convergint

POLICY: COLLEAGUE DATA PROTECTION NOTICE

Last Updated: April 15, 2024

Convergint Technologies LLC ("Company", "we") has prepared this Colleague Data Protection Notice ("Notice") to describe the Company's practices regarding the collection, use, storage, disclosure, and transfer (collectively, “Process” or “Processing”) of information from which Company’s Colleagues can be identified, whether directly or indirectly ("Personal Data"). This Notice does not apply for data collected by the Company from non-Colleagues, or data collected from Colleagues in a non-employment related context. For the purposes of this Notice, "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 policy includes the following Annexes setting forth rights available in certain jurisdictions.

- 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.

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, contact information and employment history) and generates 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 submitting applicant referrals. 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.

What Personal Data We Process

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

- Personal details and contact information, such as name, maiden name and/or surname, e-mail and telephone details, home address, date of birth, social security/insurance number, national identification number, government issued numbers, personal identification code, gender, marital status, dependents, emergency contact information, and photograph;
- Identifiers, such as online identifiers (e.g., as cookies and IP addresses) and photographs or fingerprint scans for identification, verification, and/or security/access control purposes.
- Payroll processing and compensation data, such as banking details, salary, bonus, benefits, pay enhancement for dependents, details on equity options, equity grants and other awards, currency, pay frequency, effective date of current compensation, salary

reviews, tax ID and fiscal code;

- Right to work/immigration data, such as citizenship status, passport data, identity card data, details of residency or work permit;
- Talent, recruitment, referral, and application details, education and training details, such as details contained in letters of applications, resumes/CVs, and referral letters, previous employment background and references, education history, professional qualifications, language and other relevant skills, details on performance management ratings, development plan and willingness to relocate;
- Work and work history, such as description of current and prior position(s), title(s), salary plan(s), pay grade(s) or level(s), unit/department(s), location(s), supervisor(s) and subordinate(s), Colleague identification number, employment status and type, terms of employment, employment contract, work history, re-hire and termination date(s), length of service, retirement eligibility, promotions and disciplinary records;
- Work schedule data, such as working time records (including vacation, sickness leave and other absence records, leave status, hours worked and department standard hours); overtime and shift work and termination date;
- 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 preferences in connection with Company-related travel; and
- Inferences drawn from other Personal Data, such as predictive or analytical information that concerns a person's performance at work.
- Other information you provide during application, onboarding, or employment.

In certain instances and jurisdictions, we obtain Personal Data through Company-owned devices, physical locations, or vehicles, or through your personal devices that you use for work purposes:

- GPS tracking devices may be utilized in Company-managed vehicles for the business purpose of vehicle maintenance, dispatch and scheduling, promoting safe driving habits, auditing, controlling fuel costs, and analyzing business related metrics. When utilized, the GPS tracking devices can provide the Company with certain vehicle information, such as: (i) vehicle location; (ii) vehicle travel routes and speed; (iii) notifications concerning excessive speed, off hour usage, driving outside the approved geographical boundary, excessive idle time, and sensor tampering; (iv) vehicle start and stop times; and (v) arrival and departure times. Vehicle location tracking is not conducted in jurisdictions where it is prohibited by law or applicable company policies or procedures (such as Germany).
- In jurisdictions where permitted by law, we may track the GPS location of your mobile device in order to support vehicle mileage reimbursement programs for your business use of personal vehicles. Technical and administrative measures are implemented to limit data collection to that which is directly relevant for purposes of 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. Additionally, Company-provided vehicles may also be equipped with a video camera recording system containing cameras.
- Audio recordings of monitored phone calls when accessing company resources, such as IT services, or when interacting with a customer or member of the public, including in a

customer account management or customer service capacity.

- Device and Network Monitoring – 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.

Any and all telephone conversations or transmissions, electronic mail or transmissions, chat messages or transmissions, or internet access or usage by a Colleague by any electronic device or system used for work purposes or connected to work systems or networks, including but not limited to the use of a computer, telephone, or mobile device, may be subject to monitoring or review at any and all times and by any lawful means consistent with Company policies.

