



Employee Data Protection Policy

October 2026

Contents

1. Introduction	3
2. Scope.....	3
3. Information We Collect	3
4. Why We Use Your Information.....	5
5. Legitimate Interests of Enfinity	5
6. Rights under EU GDPR.....	6
7. How We Share Personal Data	7
8. Security of Your Personal Data	7
9. International Data Transfers	7
10. Workplace Monitoring.....	8
11. Use of AI-Assisted Tools.....	8
12. Marketing.....	8
13. Departing, Absent, or Terminated Employees	9
14. Retention of Personal Data.....	10
15. Questions	10
16. Approval; Amendment of Policy	10
17. Country-specific Annexes.....	11

1. Introduction

Enfinity Global Group (“**Enfinity**”, the “**Data Controller**”, or the “**Company**”) is committed to complying with the applicable data privacy and security requirements in the countries in which it operates. Enfinity complies with internationally recognized standards of privacy protection, and with various privacy laws including, but not limited to, the EU General Data Protection Regulation (“**GDPR**”), the UK General Data Protection Regulation (“**UK GDPR**”), the California Consumer Privacy Act, as amended (“**CCPA/CPRA**”), India’s Digital Personal Data Protection Act, 2023 (“**DPDPA**”), and Japan’s Act on the Protection of Personal Information (“**APPI**”) as applicable.

This Employee Data Protection Policy (the “**Policy**”) summarizes our practices for gathering, storing, and using employee personal information. We encourage you to review this information so that you understand how we collect, use, and share your personal information.

2. Scope

This Policy applies to personal data of all current or former Enfinity employees (at all levels), officers, directors, contractors, or any persons who act on behalf of Enfinity (or otherwise work for Enfinity, regardless of the type of contractual relationship with Enfinity, and whether permanent or temporary) (each, an “**Enfinity Professional**”).

This Policy applies to our group of companies. For Enfinity Professionals, the controller of your personal data is the Enfinity entity that is your employer. So, when we mention “Enfinity”, “we”, “us” or “our” in this Policy, we are referring to the relevant company within our group of companies acting as controller for your personal information. Any privacy-related queries for your data controller may be directed to privacy@enfinity.global.

3. Information We Collect

We collect, use, and store (collectively “**process**”) different types of personal data about you in the operation of our business. We process personal data about Enfinity Professionals primarily for managing our employment relationship with you and managing your interactions with workplace facilities/information systems. If you are a former Enfinity Professional, we process personal data about you primarily for legal compliance. If you are external staff, the type of personal data we process is limited to what we need to manage your engagement with Enfinity and access to Enfinity facilities and information systems. If you are a candidate, the type of personal data we process is generally limited to what we need to engage with you about Enfinity career opportunities, consideration of your application for employment to specific roles at Enfinity, including candidate screening, interview scheduling and management, lawful background screening, and to on-board you at Enfinity if you receive and accept an offer of employment with us. Our processing of candidate personal data during the recruitment process is described in the Recruitment Privacy Statement; this Policy applies to you once you become an Enfinity Professional.

The personal data we process can include, but is not limited to, the following:

- **Name and contact data.** Your first and last name, employee identification number, email address, mailing address, phone number, photo, beneficiary and emergency contact details, and other similar contact data. Additionally, you may

opt to provide additional contact information such as personal email address(es) and/or cell phone number(s).

