



## POLICY: COLLEAGUE & APPLICANT PRIVACY NOTICE

**Last Updated:** March 15, 2026

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 third party Privacy Policy located at <https://www.convergint.com/privacy/>.

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](#).
- Annex 6 contains [additional information specific to Colleagues in Latin America \(Argentina, Chile, Columbia, Mexico, and Brazil\)](#).
- Annex 7 contains [additional information specific to Colleagues in the Middle East](#).

Residents of other regions may contact [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com) with any questions about how we process Personal Data.

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

#### *How we collect Personal Data*

“**Personal Data**” means any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, to an identified or identifiable individual, or that is otherwise defined as personal data, personal information, or a similar term under applicable privacy or data protection laws. 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 Data 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 process your application for employment and/or 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 Data in order to exercise your statutory rights, such as statutory leave entitlements. Failing to provide such Personal Data 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 Data, 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@convergent.com](mailto:dataprotectionofficer@convergent.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; and communicating with applicants about applications and opportunities. We may communicate with applicants through channels corresponding with the information applicants provide — e.g., through email, phone, or SMS / text messaging. Where particular types of communication require consent by applicable law, we will obtain such consent.



- 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 Data and increase the efficiency and effectiveness of human resources review and analysis. We do not make decisions with legal or similarly significant effects based only on automation.
- 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 Convergent as a reference;
- Other Convergent 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;
- Convergent 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 Convergent 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 Convergent 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.

Where required, we rely on appropriate transfer mechanisms, such as adequacy decisions or standard contractual clauses, for international transfers. We assess local laws and apply supplementary measures where needed.

#### **5. ACCURACY**

We use reasonable efforts to ensure that your **Personal Data** is kept as accurate, complete and up to date as possible. We do not routinely update your **Personal Data**, unless such an update is necessary. In order to help us maintain and ensure that your **Personal Data** 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, Convergent may de-identify or anonymize such Personal Data.



## 8. OPT OUT OF TEXT MESSAGING (US APPLICANTS)

You may have the opportunity to receive text messages from or on behalf of Convergent from time to time. U.S. applicants that do not wish to continue receiving text message from or on behalf of Convergent may text the applicable Short Code or directly reply to any message received from or on behalf of Convergent with the appropriate Short Code (e.g., STOP, QUIT, END, REVOKE, OPT OUT, CANCEL, or UNSUBSCRIBE) to opt out of receiving future text messages. You may receive an additional mobile message confirming your decision to opt out.

## 9. CONTACT INFORMATION

For any questions regarding this Notice or to exercise applicable privacy rights, contact Convergent's Data Protection Officer at [dataprotectionofficer@convergent.com](mailto:dataprotectionofficer@convergent.com), submit your data privacy request via webform at <https://www.convergent.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.

## 10. 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.

## 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 Data 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 Data 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 Data, 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 Data:

- **Access and Mobility**- You may have the right to request whether we hold Personal Data on you and to request a copy of such information. To do so, please contact us at [dataprotectionofficer@convergint.com](mailto: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 Data about another person, or if we are legally prevented from disclosing such information. You may also have the right to request that computerized Personal Data 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 Data and we are under no obligation to communicate such information if doing so raises serious practical difficulties.
- **Accuracy** - We aim to keep your Personal Data accurate, current, and complete. We encourage you to contact us at [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com) to let us know if any Personal Data is not accurate or changes, so that we can update your Personal Data.



- **Withdraw Consent** - If you have provided your consent to the processing of your Personal Data, you may have the right to fully or partly withdraw your consent. To withdraw your consent please contact us at [dataprotectionofficer@convergint.com](mailto: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 Data 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 Data protection rights may have been violated, you have the right to lodge a complaint with the applicable supervisory authority, or to seek a remedy through the courts.

You may enquire about your Personal Data by contacting us at [dataprotectionofficer@convergint.com](mailto: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 Data 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 Data. 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 Data for the following lawful bases:

- **Legitimate business purposes:** where we have a legitimate business interest to perform processing on your Personal Data provided your interests and fundamental rights do not override those interests.
- **Contractual:** we primarily process your Personal Data to fulfill contracts, including payroll, onboarding and performance reviews.
- **Legal obligations:** there is a legal and/or regulatory obligation to process your Personal Data and we must comply.
- **Consent:** in limited circumstances, we may ask you to provide your consent for us to process your Personal Data and where this is provided you have a right to withdraw this at any time. You will be provided with additional information on what processing this relates to when we ask for your consent.

