convergint

POLICY: COLLEAGUE & APPLICANT PRIVACY NOTICE

Last Updated: April 14, 2025

Welcome! This Privacy Notice ("Notice") describes how Convergint, including its subsidiaries and affiliates, collect, use, retain, and disclose Personal Data (defined below) from Colleagues or job applicants. For purposes of this Notice, "Company" or "we" means the relevant Convergint entity that employs you or to which you are applying. "Colleague" means:

- Past and present colleagues (employees) of the Company;
- Past and present consultants, independent contractors, and agents of the Company;
- Job applicants, candidates, and referrals;
- Temporary colleagues or contracted workers;
- Retirees; and
- Past and present directors and officers of the Company.

This Notice does not apply to:

- Data collected by the Company from non-Colleagues, or data collected from Colleagues in a non-employment related context. In these situations, please refer to our Privacy Policy located at https://www.convergint.com/privacy/.
- Colleagues in Latin America and the Middle East, for whom we maintain separate privacy notices (please see https://www.convergint.com/colleague-application-privacy-notice/).

Convergint is a global group of entities, and as such this policy includes certain jurisdiction-specific content.

- Annex 1 contains additional information specific to Colleagues in California, including our Notice at Collection.
- Annex 2 contains additional information specific to Colleagues in Canada.
- Annex 3 contains additional information specific to Colleagues in the UK, European Union and Switzerland.
- Annex 4 contains additional information specific to Colleagues in Asia.
- Annex 5 contains additional information specific to Colleagues in Oceania.

1. HOW WE COLLECT PERSONAL DATA, WHAT PERSONAL DATA WE PROCESS, AND HOW WE USE PERSONAL DATA

How we collect Personal Data

The Company collects some categories of Personal Data directly from its Colleagues (for example, your job application, contact information, and employment history) and creates other categories of Personal Data (for example, performance reviews and absence records). We may also collect Personal Data from third parties, such as recruitment agencies or those that refer you for positions, or social media platforms, job boards, or similar sites onto which you have placed your information (such as, for example, LinkedIn). In some instances, the personal information we collect has been inferred about you based on other information you provide us, through your interactions with us, or from third parties.

Certain information is required to enable the Company to enter and administer a contract of employment with you, and you have obligations under your employment contract which require the processing of certain Personal Data. If you do not provide necessary information, this may hinder the Company's ability to administer the rights and obligations essential to our employment

relationship with you. You may also have to provide the Company with personal information in order to exercise your statutory rights, such as statutory leave entitlements. Failing to provide such personal information may mean that you are unable to exercise your statutory rights.

What Personal Data We Process

The categories of Colleagues' Personal Data that the Company Processes are:

- Personal details and contact information, such as name, e-mail and telephone details, address, date of birth, insurance numbers, identification numbers (including government issued numbers such as social security number), gender, marital status, dependents, emergency contact information, and photographs;
- Identifiers, such as online identifiers (e.g., cookies and IP addresses), badge information, and photographs or fingerprint scans for identification, verification, employee ID numbers, or security and access control purposes.
- Payroll processing and compensation data, such as information about banking details, salary, bonus, benefits, equity grants and other awards, and tax
- Right to work and immigration data, such as citizenship, passport, identity card, and details of residency or work permit;
- Talent, recruitment, and application data, such as information about or contained in applications, resumes/CVs, referral letters, background checks, references, education history, professional qualifications, skills, languages spoken, performance ratings, development plans, and work preferences;
- Work and work history, such as descriptions of current and prior positions, titles, salaries, departments, locations, supervisors, direct and indirect reports, performance history, employment status and type, terms of employment, hire and termination date(s), retirement information, promotions, and disciplinary records;
- Work schedule data, such as working time records including vacation, sick leave, other absence records, leave status, hours worked, overtime, and shift work;
- Accident, health, and medical data, in connection with health and safety, benefits, and worker's compensation administration
- Benefits administration data, such as Personal Data necessary to administer your benefits including health, retirement, insurance, and other benefits that we may offer Colleagues from time to time;
- Travel information, such as travel bookings, itineraries, government issued numbers, and travel preferences; and
- Inferences drawn from other Personal Data, such as inferences about a person's performance at work.
- Other Sensitive personal information, as further described in this Policy including under the "Sensitive Personal Data."
- Other information you provide during application, onboarding, or employment.