- **Demographic data.** Your date of birth and gender as well as more sensitive personal data (also known as special category data) including information relating to racial and ethnic origin. In some cases, such as for your date of birth, this information may be used also for corporate initiatives dedicated to employees and the team building, including by making such information available on the Company systems.
- **National identifiers.** Your national ID/passport, citizenship status, residency and work permit status, social security number, or other taxpayer/government identification number.
- **Employment details.** Your job title/position, office location and/or remote working location, employment contract, offer letter, hire date, termination date, performance history and disciplinary records, training records, leave of absence, sick time, and vacation/holiday records.
- **Spouse's/partner's and dependents' information.** Your spouse and dependents' first and last names, dates of birth, and contact details.
- **Background information.** Your academic and professional qualifications, education, CV/Resume, credit history and background screening and vetting purposes where permissible and in accordance with applicable law.
- **Video, voice, and image.** We may collect and use your video, voice, and image data, subject to the requirements of local law and internal policy. Your photo may also be collected in the course of events, meetings, or conferences, and may be used to promote corporate activities and initiatives and made available on websites, presentations, brochures, and other online and offline materials of Enfinity.
- **Financial information.** Your bank account details, tax information, salary, retirement account information, company allowances and other information necessary to administer payroll, taxes, benefits, and equity and incentive compensation.
- **Feedback and survey data.** Your responses to employee surveys, and feedback collected about direct reports, managers, and co-workers.
- **Workplace, Device, Usage, and Content data.** Application data (such as data from Office 365, Teams, Outlook, or internal business processes) including emails sent and received, calendar entries, to-do items, instant messages, technical data and information (containing only limited identifiers, if any personal data at all) in the context of using (online) applications, building and information system access, business devices, system and application usage when accessing and using corporate buildings and assets. We may also collect personal data about you from third parties or public sources as needed to support the employment relationship or to engage with you concerning job opportunities at Enfinity. For example, before and during your employment or assignment with Enfinity, we may collect information from public professional networking sources, such as your LinkedIn profile, for recruitment purposes. We also may conduct lawful background screenings, to the extent permitted by law, through a third-party vendor for information about your past education,

employment, credit and/or criminal history. In the event of a natural disaster or other life/safety emergency, we may rely on public social media posts or other public sources to account for Enfinity Professionals if otherwise unable to contact them. Additionally, if there is an investigation of an incident involving Enfinity Professionals, we may obtain information relevant to the incident from external sources including private parties, law enforcement or news sources and public social media posts.

4. Why We Use Your Information

We will process your personal data where:

- a) You have given your **consent** to the relevant processing activity for the purposes of which we have informed you. Where this is the case, you always have the right to withdraw that consent;
- b) It is necessary for the **performance of and compliance with your employment contract** or other applicable engagement contract with us or in order to **take steps prior to entering into that contract** or another contract with you;
- c) We need to process your information in order to **comply with a legal or regulatory obligation** (for example, complying with duties under employment, social security, social protection, and tax legislation, including complying with our obligations under equality legislation or in relation to statutory sickness or maternity rights);
- d) It is necessary for **vital interests** relating to you or another person (for example, avoiding serious risk of harm to you or others); or
- e) It is necessary for our **legitimate interests** (or those of a third party) provided that our legitimate interests are not overridden by your interests or rights which require protection of your data.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

5. Legitimate Interests of Enfinity

Where you are an Enfinity Professional in the European Economic Area (EEA) or the United Kingdom, or in another jurisdiction that recognizes legitimate interests as a lawful basis for processing, we may use your personal information where this is necessary for our legitimate interests (or those of a third party). This includes where use of your personal information is necessary:

- To ensure effective administration and management of your employment or engagement, benefits, management of the business, and business continuity;
- To ensure our assets, network, and information are protected, kept confidential, and not used for inappropriate or unlawful purposes;

- To prevent, detect, or investigate unauthorized use of our systems and ensure we comply with law and our policies;
- To ensure we can contact you or your family in the case of an emergency;
- To check you are legally entitled to work, manage performance, discipline, and promotion processes;
- To manage training and development requirements;
- To deal with disputes and accidents and take legal or other professional advice;
- To prevent fraud and financial crime;
- To comply with our legal obligations, regulations, government clearances, or contracts; investigate potential misconduct or violations of company policy or law; or to respond to data subject rights, a court order, administrative or judicial process, such as a subpoena, government audit or search warrant;
- In response to lawful requests by public authorities (such as regulatory bodies, law enforcement authorities, and national security organizations);
- To seek legal advice from external lawyers and advice from other professionals such as accountants, management consultants, etc.;
- As necessary to establish, exercise or defend against potential, threatened or actual litigation;
- Where necessary to protect Enfinity, your vital interests, such as safety and security, or the vital interests of other persons; and
- In connection with the sale, assignment or other transfer of all or part of our business (such as a potential purchaser and its legal/professional advisors).

