HR Privacy Notice

RapidDeploy Inc. ("RapidDeploy") is providing this RapidDeploy HR Privacy Notice ("**HR Privacy Notice**") to give its employees, job applicants, contractors (collectively "**Personnel**") and other individuals whose Personal Data is collected for human resources purposes (such as dependents) information regarding how we collect and use your Personal Data for these purposes. In this Notice, "**Personal Data**" means data relating to an identified or identifiable individuals and households.

This HR Privacy Notice applies only to Personal Data used in the context of Human Resources, employment, and other internal business functions relating to our Personnel and their family members or beneficiaries, including internal computer systems, networks, and online services. RapidDeploy's external Privacy Policy ("**Privacy Policy**") describes how we collect, use and protect the Personal Data of consumers and users of RapidDeploy's products and services, and our Services (as defined in the Privacy Policy). The Privacy Policy will apply to the extent RapidDeploy Personnel use any products or services subject to the Privacy Policy.

If you are a current RapidDeploy employee, you can send an email to hr@rapiddeploy.com to exercise your rights of access and correction with respect to Personal Data subject to this HR Privacy Notice, and in some cases, you may be able to access or update information directly through online services or portals. You may also contact your local HR manager for assistance. If you are a contractor, or an applicant, former employee or family member, please contact us at the address or email listed below for assistance with your privacy requests.

GENERAL PURPOSES FOR COLLECTING, USING AND DISCLOSING PERSONAL DATA

RapidDeploy collects Personal Data about its prospective, current, and former Personnel and other individuals as appropriate in the context of an employment or contractual work relationship (such as dependents), including for recruitment and IT/technical support services, and internal software, networks and devices. The categories of Personal Data we process, along with representative data elements, are listed in the chart below. We generally use, disclose and retain Personal Data processed under this HR Privacy Notice for the following purposes:

(a) Personal Data pertaining *prospective* employees or contractors may be collected, used and shared for:
- Recruitment and staffing, including evaluation of skills and job placement,
- Hiring decisions, including negotiation of compensation, benefits, relocation packages, *etc.*,
- Determining an individual's eligibility to work and assisting with work permits or visas,
- Risk management, including background checks, vetting and verification, and
- Our Business Purposes (defined below).

(b) Personal Data pertaining to *current* employees and contractors may be collected, used and shared for:
- Staffing and job placement, including scheduling and absence management,
- Administration of compensation, insurance and benefits programs,
- Time and attendance tracking, expense reimbursement, other workplace administration and facilitating relationships within RapidDeploy,
- IT uses, such as managing our computers and other assets, providing email and other tools to our workers,
- Diversity programs,
- Health and wellness programs and accommodating disabilities,
- Occupational health and safety programs (including required reporting, disaster and pandemic planning, and incident management),
- Talent and performance development, skills management and training, performance reviews (including customer surveys), engagement surveys, and recognition and reward programs,
- HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes,

- Risk management, including employee and premises monitoring, such as in our retail locations, or adjacent to RapidDeploy premises,
- Providing employment and income verification,
- As requested by individuals, and
- Business Purposes.

(c) Personal Data pertaining to *former* employees and contractors may be collected, used and shared for:
- Re-employment,
- Administration of compensation, insurance and benefits programs,
- For archival and recordkeeping purposes,
- Providing employment and income verification,
- As requested by individuals, and
- Business Purposes.

(d) Personal Data pertaining to individuals whose information is provided to RapidDeploy in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, *etc.*) may be collected, used and shared for:
- Administration of compensation, insurance and benefit programs,
- Workplace administration,
- To comply with child support orders or garnishments,
- To maintain internal directories, emergency contact lists and similar records, and
- Business Purposes.

Business Purposes means the following purposes for which Personal Data may be collected, used and shared:
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials,
- Security, loss prevention, information security and cybersecurity,
- Legal and regulatory compliance, including without limitation all uses and disclosures of Personal Data that are required by law or for compliance with legally mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines, and other processing in connection with the establishment and defense of legal claims,
- Corporate audit, analysis and consolidated reporting,
- To enforce our contracts and to protect RapidDeploy, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property,
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research or analytics,
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the analysis and improvement of technical and organizational services, operations, and similar matters; and
- As needed to facilitate corporate governance, including mergers, acquisitions and divestitures.