We do not make decisions with legal or similarly significant effects based only on automation.

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 Colleagues 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 as detailed further below. If you are a UK based Colleague, you have additional rights under local law to complain directly to us using the email address below.

To make such a request or lodge an objection, please send an email to [dataprotectionofficer@convergent.com](mailto:dataprotectionofficer@convergent.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](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@convergent.com](mailto:dataprotectionofficer@convergent.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 Data, your privacy rights, Sensitive Personal Data, and Cross-Border Data Transfers under applicable law, including the PRC Personal Data Protection Law (PIPL), the Indian Digital Personal Data Protection Act, 2023 (DPDP Act), and rules and regulations issued thereunder. 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
<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Your consent</b> - where we obtain your consent.</li> <li>• <b>Human resource management</b> - where it is necessary for implementation of human resources management in accordance with this policy and other employment handbooks.</li> <li>• <b>Statutory obligations</b> - where it is necessary for the performance of statutory duties or statutory obligations.</li> <li>• <b>Emergency</b> - where it is necessary for the response to a public health emergency or for</li> </ul>	<p>We process your Personal Data only in accordance with the applicable laws and regulations and for a lawful purpose:</p> <ul style="list-style-type: none"> <li>• for which you have given your consent; or</li> <li>• for certain legitimate uses, including: <ul style="list-style-type: none"> <li>- 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;</li> <li>- for the purposes of employment or those related to safeguarding us from loss or liability, such as prevention of corporate espionage,</li> </ul> </li> </ul>



<p>the protection of the life, health and property safety in an emergency.</p> <ul style="list-style-type: none"> <li>• <b>Personal data disclosed by you</b> - where you have disclosed your Personal Data or your Personal Data has been disclosed to the public.</li> <li>• Others provided by the PIPL and applicable Chinese laws and regulations.</li> </ul>	<p>maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by employee; or</p> <ul style="list-style-type: none"> <li>- to comply with a legal or regulatory obligation.</li> </ul>
--	--

## 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. For clarity, some laws (such as the DPDP Act) do not regulate Sensitive Personal Data as a separate statutory category.

## 3. CROSS-BORDER DATA TRANSFER

In order to carry out global management of human resource operations, global projects, and business administration, Convergent’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 Convergent’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
<p>You have certain rights under the Personal Data Protection Law of China (“PIPL”) and other applicable Chinese laws and regulations. These rights are set out below:</p> <ul style="list-style-type: none"> <li>• <b>Right to know</b> - You have the right to know and make decisions on the processing of your Personal Data.</li> <li>• <b>Right to refuse</b> - You have the right to restrict or refuse others to process your Personal Data.</li> <li>• <b>Right to access</b> - You have the right to consult or copy your Personal Data.</li> <li>• <b>Right to transfer</b> - You have the right to request us to transfer your Personal Data to other parties designated by you, to the extent permitted by the applicable laws and regulations.</li> <li>• <b>Right to correct</b> - You have the right to request us to make corrections or supplements,</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Right to access information about Personal Data</b> - 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;</li> <li>• <b>Right to correction and erasure of Personal Data</b> - You have the right to</li> </ul>



in case you find that your Personal Data is inaccurate or incomplete.

- **Right to delete** - You have the right to delete your Personal Data 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 Data, we will cease the processing of the Personal Data, 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 Data.

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. If you are not satisfied with our response to your grievance, you may escalate your complaint to the Data Protection Board of India, in accordance with applicable law.

- **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](mailto: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 Data held by Convergint, or to make a complaint about the way we have handled your Personal Data. To seek access to your Personal Data or to make a complaint, please email [dataprotectionofficer@convergint.com](mailto: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.

Personal Data may be disclosed to related Convergint entities and service providers located overseas. Where this occurs, Convergint takes reasonable steps to ensure overseas recipients handle Personal Data in accordance with applicable privacy laws.