If you would like further information on our legitimate interests as applied to your personal information, please send your inquiry to privacy@enfinity.global.

6. Rights under EU GDPR

This Section describes the data-subject rights that apply generally to Enfinity Professionals in the European Economic Area (EEA). The GDPR and local laws implementing or supplementing the GDPR provide Enfinity Professionals in the EEA with several rights, including, but not limited to, the right to:

- **Access:** You have the right to request access to your personal data. You are entitled to ask us if we are processing your personal data and, if we are, you can request access to your personal data. This enables you to receive a copy of the personal data we hold about you and certain other information about it.
- **Correction:** You are entitled to request that we correct inaccuracies (rectification) of your personal data. In response to your request, we will update any incomplete or inaccurate personal data we hold about you to ensure it is accurate and correct.

- **Erasure:** You have the right to request erasure of your personal data in certain circumstances, and subject to our obligations to maintain your information under applicable laws or if retention of your personal data is required in connection with claims.
- **Restriction:** You are entitled to ask us to suspend the processing of certain of your personal data, for example if you want us to establish its accuracy or the reason for processing it.
- **Transfer:** You may request to receive information you provided to us in a machine-readable portable format or the transfer of certain personal data to another party.
- **Automated decisions:** You may contest any automated decision made about you where this has a legal or similar significant effect and ask for it to be reconsidered. EEA residents will not be subject to decisions that will have a legal effect, or a significant impact on you, based solely on automated decision-making.
- **Object:** You have a right to object to Enfinity's processing of your personal data where this is based on Enfinity's legitimate interests (or those of a third party). You may challenge our reliance on legitimate interests. However, Enfinity may be entitled to continue processing your personal data based on our legitimate interests or where this is relevant to legal claims. You also have the right to object where we are processing your personal information for direct marketing purposes.

The country-specific Annexes set out how these rights apply in each jurisdiction, together with any additional or differing rights and the local supervisory authority. See Annexes 1-7 for information on employee rights in the various jurisdictions wherein Enfinity operates.

7. How We Share Personal Data

Enfinity will only share your personal data with those who have a legitimate business need for it. Whenever Enfinity transfers your personal data to a third party, including our subsidiaries, affiliates, and third-party service providers, we will ensure that your personal data is secured and used in a manner consistent with this privacy policy. Depending on the circumstances, the categories of recipients may include, without limitation, providers of human resources, recruitment and payroll systems; IT, cloud hosting and information security providers; benefits, insurance and occupational health providers; professional advisors such as auditors, lawyers and accountants; and, where required by law, courts, regulators and other public authorities. Where a recipient acts as a processor, it processes your personal data only on Enfinity's documented instructions and under a written data processing agreement.

8. Security of Your Personal Data

Enfinity is committed to securing your personal data and uses a variety of security measures to protect your personal data from unauthorized access, use, destruction, or disclosure.

9. International Data Transfers

Employee personal data may be transferred to or processed to countries outside of where the personal data was originally collected. For example, Enfinity operates in multiple countries, with its global headquarters in the United States, and employee personal data collected in other countries is routinely transferred to the United States for processing in relation to Enfinity's legitimate interests listed above. When we engage in such transfers, we use a variety of legal mechanisms, in accordance with applicable privacy laws, to help protect your rights and enable these protections to travel with your data.

10. Workplace Monitoring

In compliance with internal policies and where permitted by applicable local law, based on its legitimate interest, Enfinity may monitor, review, investigate, audit, or intercept information stored, sent, received or otherwise facilitated by or through Enfinity Systems, in order to administer the use and access to Enfinity Systems and ensure network and information security. However, Enfinity does not perform such monitoring in the ordinary course. Such monitoring of electronic communications may only be conducted by authorized representatives of Enfinity, which are those employees approved and designated as authorized representatives by the Enfinity Global General Counsel. Nothing in this policy should be construed to interfere with Enfinity's ability to process employee data for purposes of complying with our legal obligations, or for investigating alleged misconduct or violations of company policy or law, subject to compliance with local legal requirements.