In certain jurisdictions, we may obtain Personal Data through Company-owned devices and vehicles, or through your personal devices or vehicles that you use for work purposes. Not all of these activities are conducted in all regions, including where they are prohibited by law, and we obtain your consent before collecting this data where consent is required by law. You may contact dataprotectionofficer@convergint.com for information on the specific practices within your region.

- GPS tracking devices may be used in Company-managed vehicles for purposes of employee time tracking, vehicle maintenance, dispatch and scheduling, promoting safe driving habits, auditing, reducing fraud, controlling fuel costs, and analyzing business

related metrics. When utilized, the GPS tracking devices can provide the Company with information such as vehicle location, travel routes and speed, off hour usage, idle time, sensor tampering, telemetry information, vehicle start and stop times, and arrival and departure times.

- Company-provided vehicles may also be equipped with a camera recording system containing cameras (also known as "DashCams"). These are used to promote safety and security, to protect Company's property, and to prevent fraudulent or wrongful conduct. DashCams may collect information such as vehicle registration, dashcam video footage, sensor data collected by DashCams related to the vehicle's operation, and colleague interactions with the DashCam system.
- GPS tracking of your mobile device may be used to support vehicle mileage reimbursement programs for your business use of personal vehicles. The data collected is limited to what is relevant for vehicle mileage reimbursement calculations. You may also have the option to report vehicle reimbursement information manually.
- Some Company locations conduct video camera monitoring of the workplace for purposes of safety and security.
- Phone calls may be monitored when interacting with company personnel, a customer or other business associate, or member of the public, including for customer service, for training, audit, and record keeping purposes.
- Meetings may be recorded or transcribed for productivity and record keeping purposes, including for later review by other Colleagues and for automatic creation of meeting summaries or notes.
- When utilizing laptops, tablets, mobile phones, or Company networks and servers (collectively, "Devices") for Company-related purposes, the Company may access contents of the Devices and monitor activity of the Devices consistent with Company policies, including without limitation files, emails, chats, messages (e.g., Slack, Teams, etc.), usage activity, and browsing history.

Your telephone conversations, emails, chat messages, or internet usage by any electronic device or system used for work purposes or connected to work systems or networks, including but not limited to computers, telephones, or mobile devices, may be subject to monitoring or review by any lawful means consistent with Company policies.

How We Process Personal Data

We may use Colleague Personal Data for the following purposes:

- Recruiting: Fielding applicants and applications; evaluating suitability for roles
- Vetting of applicants: conducting interviews, screenings, assessments, and background checks, including using automated and machine learning technologies (such as AI enabled technology) to analyze applicant Personal Information and increase the efficiency and effectiveness of human resources review and analysis
- Onboarding of applicants: confirming legal status and right to work, establishing payroll and tax
- Managing workforce: managing work activities and personnel, including managing and allocating Company assets, workforce analysis and planning, human resources activities and operations, business and strategic planning and management, auditing and reporting, financial management and reporting, conducting business with customers, vendors, or other associates, appraisals and performance evaluations, promotions and succession planning, administering salary, bonuses, equity grants, and benefits, training, maintaining Colleague directories, disciplinary matters and terminations, travel arrangements,

providing proper security, and other administrative functions to assist Colleagues in meeting their job expectations

- IT: providing appropriate IT equipment and services, operating, managing, and safeguarding the Company's IT and communications systems
- Communications and emergencies: facilitating communication with and between Colleagues, providing references, protecting the health and safety of Colleagues and others, facilitating communication to promote the well-being of Colleagues or customers including during an emergency;
- Complying with legal obligations: complying with our regulatory obligations, court orders, subpoenas, and similar requests, performing background checks as required by applicable laws, conducting checks against exclusion and sanction lists as required by applicable laws;
- Compliance: conducting and managing complaints, investigations, and claims, processing work-related claims, such as worker's compensation claims, complying with legal, regulatory, and other requirements, such as health and safety, income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public or regulatory authorities, complying with internal policies and procedures, defending or pursuing litigation, responding to legal process, and pursuing legal rights and remedies;
- Safety and security: protecting the safety and security of individuals, including Colleagues, customers, and the general public, and the security of the Company's properties and assets, including physical assets and confidential information.
- Other: To carry out other purposes as part of our business activities when reasonably required by us.