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/>.

## ANNEX VI: LATAM

### ARGENTINA



If you are a resident of Argentina, you have certain rights under the Personal Data Protection Law No. 25,326 ("PDPL"), its Regulatory Decree No. 1558/2001, supplementary rules and regulations issued by the Argentine data protection authority, as set forth below. This section applies to both individuals and legal entities whose data is being processed.

**Data Controller.** The data controller responsible for the processing of your Personal Data is Seal Solucion de Integracion SRL, with registered address at Argentina.

**Provision of Personal Data.** Providing Personal Data is voluntary; however, failure to provide certain information, or providing false or inaccurate information, may hinder our ability to administer the rights and obligations essential to our employment relationship with you, or to enable you to exercise your statutory rights.

**Lawful Basis:** Under the PDPL, we must have a lawful basis for the processing of your Personal Data. Depending on the circumstance, we may rely on one or more of these legal bases:

- **Your consent** - where we obtain your prior, express, and informed consent. By reading and acknowledging this Policy, you hereby provide your consent to our processing of your Personal Data in accordance with this Policy.
- **Unrestricted public-access sources** - where your Personal Data is obtained from publicly available sources.
- **Legal obligation** - where it is necessary to comply with applicable government powers or by virtue of a legal obligation.
- **Basic identifying data** - where your Personal Data consists of lists limited to name, identity document, taxpayer or pension identification number, occupation, date of birth, and domicile.
- **Contractual relationship** - where your Personal Data arises from a contractual, scientific, or professional relationship with you, and it is necessary for the development or fulfillment of such relationship.

**International Data Transfer:** Where the transfer of your Personal Data to third parties located outside Argentina is required, please note that such countries may not offer levels of personal data protection equivalent to those provided under the PDPL in Argentina. By accepting this Privacy Policy, you expressly consent to such international data transfer, if necessary.

**Privacy Rights:** If you are a resident of Argentina, you have the following rights under the PDPL:

- **Information** - You have the right to be informed, prior to the collection of your data, of the purpose of the processing and its recipients, the existence of the database, the identity and domicile of the data controller, whether providing the information is mandatory or voluntary, and the consequences of providing or refusing to provide your data.
- **Access** - You have the right to obtain access to your Personal Data within ten (10) calendar days of your request.
- **Rectification, Update, and Deletion** - You have the right to request the rectification, update,



or deletion of your Personal Data when it is inaccurate, incomplete, outdated, or no longer necessary for the purpose for which it was collected. The data controller must proceed within five (5) business days of receiving the request. Deletion shall not proceed when it may cause harm to the rights or legitimate interests of third parties, or when there is a legal obligation to retain the data.

- **Confidentiality** - You have the right to request that your Personal Data be treated as confidential.
- **Complaints** - THE AGENCY FOR ACCESS TO PUBLIC INFORMATION, in its capacity as Control Authority of the PDPL, has the power to deal with complaints and claims filed by those affected in their rights for breach of the regulations in force regarding the protection of personal data.

To exercise your rights, please send an email to [dataprotectionofficer@convergent.com](mailto:dataprotectionofficer@convergent.com) specifying your request and providing details to verify your identity.

## CHILE

If you are a resident of Chile, the following information is applicable to you. Convergent Chile Servicios de Integración SpA, RUT 76.962.871-1, legally represented by Andrea Gutiérrez Rojas, national identity card N° 12.722.406-4, domiciled in the city of Santiago, Las Condes, Cerro El Plomo 5855, Office 307, processes your personal data in accordance with Law N°19.628 on the Protection of Private Life and its amendments introduced by Law N°21.719 on Personal Data Protection (together the "Personal Data Protection Law" or "LPDP"), Chile's Political Constitution and other applicable regulations.

During the legal vacancy period prior to the full entry into force of Law N°21.719, Convergent will apply the standards introduced by said law to the greatest extent possible, in accordance with the implementation regime established by Chilean regulations.