11. Use of AI-Assisted Tools

Enfinity may use AI-assisted tools within the systems it uses to manage the employment relationship, to support administrative, organizational, analytical and reporting activities. Where such tools process your personal data, they do so on Enfinity's documented instructions, for the purposes and on the legal bases set out in this Policy, and subject to the same safeguards, retention rules and international transfer mechanisms described in this Policy. Enfinity provides such tools only with the personal data necessary for the relevant purpose.

Enfinity sets limits on the use of such tools. They are not used to take decisions about you based solely on automated processing that produce legal effects concerning you or similarly significantly affect you, and are not relied on as the basis for decisions about your employment, including performance management, promotion, remuneration or termination. Any output generated by an AI-assisted tool that informs a decision about you is subject to review by an authorized member of Enfinity personnel. Where you apply for a role at Enfinity, our use of AI-assisted tools in the recruitment process is described in the Recruitment Privacy Statement. Where applicable, any rights you may have in relation to automated decision-making are set out in the section "Rights under EU GDPR" above, which applies to Enfinity Professionals in the EEA, and in the country-specific Annex to this Policy that applies to your jurisdiction.

12. Marketing

Under certain circumstances, Enfinity may process personal data provided by you for external marketing purposes, including communication activities, institutional campaigns, editorial projects concerning the presentation of the Company and its services, both through traditional methods (such as paper mail, telephone calls with operator, etc.) and by automated means (such as internet communications, email, text messages, applications for mobile devices such as smartphones and tablets, social

network accounts such as Facebook or Twitter, etc.). Enfinity shall obtain your consent prior to use of your personal data for external marketing purposes.

13. Departing, Absent, or Terminated Employees

To balance ongoing legitimate business interests of Enfinity with employee privacy rights, Enfinity will manage departing employee email accounts in accordance with the following policy:

- a. **Prior to (or on day of) departure of employee:** Enfinity will instruct the departing employee to collect/delete personal electronic communications from his/her account and forward any critical business email that Enfinity may need to appropriate internal business colleague before departing.
- b. **Account Deactivation:** Enfinity will deactivate email account of the departing employee after his/her departure. The deactivation process will include disabling the departing employee's access to his/her email account. However, Enfinity may have legitimate business interests (GDPR Article 6.1 f) to leave a departing employee's email account open for a period of time after departure of the employee, as there may be business critical email coming into the departing employee's account during such period.
- c. **Notification:** This Policy constitutes notice, to the extent required by applicable law, to all Enfinity Professionals. In addition to this Policy, the departing employee may receive additional notifications of deactivation of their email account and the company's policy regarding email account management.
- d. **Automatic Response Activation:** Upon departure, Enfinity may activate automatic responses for the departing employee email account that states departure of the employee from Enfinity and provides alternative Enfinity business contact information. Such automatic response will be active for a period determined by Enfinity, generally 1-3 months.
- e. **Temporary Access to Departing, Absent, or Terminated Employee Emails or Files:** In certain exceptional situations related to a departing employee (e.g., sudden or unexpected departure) or an absent employee where business continuity needs cannot reasonably be met through alternative means, access to the departing employee's or absent employee's email account or files stored on Enfinity Systems may be granted subject to Legal department review and approval and in accordance with applicable local law. Subject to Legal department approval, such access will be restricted to authorized Enfinity personnel only and may include the departing employee's manager, the IT department, Legal department, and any other personnel designated by the company. The temporary access to the departing employee's email account or files will be limited to only the information that is necessary to carry out business-related functions or purposes. Any access must be necessary and proportionate to the identified business need. The departed or absent employee will be notified by Enfinity related to such access.

In addition, upon termination of employment, access to a terminated employee's email account or files stored on Enfinity Systems may be granted, subject to review and approval by the Legal Department, for all purposes permitted by law, including but not limited to litigation, arbitration and negotiation. Subject to the approval of the Legal Department, access to terminated employee's email account or files will be restricted to authorized Enfinity personnel only and may

include the departing employee's manager, the IT Department, the Legal Department and any other personnel designated by the Company and will be limited to only the information that is necessary to carry out business-related functions or purposes and must be necessary and proportionate to that purpose.

