

EMPLOYEE PRIVACY NOTICE

Last updated: June 23, 2025

This Employee Privacy Notice ("**Notice**") applies to all persons who work for us, whether employed by us or not. It also applies to former employees. We use the word "you" to refer to anyone within the scope of this Notice.

This Notice explains the types of information we process about you, why we are processing it and how that processing may affect you. This Notice may be supplemented by additional statements to comply with local requirements in the country where you are located. Please read the Annex to this Notice for, where relevant, additional information relevant to the location in which you are employed or engaged.

References in this Notice to employment, work (and similar expressions) include any arrangement we may have under which an individual provides us with work or services. By way of example, when we mention an "employment contract", that includes a contract under which you provide us with services.

1. **Introduction**

runZero Inc. ("**runZero**", "**we**" or "**us**") has issued this Notice to describe how we handle personal information that we hold about you. We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law.

If you have any comments or questions about this Notice, then please contact us using the contact details under the "How to contact us" heading below.

2. **Personal information we collect and process when you work for us**

Sources of personal information

When you start work with us, the initial data about you that we process is likely to come from you: for example, contact details, bank details and information on your immigration status and whether you can lawfully work. We may also require references and information to carry out background checks.

In the course of your employment or engagement, you may be required to provide us with information for other purposes such as sick pay and family rights. If you do not provide information that you are required by statute or contract to give us, you may lose benefits or we may decide not to employ or engage you or to end your contract. If you have concerns about this in a particular context, you should speak to the People Team.

We may also receive personal information relating to you from others. Internally, personal information may be derived from your managers and other colleagues or from our IT systems; externally, it may be derived from our customers or those with whom you communicate by email or other systems.

Categories of personal information

We may collect the following categories of information from and about you in connection with your employment or engagement:

- **Identification Data:** name, gender, tax registration number, social security information and other details in identity documents (runZero may also collect copies of such IDs);
- **Contact Data:** physical address, telephone number, email address and other contact details;
- **Spouse and Dependent Data:** information relating to your next-of-kin, spouse, dependents and other family members (in particular, their names and dates of birth and details of entitlements under relevant benefit schemes);
- **Background Data:** age, date of birth, racial or ethnic origin, religion, academic/professional qualifications, education, CV/résumé, other information collected when you applied for a role at runZero, and background check information (for vetting purposes, where permissible and in accordance with applicable law);
- **Employment Data:** job title and position, office location, employment contract, performance and disciplinary records, employment and training history, grievance procedures, sickness/holiday and working time records;
- **Payroll Data:** bank account details, salary information, tax information, withholdings, benefits, expenses, company allowances, stock and equity grants;
- **Audio/Visual Data:** photographs and other audio-visual information used for workplace initiatives and call or video conference recordings used for sales and customer support purposes; and
- **IT Data:** information regarding your use of IT applications, systems and equipment provided by runZero including IP addresses, network identification data, activities conducted on runZero's IT applications and systems, data usage, cookies, device IDs and web browsing history.

Some of the personal information may be considered sensitive data or “special categories” of data under applicable data protection laws, for example, data relating to race and ethnic origin, which we may process for the purpose of monitoring and improving diversity and inclusiveness at our workplaces or for defending claims against runZero and data relating to physical or mental health condition (“Health Data”) which we may process for adapting your work space or patterns, administering insurance policies or defending claims against runZero.

3. Legal grounds for processing personal information – EEA and UK only

If you are based in the EEA or the UK, our legal basis for collecting and using your personal information will depend on the personal information concerned and the specific context in which we collect it. There are various legal bases on which we can rely when processing your personal information. In some contexts, more than one ground applies.

We have summarized the most relevant grounds below:

Term	Ground for processing	Explanation
Contract	Processing necessary for performance of a contract with you or to take steps at your request to enter a contract	This covers carrying out our contractual duties and exercising our contractual rights.
Legal Obligation	Processing necessary to comply with our legal obligations	Ensuring we perform our legal and regulatory obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Legitimate Interests	Processing necessary for our or a third party's legitimate interests	<p>We or a third party have legitimate interests in carrying on, managing and administering our respective businesses effectively and properly and in connection with those interests processing your data.</p> <p>Your data will not be processed on this basis if our or a third party's interests are overridden by your own interests, rights and freedoms.</p>
Consent	You have given specific consent to processing your data	In general, processing of your data in connection with employment will not be conditional on your consent. But there may be occasions where we do specific things such as provide a reference, seek to monitor diversity or obtain medical reports and rely on your consent to our doing so.