### Lawful basis for processing:

According to the LPDP, the processing of your personal data must be justified on a lawful basis recognized by law. Depending on the processing operation in question, Convergent may invoke the following lawful bases:

- **Consent:** When you have given your free, informed, specific, and unambiguous consent for the processing of your Personal Data for one or more specific purposes. When the processing is based on your consent, you have the right to revoke it at any time, without affecting the lawfulness of the processing carried out prior to said revocation (Art. 12, LPDP).
- **Execution or performance of a contract:** When the processing is necessary for the execution or performance of a contract to which you are a party, or for the adoption of pre-contractual measures at your request (Art. 13 c), LPDP).
- **Compliance with a legal obligation:** When the processing is necessary to comply with a legal or regulatory obligation applicable to Convergent (Art. 13 b), LPDP).

- **Necessity of the processing for preventive or occupational medicine purposes, the assessment of the applicant's working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services:** In order to determine your working capacity and make an informed decision during the selection process, we will process your health data. This includes medical examination results and psychological, psychosocial, or psychometric assessments as required. The processing of these personal data is justified for occupational medicine purposes and to evaluate the applicant's working capacity (Art. 16 bis e, LPDP).
- **To safeguard the life, physical integrity, or mental health of the data subject or another person; or when the data subject is physically or legally incapable of giving consent:** For example, in the event of a health crisis involving a collaborator of such magnitude that it is not possible to obtain their consent, for the purpose of taking them to the nearest medical care center (Art. 16 bis a, LPDP).
- **Legitimate interests:** When the processing is necessary for the satisfaction of legitimate interests of Convergent or a third party, provided that this does not affect the rights and freedoms of the data subject. When this basis is invoked, Convergent must carry out the corresponding proportionality assessment, and you may request information at any time regarding the legitimate interest that justifies it (Art. 13 d), LPDP). This basis will be fully available upon the entry into force of Law N° 21.719.
- **Formulation, exercise or defense of rights in court:** When the processing is necessary for the formulation, exercise or defense of a right before courts of justice or public bodies (Art. 13 e), LPDP).

The Personal Data processed, sources from which we obtain Personal Data, our data processing activities and purposes, data transfers, data protection measures, and data retention practices are described in the main portion of this Policy, above.

#### **Attendance control and geolocation data:**

Convergent may establish measures for recording time, attendance, and punctuality using techniques based on the processing of biometric, image, and/or geolocation personal data. Such processing activities shall be based on the specific consent of the collaborator, which will have been previously obtained in the Employment Contract and its respective Annexes. We will duly inform the worker in each case regarding the identification of the biometric system used, the duration for which the processed personal data will be retained, and the mechanisms and procedures through which the worker may exercise their rights.

The aforementioned data may be communicated or transferred to third-party service providers for the operation of time, attendance, and punctuality control systems, in strict compliance with the LPDP.

#### **Use of security cameras:**

To meet the needs and requirements of the activities carried out by Convergent, and/or to ensure the safety of workers and company assets, we may install security cameras on our premises. This will be conducted in strict adherence to current labor legislation.



Any personal data collected through the use of such surveillance systems shall be justified by the necessity of the processing for the compliance of legal obligations regarding the worker, and its purpose shall be to guarantee the safety of workers, Convergent's assets, and its activities.

In the framework of fulfilling its legal duties, Convergent will adopt the relevant technical and organizational measures to safeguard the security and confidentiality of the collected personal data. Images or recordings may be destroyed or completely deleted after a reasonable retention period; in no event may they be stored indefinitely, unless there is a judicial order or equivalent requiring us to retain them for a longer period, after which they will be duly deleted.

### **Data subjects rights concerning the processing of their personal data:**

If you reside in Chile, you are entitled to the following rights regarding the processing of your personal data. Please note that the exercise of these rights are subject to the conditions and exceptions established by the LPDP:

- **Right of access:** You may request confirmation as to whether your personal data is being processed and, if so, obtain a copy of such data and information regarding: the purposes of the processing; the categories of recipients to whom the data has been or will be communicated or transferred; the retention period; the source of the data; and, when processing is based on legitimate interest, what these interests are (Art. 5, LPDP).
- **Right to rectification:** You may request that we rectify your personal data when it is inaccurate, outdated, or incomplete (Art. 6, LPDP).
- **Right to erasure:** You may request the deletion of your personal data under certain circumstances, including, among others, when it is no longer necessary for the purposes for which it was collected, when you have withdrawn your consent and there is no other legal basis for the processing, or when the data has been processed unlawfully (Art. 7, LPDP).
- **Right to object:** You may object to the processing of your personal data in certain cases, particularly when the processing is based on Convergent's legitimate interest or when the data has been obtained from publicly accessible sources (Art. 8, LPDP).
- **Right to object automated individual decision-making:** You may object to decisions based solely on the automated processing of your personal data—including profiling—that produce legal effects concerning you or significantly affect you, unless one of the legal exceptions applies (Art. 8 bis, LPDP).
- **Right to restriction of processing:** You may request the temporary suspension of the processing of your personal data while a request for rectification, erasure, or objection is pending resolution (Art. 8 ter, LPDP).
- **Right to data portability:** When processing is carried out by automated means and is based on your consent, you may request to receive your personal data in a structured, commonly used, and machine-readable electronic format, and request that it be transmitted directly to another data controller where technically feasible (Art. 9, LPDP).
- **Right to withdraw consent:** When processing is based on your consent, you may withdraw



it at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Art. 12, LPDP).

### **How to exercise your rights:**

To exercise any of the rights described above, please send a written request to [dataprotectionofficer@convergent.com](mailto:dataprotectionofficer@convergent.com). Your request must include: your full name, the specific right you wish to exercise and information that allows for the identification of the personal data or the processing to which your request refers. Where applicable, you may attach supporting documentation for your request. Convergent will acknowledge receipt of your request and provide a written response within 30 calendar days following the date of receipt of all necessary documentation. This period may be extended once for up to an additional 30 calendar days when required by the complexity or volume of the requests, in which case you will be notified in a timely manner.

When required by law, Convergent will take reasonable measures to verify the applicant's identity before processing the request.

### **Right to complain to the authority:**

If you consider that the processing of your personal data does not comply with the applicable regulations, you have the right to complain with the competent personal data protection authority in Chile. Once it comes into force, this authority will be the Personal Data Protection Agency (APDP). During the transition period prior to December 1, 2026, supervisory functions will be exercised in accordance with the current institutional framework.

Additionally, you may file a judicial claim directly before the competent Court of Appeals should you consider that an administrative act or a final resolution issued by the APDP is unlawful.

## **COLOMBIA**

If you are located in Colombia, your Personal Data is processed in accordance with the Ley 1581 de 2012 and its regulatory decrees.

The data controller is CONVERGINT COLOMBIA SERVICIOS DE INTEGRACIÓN S.A.S., with registered address in Bogotá D.C., Colombia.

You have the right to:

- Access your Personal Data
- Update and rectify inaccurate data
- Request deletion when applicable
- Revoke authorization where legally permitted
- File complaints before the Superintendencia de Industria y Comercio



Requests may be submitted to: [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com)

## **MÉXICO**

If you are a Colleague or job applicant in Mexico, this Annex applies to you. In the event of any inconsistency between this Annex and the main Notice, this Annex shall prevail. Convergint processes Personal Data in accordance with the Ley Federal de Protección de Datos Personales en Posesión de los Particulares, its Regulations, and other applicable Mexican data protection laws (the “Mexican Data Protection Law”).

### **Data Controller**

The data controller is the applicable Convergint entity employing you or receiving your application in Mexico (the “Controller”).

### **ARCO Rights**

Under Mexican law, you have the right to:

- Access your Personal Data and information regarding its processing;
- Rectify inaccurate or incomplete data;
- Cancel your Personal Data when legally applicable;
- Object to the processing of your Personal Data for legitimate reasons;
- Revoke your consent to the extent permitted by law.

To exercise these rights, please contact: [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com). Your request must include your name, proof of identity (or legal representation), a clear description of the data concerned, and a contact method to receive our response. Requests will be handled within the timeframes established by applicable law.

### **Sensitive Personal Data**

Where required, the Controller will obtain express consent for the processing of Sensitive Personal Data, as defined under Mexican law.

### **Transfers**

Personal Data may be transferred nationally or internationally in accordance with the main Notice. Where required by Mexican law, your consent will be obtained prior to such transfers, unless a legal exception applies.