Sensitive Personal Data

In some jurisdictions, where permitted by law, and with your consent where required under applicable law, the Company may Process certain categories of Personal Data that may be considered sensitive in certain jurisdictions ("Sensitive Personal Data"), including:

- Government issued identification numbers such as social security numbers, driver's licenses, state identification cards, and passport details.
- Precise geolocation information to track location of vehicles or Devices.
- Contents of communications including email, text messages, and chats transmitted using Devices used for work purposes, Devices connected to work systems or networks, or Company-managed accounts, as well as any other accounts we may have lawful access to. Communications that are personal and unrelated to Company business could potentially be accessed unintentionally as ancillary or incidental to a review focused on Company matters.
- Accident, health, and medical data, citizenship or immigration status, racial and/or ethnic data, sexual orientation, and gender identity to carry out obligations in the field of employment, benefits administration, insurance, social security, to facilitate accommodations, for inclusion and diversity assessment and program administration, and for the establishment or defense of legal claims.
- Biometric data, such as fingerprint or facial scans for verification, security and access control purposes

Personal Data about Family Members or other personal relationships

If a Colleague provides the Company with Personal Data (including Sensitive Personal Data)

about beneficiaries, domestic partners, family members or emergency contacts (collectively, "Colleague Contact(s)"), it is that Colleague's responsibility to provide such individuals a copy of this Notice in order to inform them of their rights. We will only Process the Personal Data of a Colleague Contact as necessary to administer benefits or communicate with the Colleague Contact about the Colleague or as needed, such as in the case of an emergency.

2. HOW WE STORE PERSONAL DATA AND WHO CAN ACCESS IT

The Company maintains Personal Data in various human resources and IT applications, including applications for payroll, benefits, talent management and performance management. The Company may maintain individual hard-copy personnel files. Access to Personal Data is restricted to those individuals who need such access for the purposes listed above or where required by law, including members of the Human Resources Department, the managers in the Colleague's line of business, and to authorized representatives of the Company's internal control functions such as Accounting, Compliance, Legal, and IT. Access may also be granted on a need-to-know basis to other Colleagues in the Company where relevant, such as if the Colleague is being considered for an alternative job opportunity, if a new manager appointed in the line of business needs to review files, or in connection with investigations.

3. DISCLOSURE AND INTERNATIONAL TRANSFERS OF PERSONAL DATA

The Company may disclose Personal Data to:

- Suppliers and service providers that support human resources and legal compliance functions, including to verify employment, conduct background checks, provide training, and process workplace claims;
- Suppliers and service providers to support business, administrative, and management functions. For example the Company may partner with third parties for recruiting, IT, consulting, legal counseling, professional advising, auditing, accounting, communications, or other purposes;
- Benefits administrators or service providers in connection with the provision of benefits, including retirement, health, life insurance, and other benefits under the terms of your employment;
- Individuals that you name as references, individuals that referred you for a position, or companies to whom you identify Convergint as a reference;
- Other Convergint subsidiaries and affiliated companies;
- Other businesses in connection with a merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings);
- Law enforcement, security, or governmental authorities to comply with laws, regulations, court orders, subpoenas, and similar requests;
- Convergint partners or customers, such as when a partner or customer requires a background check, substance testing, or other information in order for a Colleague to perform work for that customer.
- Entities or persons as needed to protect our legal rights, honor our legal obligations, and protect legitimate security or safety interests of colleagues, customers, or communities;
- Entities or persons as necessary to comply with a legal or regulatory obligations or requests, to promote safety or security, or otherwise to protect its rights or the rights of any third party.

4. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Given the global nature of the Company, we may (subject to applicable law) transfer Personal Data to other entities in the Convergint group of affiliated entities located in different countries. Such Personal Data may be transferred for the purposes set out above to recipients located outside the jurisdiction in which you are located. The recipients may be located in countries where data protection laws may not provide an equivalent level of protection to the laws in your home jurisdiction. The Convergint group of affiliated entities have entered into an intra group data transfer agreement which contains contractual commitments in order to promote protection of Personal Data when it is transferred between them.

5. ACCURACY

We use reasonable efforts to ensure that your Personal Information is kept as accurate, complete and up to date as possible. We do not routinely update your Personal Information, unless such an update is necessary. In order to help us maintain and ensure that your Personal Information is accurate and up to date, you must inform us, without delay, of any change in the information you provide to us.

6. SECURITY

The security of your information is important to us. The Company maintains appropriate administrative, technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data. These measures are aimed at promoting the on-going integrity and confidentiality of Personal Data. The Company evaluates these measures on a regular basis to promote the security of the processing.

7. DATA RETENTION

The Company will retain Personal Data in accordance with applicable legal requirements, and only for as long as necessary for the purposes described above or as long as required by law or to defend potential legal claims. The Company will retain Personal Data in accordance with any applicable data retention policies as updated from time to time, or as required or permitted by applicable law. Where appropriate, Convergint may de-identify or anonymize such Personal Information.

8. CONTACT INFORMATION

For any questions regarding this Notice or to exercise applicable privacy rights, contact Convergint's Data Protection Officer at dataprotectionofficer@convergint.com, submit your data privacy request via webform at https://www.convergint.com/about/contact-us/, specifying "Privacy Request – Attn: Legal" in the body of the request, or submit your data privacy request via toll-free number at 1-877-641-8181.

9. NOTICE UPDATES

You may request a copy of this Notice from us using the contact details set out above. This Notice may be revised periodically in our sole discretion, and any changes will be effective upon the revised Notice being updated in applicable Colleague Handbooks and on the Company intranet. If we make material changes we will notify you via email at the email address we have on file for you.

convergint

ANNEX I — CALIFORNIA PRIVACY

The information contained in this Annex applies if you are a Colleague in California. In the event of any inconsistency between the terms of this Annex and the terms of the main policy, the terms of this Annex shall prevail. As a California resident, you may make the following requests with respect to your Personal Data in accordance with applicable law:

- **Access** – Information about the categories of Personal Data; the categories of sources of that Personal Data; the business or commercial purposes for which we collect Personal Data; and the third parties to whom we disclose Personal Data is disclosed in Sections 1 and 3 of this Notice. You can request that we disclose to you, in a portable format, the categories of Personal Data collected about you, the categories of sources from which the Personal Data is collected, the categories of Personal Data sold or disclosed, the business or commercial purpose for collecting the Personal Data, the categories of third parties with whom we disclose the Personal Data, and the specific pieces of Personal Data collected about you over at least the past 12 months.
- **Deletion** – You can request that we delete your Personal Data that we maintain about you, subject to certain exceptions. We will delete or deidentify personal information that is not subject to a lawful exception from our records. Please be aware that there are a number of exceptions under the law under which we are not required or may be unable to delete your Personal Data.
- **Correction** – You can request that we correct your Personal Data, such as when the information is inaccurate, incomplete or no longer up to date.
- **Limit Use/Disclosure of Sensitive Personal Data** – You can request that we limit the use or disclosure of your Sensitive Personal Data for purposes incompatible with the disclosed purpose for which the Sensitive Personal Data was collected, subject to certain exceptions. We use Sensitive Personal Information only as it is necessary to perform the services for which it was collected, as described above.
- **Opt-out of Sale or Sharing** –We do not sell or share your personal information, as those terms are defined under California law. We have not sold or share any Personal Data with any third parties in the preceding 12 months. For purposes of this Section, “sell” means the sale, rental, release, disclosure, dissemination, availability, transfer, or other oral, written, or electronic communication of your Personal Data to an outside party for monetary or other valuable consideration and “sharing” means disclosure of Personal Data to third parties for cross-context behavioral advertising purposes, each subject to certain exceptions in applicable law.