If we process sensitive personal information about you, as well as ensuring that one of the grounds for processing mentioned above applies, we will make sure that one or more of the grounds for processing sensitive personal information applies. In outline, these include:

- Where you have provided your explicit consent;
- Where the processing is necessary for the purposes of your or our obligations and rights in relation to employment in so far as it is authorized by law or collective agreement;
- Where the processing relates to data about you that you have made public;
- Where the processing is necessary for the purpose of establishing, making or defending legal claims.

4. How we use your personal information (our purposes) and our lawful basis for processing it

We use the personal information that we collect from and about you only for the purposes described in this Notice. The following table provides more details on our purposes for processing your personal information and the related legal bases.

Purpose	Examples of personal information that may be processed	Grounds for processing
Administering your employment or service contract including entering it, performing it and changing it	Identification Data Contact Data Employment Data For example: information on your terms of employment or engagement including your pay and benefits, your participation in retirement benefits, life and medical insurance and any bonus or share scheme.	Contract Legal obligations Legitimate interests
Contacting you or others on your behalf	Contact Data Spouse and Dependent Data	Contract Legitimate interests
Payroll administration	Identification Data Payroll Data	Contract Legal obligation Legitimate interests
Supporting and managing your work and performance and any health concerns	Employment Data IT Data Health Data For example: <ul style="list-style-type: none">Information connected with your work, anything you do at work and your performance including records of documents, Slack messages, and emails created by or relating to you and information on your use of	Contract Legal obligation Legitimate interests In relation to sensitive Health Data: Employment obligations, occupational health and working capacity

Purpose	Examples of personal information that may be processed	Grounds for processing
	<p>our systems including computers, laptops or other devices.</p> <ul style="list-style-type: none"> • Management information regarding you including notes of meetings and appraisal / performance records. • Information relating to your compliance with our policies. • Information concerning disciplinary allegations, investigations and processes and relating to grievances in which you are or may be directly or indirectly involved. • To the extent required or permitted by local law, information concerning your health, including self-certification forms, medical and occupational health reports. 	
Changing or ending your working arrangements	<p>Identification Data Employment Data</p> <p>For example: information connected with anything that may affect your continuing employment or the terms on which you work including any proposal to promote you, to change your pay or benefits, to change your working</p>	<p>Contract Legitimate interests</p>

Purpose	Examples of personal information that may be processed	Grounds for processing
	arrangements or to end your employment.	
Physical and system security	Security & Access Data IT Data	Legal obligation Legitimate interests
Providing references in connection with your finding new employment	Employment Data	Consent
Providing information to third parties in connection with transactions that we contemplate or carry out	Employment Data For example: information on your contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or provider of outsourced services.	Legitimate interests
Monitoring of diversity and equal opportunities	Identification Data Background Data More specifically: to the extent required or permitted by local law, information on nationality, racial and ethnic origin, gender, sexual orientation, religion, philosophical beliefs, disability, age and other diversity markers.	Consent In relation to sensitive personal information: Consent
Monitoring and investigating compliance with policies and rules both generally and specifically	Employment Data IT Data Security and Access Data More specifically: we expect our employees and staff to comply with our policies and rules and may monitor our systems to check compliance (e.g. rules on accessing prohibited websites at work). We may also have specific concerns about compliance and check system and other data to look into those concerns (e.g. log in records,	Legitimate interests

Purpose	Examples of personal information that may be processed	Grounds for processing
	records of usage and emails and documents).	
Disputes and legal proceedings	Employment Data Payroll Data IT Data Any other information relevant or potentially relevant to a dispute or legal proceeding affecting us.	Legitimate interests Legal obligation
Day-to-day business operations including conducting and improving marketing, sales, support and customer relations.	Contact Data Employment Data Audio/Visual Data More specifically: information used on global or local internal or external directories to identify what you do and how you can be contacted (to enable collaboration with colleagues and others). Any information relating to the work you do for us, your role and contact details including call or other interactions with current or potential customers.	Legitimate interests
Maintaining appropriate business records during and after your employment or engagement	Employment Data Other information relating to your work, anything you do at work and your performance relevant to such records.	Contract Legal obligation Legitimate interests

5. Who we share your personal information with

Internal use

Your personal information may be disclosed to your managers, the Legal Team, the People Team and administrators for employment, administrative and management purposes as mentioned in this Notice.