### **Complaints**

If you believe your data protection rights have been violated, you may file a complaint before the Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

## **BRAZIL**

If you are a Colleague or job applicant in Brazil, this Annex applies to you. In the event of any



inconsistency between this Annex and the main Notice, this Annex shall prevail regarding the processing of Personal Data subject to the Brazilian General Data Protection Law (Law No. 13,709/2018 or “**LGPD**”).

The processing of personal data will be carried out by **Convergent Comércio e Serviços de Tecnologia Ltda (CNPJ: 58.619.404/0001-48)**.

In case of questions or for clarifications regarding the processing of personal data, please contact the Data Protection Officer (“DPO”) appointed at <https://convergent.com.br/lgpd/>, via email at [privacidade-br@convergent.com](mailto:privacidade-br@convergent.com)

## **LAWFUL BASIS**

The Company processes your Personal Data in strict compliance with the legal bases set forth in the LGPD. Depending on the context of the processing, we rely on:

- Performance of a Contract or pre-contractual procedures: For recruitment, hiring, employment management, payroll, and benefits administration.
- Compliance with Legal or Regulatory Obligations: Specifically regarding labor laws, tax, social security (including, where applicable, reporting systems such as eSocial), and occupational health and safety (e.g., ASO/PCMSO).
- Regular Exercise of Rights: For use in judicial, administrative, or arbitration proceedings.
- Legitimate Interests: For security, monitoring of corporate assets, internal governance and fraud prevention, subject to necessity and proportionality assessments.
- Protection of life or physical safety: Where relevant
- Consent: Where required by law for specific activities, such as certain marketing uses or geolocation tracking on personal devices. Where consent is relied upon, you have the right to withdraw it at any time, subject to legal or contractual limitations.

## **SENSITIVE PERSONAL DATA AND MINORS**

- Sensitive Data: Processing of sensitive data (e.g., health data, biometrics, union membership, racial/ethnic origin, religious belief, political opinion, or sexual orientation) is limited to the minimum necessary to comply with legal or regulatory obligations, when necessary for fraud prevention, compliance investigations, or risk mitigation, when required for access control and security measures (including biometric systems, where applicable); or based on specific and highlighted consent, where legally required.
- Data of Minors: When processing Personal Data of your dependents who are minors (e.g., for health insurance or family benefits), such data must be provided by a parent or legal guardian in the best interest of the minor.

## **BRING YOUR OWN DEVICE (BYOD)**





Where Colleagues use personal devices for professional purposes under the Company's Bring Your Own Device ("BYOD") program, Personal Data may be processed to ensure information security, protection of confidential data, access control, time tracking (where applicable), and compliance with internal policies. Such processing:

- Is limited to what is strictly necessary and proportionate to the intended business purpose;
- Does not involve unrestricted access to personal content unrelated to professional activities;
- Is based on an appropriate lawful basis under the LGPD, such as contractual necessity, legal obligation, or legitimate interest, as applicable;
- May be formalized in employment agreements or related contractual annexes, where required;
- Is subject to technical and organizational safeguards designed to protect the Colleague's privacy.

Where biometric systems, geolocation or device management tools are implemented on personal devices, their use will be restricted to professional contexts and in accordance with Brazilian data protection and labor regulations.

## **INTERNATIONAL DATA TRANSFERS**

Personal Data may be transferred outside Brazil, including to other Convergent group entities or cloud service providers. Under the LGPD, international transfers may occur only when:

- The destination country provides an adequate level of protection recognized by the ANPD; or
- Appropriate safeguards are implemented, including standard contractual clauses or other mechanisms approved by the ANPD; or
- Another legal basis under the LGPD applies.

Use of cloud infrastructure hosted outside Brazil constitutes an international data transfer under Brazilian law. Appropriate technical, organizational, and contractual safeguards are implemented to protect such transfers.

## **RIGHTS**

Under the LGPD, you have the right to:

- Confirmation of the existence of processing;
- Access to Personal Data;
- Correction of incomplete, inaccurate, or outdated data;
- Anonymization, blocking, or erasure of unnecessary or excessive data, or data processed in



non-compliance with the LGPD.

