its sale, of sharing for cross-context behavioural advertising, and of certain profiling; to limit the use of sensitive personal information; and to appeal a refused request, in each case without discrimination for exercising your rights. Where required, we honour recognised universal opt-out signals, such as the Global Privacy Control. We do not sell personal information.

California. California residents have the rights described above under the CCPA/CPRA, including the right to know the categories of personal information collected and disclosed, to delete and correct it, to opt out of its sale or sharing, and to limit the use of sensitive personal information. We do not sell personal information.

Other jurisdictions

Where we process personal data subject to other regimes (such as China's PIPL, India's Digital Personal Data Protection Act, the Kingdom of Saudi Arabia's PDPL, the United Arab Emirates regime or South Africa's POPIA), we assess and apply the requirements of those laws, including any local consent, cross-border transfer and representation requirements.

23. Representatives

Where the nature or scope of an engagement requires us to appoint a representative in a jurisdiction in which we are not established (for example, a representative in the EU or EEA under Article 27 of the EU GDPR, or a representative in Switzerland under the FADP), we will appoint a designated representative in the relevant jurisdiction for that engagement and make their contact details available to affected individuals and supervisory authorities on request.

24. Third-party websites and services

Our websites and materials may contain links to third-party websites, systems or services. We are not responsible for the privacy practices, content or security of external third parties, and we encourage you to review the privacy notices of any third-party services you access.

25. Changes to this Notice

We may update this Notice periodically to reflect legal or regulatory developments, operational or technology changes, new services or activities, or evolving privacy and governance practices. Where material changes occur, we will provide additional notice through website updates, notifications or other appropriate means.

26. Contact and complaints

For questions, concerns or privacy-related requests, please contact:

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

Where a jurisdiction requires a formally designated data protection officer or equivalent (for example, under Singapore's PDPA or Brazil's LGPD), the same contact fulfils that function.

We encourage you to contact us first so that we can address your concern. You also have the right to complain to a supervisory authority, including:

- United Kingdom: Information Commissioner's Office (https://ico.org.uk/make-a-complaint/);
- EU / EEA: your national data protection authority;
- Switzerland: Federal Data Protection and Information Commissioner;
- Canada: Office of the Privacy Commissioner of Canada;
- Singapore: Personal Data Protection Commission;
- Australia: Office of the Australian Information Commissioner;
- Brazil: Autoridade Nacional de Proteção de Dados; and
- United States: your state attorney general or, in California, the California Privacy Protection Agency.