We will share your personal information with other members of the runZero group around the world in order to administer human resources, staff member compensation and benefits at an international level on our HR systems, as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management.

Transfers to third party service providers

In addition, we make certain personal information available to third parties who provide services to us.

Specific examples of such third parties and the circumstances in which your personal information may be disclosed to them include the following:

- our benefit/reward plans service providers (including retirement schemes, employee share schemes and medical insurance providers), e.g. Sequoia, Guardian, Blue Cross Blue Shield, Rippling, Guideline, Carta;
- third party companies who provide us with payroll, tax and expense administration support services, e.g. Rippling, Quotapath;
- providers of our HR platform - e.g. Rippling;
- third parties who provide, support and maintain our IT and communications infrastructure (including for data storage purposes) and provide business continuity services, e.g. Google, Slack, Zoom;
- third parties who assist in the provision of work related travel expenses, e.g. Expensify;
- third parties who provide services in relation to staff training, qualifications and staff surveys, e.g. Mineral; and
- auditors, advisors, legal representatives and similar agents in connection with the advisory services they provide to us for legitimate business purposes and under a contractual prohibition of using the personal information for any other purpose.

Transfers to other third parties

We may also disclose personal information to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process;
- In response to lawful requests by public authorities (including for tax, immigration, health and safety, national security or law enforcement purposes);
- As necessary to establish, exercise or defend against potential, threatened or actual litigation;
- Where necessary to protect the vital interests of another person;
- In connection with the group reorganization, sale, assignment or other transfer of all or part of our business e.g. potential buyers or investors of the company or any part of the business of the company; or

- With your consent (e.g. providing a reference to your potential future employer, embassies or government authorities in connection with your visa or work permit applications).

6. How we keep your personal information secure

We take care to allow access to personal information only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it.

Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the security and confidentiality of the information is maintained.

We use appropriate technical and organisational measures to protect the personal information that we collect and process about you. The measures are designed to provide a level of security appropriate to the risk of processing your personal information. Specific measures we use include encrypting your personal information in transit and at rest; employing advance malware protections; implementation of other reasonable security defenses (including vulnerability management, access management, recovery/resilience measures).

7. International data transfers

runZero is fully remote workforce with its principle place of business in Austin, Texas in the United States.

Our third party service providers and partners also operate globally. This means that, in connection with our business and for employment, administrative, management and legal purposes, we may transfer your personal information outside of the country where you are located, including to the United States. As a result, your personal information may be transferred to a jurisdiction that may not provide the same level of data protection as your country of residence.

When we transfer your personal information internationally, we will take steps to ensure that your personal information is treated securely, lawfully, and in accordance with this Notice. Where we transfer your personal information to countries and territories outside of the EEA and the UK, for example, which have been formally recognised as providing an adequate level of protection for personal information, we rely on the relevant “adequacy decisions” from the European Commission and “adequacy regulations” (data bridges) from the Secretary of State in the UK.

Where the transfer is not subject to an adequacy decision or regulations, we have taken appropriate safeguards to require that your personal information will remain protected in accordance with this Notice and applicable laws. Where applicable, we enter into the [Standard Contractual Clauses approved by the European Commission](#) (and equivalent clauses in the UK) for transfers to our third party service providers and partners.

8. Data retention

runZero may keep your information for a reasonable period as is necessary for the purposes set out in this Notice and as otherwise required to fulfil legal or business purposes. Generally, this means your

personal information will be retained until the end of your employment or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters (e.g. to defend legal claims or to take disciplinary action), document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits.

We may anonymise your personal information so that it can no longer be associated with you. If we do that, we will continue to hold and use that (as, once anonymised, it will no longer constitute personal information.)

9. Your data privacy rights

Depending on your location and subject to applicable law, you may have the following data protection rights with regards to your personal information:

- You can **access, correct, update** or **request deletion** of your personal information.
- In certain circumstances, you can **object to processing** of your personal information, ask us to **restrict processing** of your personal information or **request portability** of your personal information.
- If we have collected and processed your personal information with your consent, then you can **withdraw your consent** at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.
- You have the right to **complain to a relevant data protection authority** about our collection and use of your personal information. For more information, please contact your local data protection authority.
- If you are located in California, please refer to the Annex for information about your data protection rights for your specific location.