CATEGORIES OF PERSONAL DATA

This chart describes the categories of Personal Data that RapidDeploy may collect in connection with its employment and contractual work relationships. Note, all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of PI and Representative Data Elements	Common Purposes for Collecting and Sharing the PI
Contact Data • Honorifics and titles, preferred form of address • Mailing address • Email address • Telephone number • Mobile number • Social media or communications platform usernames or handles	We use your Contact Data to communicate with you by mail, email, telephone or text about your employment, including sending you work schedule information, compensation and benefits communications and other company information. Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.

Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Company ID number • Company account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use your Identity Data to identify you in our HR records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, for internal record-keeping and reporting, including for data matching and analytics, and to track your use of company programs and assets, and for most processing purposes described in this HR Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security number • Driver's license number • Passport number • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number)*	We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks, subject to applicable law, enable us to administer payroll and benefits programs and comply with applicable laws, such as reporting compensation to government agencies as required by law, as well as for security and risk management, such as collecting driver's license data for employees who operate company automobiles, professional license verification, fraud prevention and similar purposes . We may also use Government ID data for other customer business purposes, such as collecting passport data and secure flight information for employees who travel.
Biographical Data • Resume or CV • Data from LinkedIn profiles and similar platforms • Education and degree information • Professional licenses, certifications and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Professional goals and interests	We use Qualification Information to help us understand our employees and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between individuals' background and relevant job functions. We also use Qualification Information to foster a creative, diverse workforce, for coaching, and to guide our decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, Reporting Information • Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	We use Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g. employment creation, maintenance, evaluation, discipline, etc.).

Financial Data • Bank account number and details • Company-issued payment card information, including transaction records • Personal payment card information, if provided for reimbursement • Credit history, if a credit check is obtained (only done in limited circumstances)	We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, and for security and fraud prevention.
Health Data • Medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities • Medical information for leave and absence management, emergency preparedness programs • Dietary restrictions or information • Wellness program data • Information pertaining to enrollment and utilization of health and disability insurance programs	We use your Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics related to our human resources functions, staffing needs, and other Business Purposes.
Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet access, including metadata and other technically-generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	We use Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with company policies. For example, we may use access logs to verify employee attendance records. Our service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business and HR functions.
Audio/Visual Data • Photograph • Video images, videoconference records • CCTV recordings • Call center recordings and call monitoring records • Voicemails	We may use Audio/Visual Data for general relationship purposes, such as call recordings used for training, coaching or quality control. We use CCTV recording for premises security purposes and loss prevention. We may also use this information to evaluate compliance with company policies. For example, we may use CCTV images to verify employee attendance records.
Inference Data • Performance reviews • Results of tests related to interests and aptitudes	We use inferred and derived data to help tailor professional development programs and to determine suitability for advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain inference data may be collected in connection with information security functions, e.g. patterns of usage and cybersecurity risk.

Compliance and Demographic data • Diversity information • Employment eligibility verification records, background screening records, and other record maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA *et al.* • Occupational safety records and worker's compensation program records • Records relating to internal investigations, including compliance hotline reports • Records of privacy and security incidents involving HR records, including any security breach notifications	We use Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, to evaluate the diversity of our staff, and as needed for litigation and defense of claims.
Protected Category Data Characteristics of protected classifications under California or federal law, e.g. race, national origin, religion, gender, or sexual orientation. **Sensitive Personal Data** Personal Data that is subject to additional restrictions under the GDPR and/or POPIA, e.g. Personal Data revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, biometric data, health information, or information relating to sexual orientation.	We use Sensitive Personal Data and Protected Category Data only as strictly necessary for the purpose it is collected with your knowledge, and consent if required by law (e.g. health information on a health insurance benefits application), and as needed to facilitate the employment relationship, to complete consumer/background check reports, and for compliance and legal reporting obligations.

CATEGORIES OF SOURCES OF PERSONAL DATA

We collect Personal Data from various sources, which vary depending on the context in which we process that Personal Data.