- f. **Record Retention:** All departing, absent, or terminated employee email messages and attachments and files will be retained in accordance with the company's record retention policy, as updated and amended from time to time.

By adhering to this policy, Enfinity seeks to manage employee email accounts in a secure and confidential manner and protect any sensitive or confidential information contained in these accounts, while preserving the legitimate business interests of Enfinity, and thereby compliantly and appropriately balancing these various interests.

14. Retention of Personal Data

Except as permitted or required by applicable law or regulatory requirements, we may retain your personal data only for as long as it is necessary to fulfill the purposes for which the personal data was collected (including, for the purpose of meeting any legal, accounting, or other reporting requirements or obligations) and for IT archival purposes.

Personal data for data subjects in the EEA is by default erased by Enfinity after termination of employment, except for certain types of personal data, which may be stored for an extended period of time due to administrative purposes, e.g. for payment of retirement income or for giving references to other employers, or where such personal data must be retained to comply with regulatory requirements.

You may request that we delete personal data about you that we hold, provided that we reserve the right not to grant such request if we are not required to delete personal data under applicable law. There are instances where applicable law or regulatory requirements allow or require us to refuse to delete this personal data. If we cannot delete your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

To request deletion of your personal data, please submit your request via privacy@enfinity.global.

15. Questions

If you have any questions regarding this Employee Data Protection Policy, please contact us at privacy@enfinity.global.

16. Approval; Amendment of Policy

This Policy has been approved by the Supervisory Body.

This Policy is an internal document of the Enfinity Global Group. It has been adopted on behalf of Enfinity for its sole use and benefit. This Policy shall be administered on behalf of Enfinity by the Supervisory Body.

There are no other parties who have any right to rely on the terms of this Policy, nor do any other parties have the right to enforce the terms of this Policy. None of Enfinity, any member of Enfinity, nor any officer, director, employee, agent, or affiliate of any of the

foregoing, shall be required to account to, or otherwise inform or notify, any other parties with respect to the matters described in this Policy.

The Supervisory Body shall have the sole and exclusive right and duty to construe and interpret the terms of this Policy, and all such constructions, interpretations and decisions by the Supervisory Body shall be final and binding on all persons and entities whatsoever.

The Supervisory Body shall have the sole and exclusive right to amend, waive, terminate, or otherwise modify the terms of this document, with respect to any specific case or generally.

This Policy is maintained in English. Where a translated version of this Policy or any of its Annexes is made available, then in the event of any conflict between the translated version and the English version, the English version shall prevail to the extent permitted by applicable law.

17. Country-specific Annexes

The Annexes below form part of this Policy. They identify the Data Controller (or, in India, the Data Fiduciary) for each country in which Enfinity employs or engages Enfinity Professionals and provide additional information required under the laws of certain jurisdictions where we operate. They supplement, and do not replace, the rest of this Policy; where an Annex differs from the main text, the Annex applies to Enfinity Professionals in that country. The Annexes are: Annex 1 – Italy; Annex 2 – The Netherlands; Annex 3 – Spain; Annex 4 – Japan; Annex 5 – United States; Annex 6 – India; and Annex 7 – United Kingdom. A translated version of this Policy may include only the Annex or Annexes relevant to the country for which it is prepared, and those Annexes keep the numbering used in this English version. The English version, containing all Annexes, is available on our website.

ANNEX 1 – ITALY

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is Enfinity Global ITA S.r.l., with registered office in via dei Pellegrini 22, 20122 Milan, Italy, cod.fisc. 10353590960.

This Annex and the Policy will be made available to Enfinity Professionals in Italy in Italian. In the event of any conflict between the Italian and English versions, the English version shall prevail to the extent permitted by applicable law.