In order to exercise the above rights, please submit a request using the contact methods provided below. Depending on your request, we may request certain information from you in order to verify your identity and residency. The verification steps will vary depending on the sensitivity of the Personal Data.

We may deny certain requests, or fulfil a request only in part, based on our legal rights and obligations. For example, we may retain Personal Data as permitted by law, such as for tax, unemployment benefits, or other record-keeping purposes, to administer benefits, or as part of an ongoing lawsuit. The Company will not discriminate against Colleagues, nor will Colleagues face any form of retaliation, for exercising their rights under this Section,

California residents may designate an authorized agent to make a request on their behalf. When submitting the request, please ensure the authorized agent is identified as an authorized agent and ensure the agent has the necessary information to complete the verification process. Depending on the sensitivity of the Personal Data in question, when using an authorized agent, we may need to verify the authenticity of the request directly with you.

ANNEX II: CANADIAN PRIVACY

The information contained in this Annex applies if you are a Colleague in Canada. In the event of any inconsistency between the terms of this Annex and the terms of the main policy, the terms of this Annex shall prevail. Depending upon the Canadian province in which you reside, you may have the following rights with respect to our use of your Personal Information:

- **Access and Mobility-** You may have the right to request whether we hold Personal Information on you and to request a copy of such information. To do so, please contact us at dataprotectionofficer@convergint.com. There are exceptions to this right, so that access may be denied if, for example, making the information available to you would reveal Personal Information about another person, or if we are legally prevented from disclosing such information. You may also have the right to request that computerized Personal Information collected from you be communicated to you in a commonly used technological format as well as to any person or body authorized by law to collect such information. This right does not extend to information that was created or inferred from your Personal Information and we are under no obligation to communicate such information if doing so raises serious practical difficulties.
- **Accuracy** - We aim to keep your Personal Information accurate, current, and complete. We encourage you to contact us at dataprotectionofficer@convergint.com to let us know if any Personal Information is not accurate or changes, so that we can update your Personal Information.
- **Withdraw Consent** - If you have provided your consent to the processing of your Personal Information, you may have the right to fully or partly withdraw your consent. To withdraw your consent please contact us at dataprotectionofficer@convergint.com. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you originally consented unless there is another legal ground for the processing.
- **Cessation of Dissemination and De-indexation** - You may have the right to request that we cease disseminating your Personal Information and/or de-index any hyperlink attached to your name if such actions are contrary to the law or a court order, or where the following conditions are met:
    - the dissemination of the information causes you serious injury in relation to your right to have your reputation or privacy respected;
    - the injury is clearly greater than the public's interest in knowing the information or the interest of any person's right to express themselves freely; and
    - the cessation of dissemination requested does not exceed what is necessary for preventing the perpetuation of the injury.
- **Re-indexation** - You may have the right to request that we re-index a link providing access to information where the following conditions are met:
    - a failure to do so causes you serious injury in relation to your right to have your reputation or privacy respected;
    - the injury caused by a failure to re-index is greater than the public's interest in knowing the information or the interest of any person's right to express themselves freely; and
    - the re-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury.
- **Complaints** - If you believe that your Personal Information protection rights may have been violated, you have the right to lodge a complaint with the applicable supervisory authority, or to seek a remedy thought the courts.

You may enquire about your Personal Information by contacting us at

dataprotectionofficer@convergint.com. We will generally respond to all access requests within 30 days of the receipt of all necessary information. In circumstances where we are not able to provide access, or if additional time is required to fulfill a request, we will advise you in writing. We may not release certain types of information based upon exemptions specified in applicable laws. Where possible, we will sever the information that will not be disclosed and provide you with access to the remaining information. Should we be unable to provide access to or disclose Personal Information to you, we will provide you with an explanation, subject to restrictions. In certain circumstances, such as where the request is excessive or unfounded, we may charge you an administration fee for access to your Personal Information. We may also charge for additional copies. We will advise you of any fees before proceeding with a request.