You can make a request to exercise any of your privacy rights by contacting privacy@runzero.com. We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

10. Updates to this Notice

We may update this Notice from time to time in response to changing legal, regulatory, technical or business developments. When we update our Notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.

You can see when this Notice was last updated by checking the “last updated” date displayed at the top of this Notice.

11. How to contact us

If you have any questions, comments, or concerns regarding this Notice, please contact privacy@runzero.com.

Annex – Jurisdiction Specific Information

EEA / UK

If you are located in the EEA / UK, the following additional information applies to you:

1. The data controller of your personal information is runZero, Inc.
1. Contact details for data protection regulators in the EEA are available [here](#).
2. In the UK, the statutory regulator is the Information Commissioner's Office. For contact details see: <https://ico.org.uk/ICO>.

California

If you are an employee residing in California, the following additional information applies to you. For purposes of this section, "personal information" has the same meaning defined in the California Consumer Privacy Act of 2018 ("CCPA"), as amended by the California Privacy Rights Act of 2020 ("CPRA") (collectively referred to as "CCPA").

1. We may collect the following statutory categories of personal information, as enumerated by the CCPA, about you when you apply for a position with us and during the recruitment process:
 - Identifiers and contact information, such as your: name, postal address, email address, phone number, date of birth, social security number, driver's license or state identification number, and other unique identifiers including online identifiers (e.g. IP address).
 - Personal information categories listed in California Civil Code § 1798.80(e) not already listed above, such as your signature, physical characteristics or description, bank account or other financial information, medical information, or health insurance information.
 - Protected classification characteristics under California or federal law, such as your age, gender, racial or ethnic origin, national origin, citizenship, religious, marital status, sexual orientation, disability or veteran status.
 - Internet or network activity information, such as your interactions with our website and job advertisement.
 - Geolocation data, such as your approximate location based on your IP address.
 - Audio, electronic, visual, and similar information such as call and video recordings.
 - Professional or employment-related information, such as your employment history, CV/résumé information, reference checks and screening checks, position applied for, and interview notes.
 - Non-public education information, such as your academic history, education grades, and academic/professional qualifications.
 - Inferences drawn from any of the above personal information to create a summary about you, for example regarding your skills, preferences, and abilities; and
 - Sensitive personal information, as defined by the CCPA, such as government identifiers (including your social security, driver's license, state identification, or passport number, if applicable), your racial or ethnic origin, religious or philosophical beliefs, or union membership.
2. The business and commercial purposes for which we collect this information are described in Section 4. "How we use your personal information (our purposes) and our legal basis for

processing it" of this Notice. The categories of third parties to whom we disclose the information for a business purpose are described in Section 5. "Who we share your personal information with" of this Notice. We retain your personal information for the length of time as required under applicable law.

3. We do not "sell" or "share", as those terms are defined by the CCPA, the above categories of personal information. We also do not use or disclose your sensitive personal information for purposes that are not necessary to process your application.
4. Employees residing in California have the following data protection rights:
 - **Know and Access:** You have the right to request to know the personal information we have collected about you, and to access such personal information in a portable and commonly used format. Once we receive and confirm your verifiable request, we may disclose to you:
 - the categories of personal information we have collected about you.
 - the categories of sources from which your personal information was collected.
 - the business or commercial purposes for collecting that personal information.
 - the categories of third parties to whom we have disclosed that personal information. And
 - the specific pieces of personal information we have collected about you.
 - **Correct:** You have the right to request that we correct any of your personal information that we have collected from you that is inaccurate.
 - **Delete:** You have the right to request that we delete certain personal information we have collected from you.
 - **Opt out of the Sale and Sharing of your personal information:** You have the right to request that a business not "sell" or "share" your personal information with a third party, as those terms are defined under the CCPA. However, as noted above, we do not sell or share your personal information within the meaning of the CCPA.
 - **Limit the use and disclosure of sensitive personal information:** We do not use or disclose "sensitive personal information" other than as described in Section 4 of this Notice or as otherwise permitted under the CCPA.
 - **Non-Discrimination:** You have the right to not be discriminated or retaliated against for exercising any of your rights described above.
5. You can make any of these requests to exercise your CCPA rights by emailing us at privacy@runzero.com. We will respond to verifiable requests received as required by law. Please note that we may request certain information from you to verify your identity in order to respond to your request. Please also note that in California, an authorized agent may submit a rights request on your behalf. We may also request that an authorized agent verify their identity and authority to submit a rights request on your behalf.