2. RIGHTS OF THE DATA SUBJECT

Data subjects may exercise, pursuant to Articles 15 to 22 of the GDPR, the right to:

- request confirmation of the existence or otherwise of their personal data;
- obtain information about the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be communicated and, when possible, the storage period;
- obtain the rectification and erasure of data;
- obtain the restriction of processing;
- obtain the portability of the data, i.e. receive them from a data controller, in a structured, commonly used and machine-readable format, and transmit them to another data controller without hindrance;
- object to the processing at any time, including in the case of processing for direct marketing purposes;
- object to an automated decision-making process concerning natural persons, including profiling;
- request from data controller access to and rectification or erasure of personal data concerning him or her or to object to their processing, as well as right to data portability;
- withdraw consent at any time without prejudice to the lawfulness of the processing based on the consent given before the withdrawal;
- lodge a complaint with the Italian Data Protection Authority (www.garanteprivacy.it).

Any request for the exercise of these rights shall be sent by registered letter or by email to privacy@enfinity.global.

3. INTERNATIONAL DATA TRANSFERS

For personal data subject to European data protection laws, we take measures designed to provide the level of data protection required in the EEA, including ensuring transfers are governed by the requirements of the Standard Contractual Clauses adopted by the European Commission, or another adequate transfer mechanism. Relevant Enfinity entities in the EEA have entered into intragroup transfer agreements based on the Standard Contractual Clauses which allows for the processing and transfer of personal data.

4. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. In the event of such changes, we will notify you: (i) by means of an internal announcement on Enfinity systems and/or (ii) by taking any other action we deem appropriate. Any changes made shall be effective upon their publication and/or notice.

ANNEX 2 – THE NETHERLANDS

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is Enfinity Global B.V., with registered office in Prins Bernhardplein 200, 1097 HL Amsterdam, The Netherlands, KVK no. 82623171 and VAT number NL862543150B01.

2. RIGHTS OF THE DATA SUBJECT

Data subjects may exercise, pursuant to Articles 15 to 22 of the GDPR, the right to:

- request confirmation of the existence or otherwise of their personal data;
- obtain information about the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be communicated and, when possible, the storage period;
- obtain the rectification and erasure of data;
- obtain the restriction of processing;
- obtain the portability of the data, i.e. receive them from a data controller, in a structured, commonly used and machine-readable format, and transmit them to another data controller without hindrance;
- object to the processing at any time, including in the case of processing for direct marketing purposes;
- object to an automated decision-making process concerning natural persons, including profiling;
- request from data controller access to and rectification or erasure of personal data concerning him or her or to object to their processing, as well as right to data portability;
- withdraw consent at any time without prejudice to the lawfulness of the processing based on the consent given before the withdrawal;
- lodge a complaint with the Netherlands Data Protection Authority:

Autoriteit Persoonsgegevens
Hoge Nieuwstraat 8
P.O. Box 93374
2509 AJ Den Haag/The Hague
Website: <https://autoriteitpersoonsgegevens.nl/>

Any request for the exercise of these rights shall be sent by registered letter or by email to privacy@enfinity.global.

3. INTERNATIONAL DATA TRANSFERS

For personal data subject to European data protection laws, we take measures designed to provide the level of data protection required in the EEA, including ensuring transfers are governed by the requirements of the Standard Contractual Clauses adopted by the European Commission, or another adequate transfer mechanism. Relevant Enfinity entities in the EEA have entered into intragroup transfer agreements based on the Standard Contractual Clauses which allows for the processing and transfer of personal data.

4. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. In the event of such changes, we will notify you: (i) by means of an internal announcement on Enfinity systems and/or (ii) by taking any other action we

deem appropriate. Any changes made shall be effective upon their publication and/or notice.

ANNEX 3 – SPAIN

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is Enfinity Iberia SLU, with registered office in Paseo de la Castellana 141, planta 15a B/C, 28046 Madrid, Spain, public registry no. M680658.

This Annex and the Policy will be made available to Enfinity Professionals in Spain in Spanish. In the event of any conflict between the Spanish and English versions, the English version shall prevail to the extent permitted by applicable law.