- **Data you provide us** – We will receive your Personal Data when you provide them to us, when you apply for a job, complete forms, or otherwise direct information to us.
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications, and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Data such as Inference Data based on our observations or analysis of other Personal Data processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine Personal Data about you that we receive from you and from third parties.

DISCLOSURE OF PERSONAL DATA

We generally process HR Personal Data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The Personal Data identified below collected from our Personnel may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of HR Departments** – All Personal Data relating to Human Resources and Recruitment.
- **Personnel of Finance Departments** – Personal Data to the extent related to company and employee transactions
- **Direct Supervisors –** Elements of Personal Data to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters;
- **Department managers searching for new employees** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs

- **Senior Supervisors –** Elements of Personal Data to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters.
- **IT Administrators** of RapidDeploy and/or third parties who support the management and administration of HR processes may receive Personal Data as necessary for providing relevant IT related support services (conducting IT security measures and IT support services)
- **Peers and colleagues –** Elements of Personal Data, to the extent permitted in jurisdiction, in connection with company address books, intracompany and interpersonal communications, and other contexts relevant to the day-to-day operation of company business.

CATEGORIES OF EXTERNAL RECIPIENTS

RapidDeploy may provide HR Personal Data to external third parties as described below. The specific information disclosed may vary depending on context but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and RapidDeploy. We generally provide information to:

- Our subsidiaries, affiliates, and parent company
- Service providers, vendors, and similar data processors that process Personal Data on RapidDeploy's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, etc.).
- To prospective seller or buyer of such business or assets in the event RapidDeploy sells or buys any business or assets.
- To future RapidDeploy affiliated entities, if RapidDeploy or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its employees will be one of the transferred assets.
- To government agencies or departments, employee unions, or similar parties in connection with employment related matters.
- To any public authority in relation to national security or law enforcement requests, if RapidDeploy is required to disclose Personal Data in response to lawful requests by public authority.
- To any other appropriate third party, if RapidDeploy is under a duty to disclose or share your Personal Data in order to comply with any legal obligation or to protect the rights, property, or safety of RapidDeploy, our employees, customers, or others.

LOCATIONS OF RECIPIENTS

RapidDeploy or its affiliates and certain service providers are located in the United States, South Africa and the European Union. Any Personal Data collected under this Policy will likely be processed under appropriate privacy law in the United States, South Africa or the European Union, in addition to any other jurisdiction where such RapidDeploy affiliate is located.

DATA ADMINISTRATION

SECURITY

RapidDeploy requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in our various security policies. RapidDeploy staff must follow the security procedures set out in applicable security policies at all times.

RETENTION AND DISPOSAL

RapidDeploy keeps Personal Data only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. RapidDeploy staff must follow any applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with applicable company policies.

ADDITIONAL DISCLOSURES – EU/EEA RESIDENTS

GDPR PRIVACY RIGHTS

Under the General Data Protection Regulation ("GDPR") and analogous legislation, residents of the EU/EEA, Switzerland, Cayman Islands, and other locations may have the following rights in addition to those set forth in the Rights & Choices section above, subject to applicable legal limitations, and provided that your request is appropriately verified:

- **Access** – You may have a right to know what information we collect, use, disclose, or sell, and you may have the right to receive a list of that Personal Data and a list of the third parties (or categories of third parties) with whom we have received or shared Personal Data, to the extent required and permitted by law.
- **Rectification** – You may correct any Personal Data that we hold about you to the extent required and permitted by law.
- **Delete** – To the extent required by applicable law, you may request that we delete your Personal Data from our systems. We may delete your data entirely, or we may anonymize or aggregate your information such that it no longer reasonably identifies you. Contact us as part of your request to determine how your Personal Data will be erased in connection with your request.
- **Data Export** – To the extent required by applicable law, we will send you a copy of your Personal Data in a common portable format of our choice.
- **Objection** – You may have the right under applicable law to object to our processing of your Personal Data that we undertake without your consent as in connection with our legitimate business interests (including any processing specified as such or processed under this Privacy Policy for a Business Purpose). You may do so by contacting us re: data rights requests. Note that we may not be required to cease, or limit processing based solely on that objection, and we may continue processing cases where our interests in processing are balanced against individuals' privacy interests. You may also object to processing for direct marketing purposes. We will cease processing upon your objection to such processing.
- **Regulator Contact** – You may have the right to contact or file a complaint with regulators or supervisory authorities about our processing of Personal Data. To do so, please contact your local data protection or consumer protection authority.