ANNEX III: EUROPEAN PRIVACY

The information contained in this Annex applies if you are a Colleague in the UK, European Economic Area, or Switzerland. In the event of any inconsistency between the terms of this Annex and the terms of the main policy, the terms of this Annex shall prevail.

1. LAWFUL BASIS

Under certain privacy laws, including GDPR, we must have a lawful basis for the processing of your Personal Data. As further described above, the Company uses your personal information for the following lawful bases:

- **Legitimate business purposes:** where we have a legitimate business interest to perform processing on your personal information provided your interests and fundamental rights do not override those interests.
- **Contractual:** we may need to process your personal information to provide a product or service you request or hire you to work for as an employee or contractor.
- **Legal obligations:** there is a legal and/or regulatory obligation to process your personal information and we must comply.
- **Consent:** in limited circumstances, we may ask you to provide your consent for us to process your personal information and where this is provided you have a right to withdraw this at any time.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

As explained elsewhere in this Notice, sensitive data is subject to requirements that are more restrictive. We may process sensitive data in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment, such as in relation to employees with disabilities.
- Where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme.
- Where it is necessary to protect you or another person from harm.
- Where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public

2. RIGHTS

You have certain rights under European privacy laws. These rights are set out below. Please note, however, that these are not absolute rights and there are limits to them and some may not be available to you in respect of all Personal Data.

- **Information** - You have the right to be provided with clear, transparent and easily understandable information about how we use your information and your rights. This is why we're providing you with the information in this Notice.
- **Access** - You have the right to obtain access to your information (if we are processing it), and certain other information (similar to that provided in this Notice). This is so you're aware and can check that we're using your information in accordance with data protection law
- **Deletion** - This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of your Personal Data where there is no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.
- **Correction** - You are entitled to have your information corrected if it is inaccurate or incomplete.
- **Consent** – If you have given your consent to any processing activity then you have a right to withdraw such consent. As explained in section 3 above however we do not generally rely on consent as a lawful basis for processing.
- **Restriction** - You have the right to restrict some processing of your Personal Data, which means that you can ask us to limit what we do with it.
- **Objection** - You have the right to object to certain types of processing, including processing based on our legitimate interests in some cases.
- **Portability** - You have rights to obtain and reuse your Personal Data for your own purposes across different services.
- **Complaints** - You may submit a complaint to your local supervisory authority.

To make such a request or lodge an objection, please send an email to **dataprotectionofficer@convergint.com**.

You may also be eligible to lodge a complaint with the competent data protection authority. The names and contact details of the Data Protection Authorities in the European Union can be found at **http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm**. The Data Protection Authority for the United Kingdom is the Information Commissioner's Office, and their contact details can be found at https://ico.org.uk/global/contact-us/. The Swiss Authority is the FDPIC and their contact details can be found at https://www.edoeb.admin.ch/edoeb/en/home.html.

ANNEX IV: ASIA PRIVACY

If you are outside of China and India, please contact dataprotectionofficer@convergint.com to inquire about the privacy rights that may be available to you.

For residents of China and India, this section provides information about the lawful basis by which we process your Personal Information, your privacy rights, Sensitive Personal Data, and Cross-Border Data Transfers. In the event of any inconsistency between the terms of this Annex and the remainder of the Notice, the terms of this Annex shall prevail.

1. LAWFUL BASIS

China	India
We collect and use your Personal Data only when it is necessary for the purposes mentioned above in this Notice. Depending on the circumstance, we may rely on one or more of these lawful basis: • **Your consent** - where we obtain your consent. • **Human resource management** - where it is necessary for implementation of human resources management in accordance with this policy and other employment handbooks. • **Statutory obligations** - where it is necessary for the performance of statutory duties or statutory obligations. • **Emergency** - where it is necessary for the response to a public health emergency or for the protection of the life, health and property safety in an emergency. • **Personal data disclosed by you** - where you have disclosed your Personal Data or your Personal Data has been disclosed to the public. • Others provided by the PIPL and applicable Chinese laws and regulations.	We process your Personal Data only in accordance with the applicable laws and regulations and for a lawful purpose: • for which you have given your consent; or • for certain legitimate uses, including: - for the specified purpose for which you have voluntarily provided your Personal Data to us, and in respect of which you have not indicated to us that you do not consent to the use of your Personal Data; - for the purposes of employment or those related to safeguarding us from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by employee; or - to comply with a legal or regulatory obligation.