2. RIGHTS OF THE DATA SUBJECT

Data subjects may exercise, pursuant to Articles 15 to 22 of the GDPR, the right to:

- request confirmation of the existence or otherwise of their personal data;
- obtain information about the purposes of the processing, the categories of personal data, the recipients or categories of recipients to whom the personal data have been or will be communicated and, when possible, the storage period;
- obtain the rectification and erasure of data;
- obtain the restriction of processing;
- obtain the portability of the data, i.e. receive them from a data controller, in a structured, commonly used and machine-readable format, and transmit them to another data controller without hindrance;
- object to the processing at any time, including in the case of processing for direct marketing purposes;
- object to an automated decision-making process concerning natural persons, including profiling;
- request from data controller access to and rectification or erasure of personal data concerning him or her or to object to their processing, as well as right to data portability;
- withdraw consent at any time without prejudice to the lawfulness of the processing based on the consent given before the withdrawal;
- lodge a complaint with a supervisory authority (Data Protection Authority):

Agencia Española de Protección de Datos (AEPD)
C/ Jorge Juan, 6, 28001 Madrid, Spain.
Website: www.aepd.es

Any request for the exercise of these rights shall be sent by registered letter or by email to privacy@enfinity.global.

3. INTERNATIONAL DATA TRANSFERS

For personal data subject to European data protection laws, we take measures designed to provide the level of data protection required in the EEA, including ensuring transfers are governed by the requirements of the Standard Contractual Clauses adopted by the European Commission, or another adequate transfer mechanism. Relevant Enfinity entities in the EEA have entered into intragroup transfer agreements based on the Standard Contractual Clauses which allows for the processing and transfer of personal data.

4. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. In the event of such changes, we will notify you: (i) by means of an internal announcement on Enfinity systems and/or (ii) by taking any other action we



deem appropriate. Any changes made shall be effective upon their publication and/or notice.

ANNEX 4 – JAPAN

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is Enfinity Japan K.K., with its registered office at VORT Kioicho 13F, 4-5-21 Kojimachi, Chiyoda-ku, Tokyo 102-0083, Japan.

The representative director is John de Perczel.

This Annex and the Policy will be made available to Enfinity Professionals in Japan in Japanese. In the event of any conflict between the Japanese and English versions, the English version shall prevail to the extent permitted by applicable law.

2. SECURITY CONTROL MEASURES

For more details on security control measures, please contact us through the contact information specified below.

3. RIGHTS OF THE DATA SUBJECT

Data subjects may exercise the following rights in Japan if requirements under the relevant laws are met:

- Request the deletion and discontinuation of data processing or transfer
- Request the discontinuation of transferring of the data to third parties
- Request the discontinuation of using, deletion, or discontinuation of transfers to third parties
- Request the correction, addition or deletion of personal information
- Request the disclosure of personal information being handled by Enfinity
- Request the disclosure of records of transfers of personal information to third parties
- Request the disclosure of information relating to protection measures for cross-border transfers.

4. CONTACT INFORMATION

If you have any opinions, questions, complaints and any other requests in respect of the treatment of your personal data, please contact privacy@enfinity.global.

ANNEX 5 – UNITED STATES

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is Enfinity Global Administration LLC, 501 Brickell Key Drive, Miami, FL 33131, USA.

2. SCOPE

This Annex applies to personal information of Enfinity Professionals who are residents of the United States. California residents are afforded the specific rights described in Section 3 (Rights of the Data Subject) pursuant to the California Consumer Privacy Act, as amended (“CCPA/CPRA”). The position for residents of other U.S. states is addressed in Section 4 (Other U.S. States).

3. RIGHTS OF THE DATA SUBJECT

Subject to applicable law, California residents have the right to:

- know and access the categories and specific pieces of personal information collected, the sources, the purposes, and the categories of third parties with whom it is shared;
- request the correction of inaccurate personal information;
- request the deletion of personal information, subject to permitted exceptions;
- opt out of the sale or sharing of personal information; Enfinity does not sell or share the personal information of Enfinity Professionals as those terms are defined under the CCPA/CPRA;
- limit the use and disclosure of sensitive personal information to the purposes permitted by the CCPA/CPRA; and
- not be subject to discrimination or retaliation for exercising any of these rights.

Any request to exercise these rights may be sent to privacy@enfinity.global. You may also lodge a complaint with the California Privacy Protection Agency.