LEGAL BASIS FOR PROCESSING PERSONAL DATA

We process Personal Data in connection with the management and administration of HR processes as described below. For example, we process Personal Data when we have a legitimate interest in the processing of that data, such as:

- To **improve recruitment processes** and staffing, e.g., by monitoring characteristics and qualifications of applicants.
- To provide **training and professional development** services to Personnel.
- To track, manage and **process Personnel expenses**, and other company finances submitted by or related to Personnel.
- To monitor **compliance with our IT and data security/use policies**, for example, to ensure that confidential information is not sent outside the network, or to ensure the proper use of employer-provided technologies (including communications). Note: such processing may include access by RapidDeploy to the content of communications sent using RapidDeploy equipment or services.
- To **manage Personnel and improve internal processes and systems**, for example, to monitor attendance and productivity, and create records of Personnel certifications, disciplinary history, and other records not required by law.
- To provide **communications services to** Personnel, as well as providing **on-site and remote networking** such as VPNs, Wi-Fi, and related logins, and when we monitor the operation and security of those services.
- To **provide and manage hardware, and software applications** that are used in business operations, e.g. when a user is assigned a given device (e.g. a laptop or computer), or user account (e.g. for software or SaaS services).
- To **support Personnel's use of essential or important technology services**, e.g. when we provide technical support.
- For **physical and information security** purposes, we may process Personal Data when we monitor and filter network traffic, scan communications for malware, and use video monitoring in our facilities.

We may also process Personal Data whenever it is strictly necessary in connection with certain activity, such as**:**

- To **maintain a relationship or fulfil a contract** – for example, processing Personal Data to pay our Personnel or reimburse expenses, as part of essential employment records, and any processing of Personal Data that you may provide in connection with benefits (such as insurance or retirement accounts).

- To **comply with** RapidDeploy's **legal obligations** – for example, sharing Personal Data with regulatory agencies in connection with tax and income reporting, and providing Personal Data in response to legal requests or for regulatory or law enforcement purposes.
- To **protect vital interests of individuals** – for example, using Personal Data to contact individuals in an emergency, or to provide information in connection with health and safety incidents.

We process **Sensitive Personal information** only when permitted by law. For example:

- When in the **public interest or required by law**, e.g. in connection with legal and regulatory reporting requirements relating to taxation, public health, etc.
- To protect an individual's **vital interests** when consent cannot be obtained, e.g. in a workplace injury.
- In connection with our **rights and obligations under law**, e.g. in connection with legal reporting requirements.

Finally, we may process any Personal Data in accordance with **your consent**, for example, in connection with your participation in an optional program, event, or other endeavor.

AUTOMATED DECISION MAKING

To the extent permitted under applicable law, the processing of Personal Data in connection with application evaluation may involve the use of automated decision-making that may extract relevant information and rate applications based on their conformity with requirements. In some cases, automated processing may reject or place a low rating on applications that are found to not meet requirements of a given engagement.]

INTERNATIONAL TRANSFERS

RapidDeploy is a US-based employer and we use service providers located in the United States. It is necessary for us transfer Personal Data to, and process it in, the United States in order to evaluate, establish, and maintain the employment relationship, and your Personal Data will be transferred to the US on that basis. The U.S. does not provide the same legal protections guaranteed to Personal Data in the European Union and South Africa. If you are in the EEA/Switzerland/UK or South Africa, your Personal Data may be transferred to the U.S. on one of the following bases:

- Pursuant to the derogations provided under applicable law (e.g. where such transfers are necessary to create and maintain the employment relationship);
- Standard Contractual Clauses (e.g. Personal Data shared with other entities, such as our subprocessors or service providers)
- Binding corporate rules (e.g. data processed by subprocessors or service providers subject to a BCR agreement); or
- Pursuant to other adequacy mechanisms (e.g. where transfers are within the EEA or to other justification subject to an adequacy decision).

If you would like additional information regarding the specific transfer mechanism applicable in the context of any transfer of your personal data, please contact us.