2. SENSITIVE PERSONAL DATA

We may process your Sensitive Personal Data listed above. Where required by the applicable laws and regulations, we will obtain your separate consent.

3. CROSS-BORDER DATA TRANSFER

In order to carry out global management of human resource operations, global projects, and business administration, Convergint's group of affiliated entities utilize unified or interconnected IT systems to process your Personal Data. Therefore, it is necessary for Company to transfer your Personal Data outside China or India to Convergint's group of affiliated entities that are located elsewhere. We will implement appropriate mechanisms for cross-border data transfer and conduct relevant procedures where required by the applicable laws and regulations. We will keep you informed of the relevant information on the cross-border data transfer and obtain your separate consent, if required by applicable laws and regulations.

4. RIGHTS

China	India

You have certain rights under the Personal Information Protection Law of China ("PIPL") and other applicable Chinese laws and regulations. These rights are set out below: • **Right to know** - You have the right to know and make decisions on the processing of your Personal Information. • **Right to refuse** - You have the right to restrict or refuse others to process your Personal Information. • **Right to access** - You have the right to consult or copy your Personal Information. • **Right to transfer** - You have the right to request us to transfer your Personal Information to other parties designated by you, to the extent permitted by the applicable laws and regulations. • **Right to correct** - You have the right to request us to make corrections or supplements, in case you find that your Personal Information is inaccurate or incomplete. • **Right to delete** - You have the right to delete your Personal Information provided to us, but where the retention period prescribed by the applicable laws and regulations has not expired, or it is technically difficult to delete the Personal Information, we will cease the processing of the Personal Information, except for the storage and any necessary measure taken for security protection. • **Right for explanation** - You have the right to request us to explain our rules for processing Personal Information.	You have certain rights under the Digital Personal Data Protection Act ("DPDP Act") and other applicable Indian laws and regulations. These rights are set out below: • **Right to access information about Personal Data** - To the extent permitted by the applicable laws and regulations, you have the right to request us providing a summary of Personal Data processed by us, the identities of other data fiduciaries and data processors with whom we shared your Personal Data and a description of your Personal Data shared, and any other information related to your Personal Data, provided you have given your consent for us to processing such Personal Data; • **Right to correction and erasure of Personal Data** - You have the right to correction, completion, updating and erasure of your Personal Data of which you have previously given consent. • **Right to withdraw consent** - You have the right to withdraw consent from processing of your Personal Data at any time after you have provided your consent to us. • **Right of grievance redressal** - You have the right to have readily available means of grievance redressal provided by us in respect of any act or omission made by us regarding the performance of our obligations in relation to your Personal Data or the exercise of your rights. • **Right to nominate** - You have the right to nominate any other individual, who shall, in the event of your death or incapacity, exercise the rights of the data principal.

ANNEX V: OCEANIA

If you are outside of Australia and New Zealand, please contact dataprotectionofficer@convergint.com to inquire about the privacy rights that may be available to you.

For residents of Australia and New Zealand, you have the right to request access or correction to your Personal Information held by Convergint, or to make a complaint about the way we have handled your Personal Information. To seek access to your Personal Information or to make a complaint, please email dataprotectionofficer@convergint.com providing your name and contact details, and explaining the request or complaint. Convergint will endeavour to provide a response within 30 calendar days of becoming aware of a request. Convergint may decline a request in certain circumstances in accordance with applicable laws, including if there are existing or

anticipated legal proceedings between Convergint and the person requesting it, or another identified third party.

If you are not satisfied with Convergint's response, Australians may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) by calling 1300 363 992 or visiting the OAIC's website at https://www.oaic.gov.au/. If you are in New Zealand, please contact the New Zealand Privacy Commissioner via their website at https://www.privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/.