- Data Portability to another service provider upon express request, where technically feasible and as regulated by the ANPD;
- Deletion of data processed based on consent (subject to legal retention obligations);
- Information about public and private entities with which data the Controller has shared your Personal Data.
- Information about the possibility of denying consent and consequences thereof;
- Revocation of consent.
- Review of automated decisions made solely based on the automated processing of personal data that affect your interests.

Requests may be submitted to [privacidade-br@convergent.com](mailto:privacidade-br@convergent.com). We may require identity verification prior to fulfilling any request, and certain requests may be denied where the retention of Personal Data is required by applicable law, including labor, tax, social security, or statutory limitation obligations.

Upon request, you may also obtain information regarding the specific purposes of processing, the form and duration of processing (subject to trade secret limitations), and the identification and responsibilities of processing agents, as required under the LGPD.

You also have the right to lodge a complaint with the Brazilian Data Protection Authority (ANPD).

## **DATA RETENTION**

Personal Data is retained in accordance with applicable Brazilian legal and regulatory requirements.

Brazilian labor and tax regulations impose mandatory retention periods for certain employment-related records, which may extend for several years after termination of employment.

Where retention is required for compliance with legal obligations or for the regular exercise of rights, deletion requests may not be immediately fulfilled.

## **DATA BREACH NOTIFICATION**

Under the LGPD, security incidents that may result in relevant risk or damage to data subjects must be communicated to the ANPD and, where applicable, to affected individuals.

Convergent maintains procedures to assess, manage, and notify security incidents in accordance with Brazilian law.

## **ANNEX VI: Middle East**





If you are outside of the Kingdom of Saudi Arabia, please contact [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com) to inquire about the privacy rights that may be available to you. If you are a resident of KSA, we are required to provide you with details of the lawful bases for processing we rely on of your Personal Data and let you know about certain privacy rights.

**Lawful Basis:** The lawful bases we rely on when we collect Personal Data directly from Colleagues are as follows:

- a. with your consent
- b. to comply with a legal or regulatory obligation; and
- c. pursuant to a contract in place between us and our Colleagues.

The lawful bases we rely on when we do not collect Personal Data directly from our Colleagues are as follows:

- a. where the Personal Data is publicly available or collected from a publicly available source;
- b. where not collecting or processing of the Personal Data may harm or affect the Colleague's vital interests; and
- c. where the Colleague's Personal Data is recorded or stored in a form that makes it impossible to identify them, directly or indirectly.

Regardless of whether we collect Personal Data from the Colleagues or from a third party, we may also process it for our legitimate interests. Those legitimate interests are described in the main Policy, above.

We only rely on Colleagues' consent if and to the extent to which one of the lawful bases set out above are not available for a particular processing activity.

**Privacy Rights:** If you are outside of the Kingdom of Saudi Arabia, please contact [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com) to inquire about the privacy rights that may be available to you.

Colleagues in the KSA have certain rights under the KSA PDPL. These rights are set out below. Please note, however, that these are not absolute rights. There are limits to them and some may not be available to in respect of all Personal Data processed by the Company.

**Information** - You have the right to be provided with information about how we use your information and your rights. This is why we are providing you with the information in this Policy.

**Access** - You have the right to obtain access and obtain a copy of your Personal Data (if we are processing it), and certain other information (similar to that provided in this Policy).

**Destruction (Erasure)** – This right 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 Personal Data 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.

**Objection** - You have the right to object to certain types of processing, including processing for direct marketing purposes.

To make such a request or lodge such an objection, please send an email to [dataprotectionofficer@convergint.com](mailto:dataprotectionofficer@convergint.com).

We will generally respond to all requests to exercise data subject rights within 30 days of the receipt of all necessary information. In circumstances where we are not able to fulfil your request, or if additional time is required to fulfill a request, we will advise you in writing. Should we be unable to fully meet your request (if, for example, your Personal Data is connected with that of another individual, making it impossible to separate without disclosing that individual's Personal Data), we will provide you with an explanation, to the extent permitted under applicable law.

Where appropriate or required by law, we will take reasonable steps to verify your identity prior to responding to your requests. The verification steps may vary depending on the sensitivity of the Personal Data.