How We Process Personal Data

The Company uses Colleague Personal Data for the following purposes:

- Managing workforce: managing work activities and personnel generally, including meeting customer needs, resource planning and allocation, appraisals and performance evaluations, promotions, succession planning and career development, administering salary and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare, life insurance and other benefit administration, social security, retirement and savings plans, training (including distribution of company policies and training materials to Colleagues), leave, transfers, honoring other contractual benefits, loans, compilation of Colleague directories, managing disciplinary matters and terminations, making business travel arrangements, and other general administrative functions to assist Colleagues in meeting their job expectations such as providing appropriate IT equipment and support or for security considerations;
- 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;
- To comply with legal obligations: complying with our regulatory obligations, court orders, subpoenas, and similar requests regarding our hiring and management of our workforce; performing background checks as required by applicable laws, conducting checks against exclusion and sanction lists as required by applicable laws;
- Compliance: conducting investigations, processing work-related claims, such as worker's compensation claims, complying with legal 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, and complying with internal policies and procedures;
- Safety and security: protecting the safety and security of other individuals, including Colleagues, customers, and the general public, and the security of the Company's properties and assets, such as confidential information.
- To carry out other purposes as part of our business activities when reasonably required by us.

The Company also uses Personal Data for the following purposes: operating and managing the IT and communications systems, managing Company assets, allocating Company assets and human resources, strategic planning, project management, business continuity, compilation of

audit trails and other reporting tools, budgeting, financial management and reporting, communications, safeguarding IT infrastructure, office equipment and other property, performing workforce analysis and planning, responding to legal process such as court summons, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims.

Sensitive Personal Data

In some jurisdictions, the Company may Process certain categories of Personal Data that may be considered sensitive in certain jurisdictions ("Sensitive Personal Data"), including:

- Colleague social security/insurance numbers, driver's licenses, state identification cards, and passport details for Colleague onboarding and HR management purposes, such as background checks, and meeting legal obligations related to taxes and social security.
- Geolocation information to track location of Company-managed 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.
- Health data, racial and/or ethnic data, sexual orientation, and gender identity to carry out obligations in the field of employment, benefits administration, 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 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 with respect to the Processing of their Personal Data. 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. The Human Resources Department maintains these files in a secure environment.

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 managers in the Company where relevant, such as if the Colleague is being considered for an alternative job opportunity, or if a new manager appointed in the line of business needs to review files.

3. DISCLOSURE AND INTERNATIONAL TRANSFERS OF PERSONAL DATA

The Company may disclose relevant Personal Data to:

- 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;
- Individuals that you name as references or individuals that referred you for a position;
- 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 or governmental authorities to comply with laws, regulations, court orders, subpoenas, and similar requests;
- 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;
- Other companies, in order to protect our legal rights or honor our legal obligations to those companies
- 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.

From time to time, the Company may also need to disclose Personal Data to other parties, such as any person (natural or legal) or organization to whom the Company may be required by applicable laws to disclose Personal Data, including, but not limited to, law enforcement authorities, financial institutions, and governmental bodies. The Company may share Personal Data with these third parties where it believes this is necessary to comply with a legal or regulatory obligation or request, to promote safety or security, or otherwise to protect its rights or the rights of any third party, including the content of communications including email, text messages, and chats.

4. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Given the global nature of the Company, we may (subject to applicable law) transfer Personal Data to other Convergint Technologies group 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 the Colleague's home jurisdiction. The Convergint Technologies group entities have entered into a intra group transfer agreement which contains contractual commitments in order to ensure 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 ensuring the on-going integrity and confidentiality of Personal Data. The Company evaluates these measures on a regular basis to ensure 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.

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 or 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.

ANNEX I — CALIFORNIA COLLEAGUE RIGHTS AND CHOICES REGARDING PERSONAL DATA

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 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 RIGHTS

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: ADDITIONAL EUROPEAN INFORMATION

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. COMPANY

References to the "Company" shall be deemed to be to the relevant Convergint entity that has employed or otherwise contracted with you.

2. DATA AND PURPOSES

The processing set out in the section of the Notice regarding special category data is not all applicable to Colleagues in the UK, European Economic Area, or Switzerland. Specifically: (i) Company does not conduct geolocation tracking of company vehicles except in limited circumstances where permitted by law and in accordance with Company policies; (ii) Company does not process racial and/or ethnic data, sexual orientation, gender identity data, or biometric information; and (iii) any monitoring of devices and equipment is only conducted in limited circumstances where permitted by law and in accordance with Company policies.

You have obligations under your employment contract which require the processing of certain Personal Data. For example, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. 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.

Certain other information, such as contact details, your right to work in your employment country and payment details, will need to be provided to enable the Company to enter a contract of employment with you. If you do not provide the necessary information, this will hinder the Company's ability to administer the rights and obligations essential to our employment relationship with you.

3. LAWFUL BASIS

The General Data Protection Regulation applies to our processing of Personal Data. Under these laws we need to demonstrate a lawful basis.

As further described above, the Company uses your personal information for the following reasons:

- **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.

Less commonly, we may process this type of information 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

4. RIGHTS

You have certain rights under European data protection legislation. 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.