4. OTHER U.S. STATES

Most other U.S. states that have enacted comprehensive consumer privacy laws exempt personal information processed in an employment context, including information about employees, job applicants, and contractors. Enfinity nonetheless applies the core privacy principles described in this Policy—including transparency, purpose limitation, data minimization, security, and retention limits—to all Enfinity Professionals in the United States.

Certain states, including Illinois, Texas, and Washington, specifically regulate biometric data. Where Enfinity collects biometric data of Enfinity Professionals, it does so only with notice and, where required, consent, and in accordance with applicable law.

In the event of a security incident affecting personal information, Enfinity will provide notification in accordance with the data breach notification laws of the applicable U.S. state or states.

5. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. Changes will be effective upon publication or notice.

ANNEX 6 – INDIA

1. IDENTIFICATION DETAILS OF THE DATA FIDUCIARY

The Data Fiduciaries are Enfinity India Private Limited and Enfinity Global Operations Private Limited, each having its registered office at 8-2-610/68/1, 2, 3, 5th Floor, Accord Blu, Road No. 10, Banjara Hills, Hyderabad 500034, India. Each entity acts as a Data Fiduciary in respect of the Personal Data of the Enfinity Professionals it employs.

2. SCOPE

This Annex applies to Enfinity Professionals in India and is provided pursuant to the Digital Personal Data Protection Act, 2023 (“DPDPA”). This notice is available in English and, on request, will be made available in any language specified in the Eighth Schedule to the Constitution of India.

3. RIGHTS OF THE DATA PRINCIPAL

Subject to applicable law, Data Principals in India have the right to:

- obtain a summary of the personal data being processed and the processing activities undertaken;
- request the correction, completion, updating, and erasure of their personal data;
- nominate another individual to exercise their rights in the event of death or incapacity;
- withdraw consent at any time where processing is based on consent, without prejudice to the lawfulness of processing prior to withdrawal; and
- access a readily available grievance redressal mechanism.

4. GRIEVANCE REDRESSAL

To exercise these rights or to raise a grievance, you may use our grievance redressal mechanism by contacting privacy@enfinity.global. If your grievance is not resolved to your satisfaction, you may lodge a complaint with the Data Protection Board of India.

5. INTERNATIONAL DATA TRANSFERS

Personal data may be transferred outside India in accordance with the DPDPA, subject to any restrictions notified by the Government of India from time to time.

6. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. Changes will be effective upon publication or notice.

ANNEX 7 – UNITED KINGDOM

1. IDENTIFICATION DETAILS OF THE DATA CONTROLLER

The Data Controller is the Enfinity entity that has entered into the agreement with the external company that employs the Enfinity Professionals in the United Kingdom, namely EG UK Development Limited, Spaces Bristol Castle Park, The Pithay, Bristol BS1 2NB, United Kingdom. An external company formally employs the Enfinity Professionals in the United Kingdom and administers their employment, payroll, and related matters on Enfinity's behalf. Because Enfinity determines the purposes and means of processing the Enfinity Professionals' Personal Data, Enfinity is the Data Controller. The external company processes that Personal Data as a processor acting on Enfinity's instructions, and as an independent controller only to the extent required to meet its own legal obligations.

2. RIGHTS OF THE DATA SUBJECT

Data subjects may exercise, pursuant to the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, the right to:

- request access to and a copy of their personal data and information about its processing;
- rectification of inaccurate or incomplete personal data;
- erasure of personal data, restriction of processing, and data portability, in the circumstances set out in the UK GDPR;
- object to processing based on legitimate interests and to processing for direct marketing;
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects;
- withdraw consent at any time, where processing is based on consent, without prejudice to the lawfulness of processing prior to withdrawal; and
- lodge a complaint with the Information Commissioner's Office (ICO), website: <https://ico.org.uk/>.

Any request for the exercise of these rights shall be sent by email to privacy@enfinity.global.

3. INTERNATIONAL DATA TRANSFERS

Transfers of personal data outside the United Kingdom are made pursuant to the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, an adequacy regulation, or another transfer mechanism approved under UK data protection laws.

4. AMENDMENTS

This Annex may be amended to reflect changes in legislation, technology, and changes in data collection and use. Changes will be effective upon publication or notice.