

---

COMPLIANCE

# Privacy Policy

About your data. Describes what personal data we collect, why we collect it, how long we keep it, and which rights you have.

|                |              |
|----------------|--------------|
| Version        | 1.0          |
| ID             | 65d031118b1a |
| Prepared by    | Safespring   |
| Approver       | Safespring   |
| Date           | 2026-03-23   |
| Classification | Public       |

Safespring is a Swedish cloud infrastructure provider, proudly Swedish owned and operated.

We deliver Public Cloud and Private Cloud services for organisations that require secure, reliable, and high-performance infrastructure. Safespring operates through legal entities in Sweden and Norway and provides services from data centres located within these jurisdictions.

This Privacy Policy describes how Safespring (“we”, “us”, “our”) processes personal data in accordance with:

- General Data Protection Regulation (“GDPR”)
- ePrivacy Directive
- Digital Services Act
- ISO/IEC 27001

## 1. Data Controller

### **Safespring AB**

559075-0245

Rättarvägen 3, 169 68 Solna

Sweden

For privacy-related matters, including the exercise of data subject rights, you may contact us at [gdpr@safespring.com](mailto:gdpr@safespring.com)

## 2. Your Rights Under GDPR

You are entitled to the following rights under applicable data protections laws:

- **The right to access:** You are entitled to receive certain information on our processing of your personal data. Such information is provided in this information document. Further, you have the right to receive a copy of the personal data we process relating to you. Upon request, we will provide a copy of your personal data in a commonly used electronic form.
- **The right to rectification:** You are entitled to obtain rectification of inaccurate personal data and to have incomplete personal data completed.
- **The right to erasure (“right to be forgotten”):** You may under certain circumstances request us to delete your personal data. Please note that this right is not unconditional. Therefore, an attempt to invoke the right might not lead to an action from us.
- **The right to restriction of processing:** You may under certain circumstances request from us to restrict the processing of your personal data. Please note that this right is

not unconditional. Therefore, an attempt to invoke the right might not lead to an action from us.

- **The right to data portability:** You are entitled to receive your personal data (or have your personal data directly transmitted to another data controller) in a structured, commonly used and machine-readable format.
- **The right to object:** You are entitled to object to certain processing activities conducted by us in relation to your personal data, such as our processing of your personal data based on our legitimate interest.
- **Right to withdraw consent:** In the event we process data on the basis of your consent, you are entitled to withdraw your consent at any time.
- **Lodge a complaint:** You have the right to lodge a complaint with the supervisory authority, see the details below.

## Contact Information

### Local Authorities

#### Sweden

Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, IMY)  
website: <https://www.imy.se/>

#### Norway

Norwegian Data Protection Authority (Datatilsynet)  
website: <https://www.datatilsynet.no/>

#### Denmark

Danish Data Protection Agency (Datatilsynet)  
website: <https://www.datatilsynet.dk/english>

#### Finland

Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto)  
website: <https://tietosuoja.fi/en/home>

## 3. Categories of Data Subjects

We may process personal data relating to:

- Website visitors
- Business contacts
- Job applicants
- Authorized Users of our services

## 4. Website Privacy

### 4.1 Purpose of Processing

When you visit our website, we may process your website data to evaluate, develop and improve our website and our services, in particular for the purpose of:

- Website functionality and security
- Analytics and performance monitoring
- Campaign effectiveness tracking
- Improvement of user experience

### 4.2 Categories of Personal Data

We may process:

- IP address (anonymised where technically feasible)
- Device and browser metadata
- Date/time and session data
- Page views and interaction data
- Referrer URLs
- Marketing parameters
- Download/click behaviour
- Error logs
- Session interaction data (if applicable)

Where possible, IP addresses are truncated or anonymised immediately upon collection.

### 4.3 Legal Basis (GDPR Art. 6)

The processing is based on:

- Art. 6(1)(a) GDPR — Consent (where required for non-essential cookies or tracking)
- Art. 6(1)(f) GDPR — Legitimate interest (in the case of strictly necessary cookies our processing is necessary for our legitimate interest to ensure that our website and services are meeting your and our needs over time).

### 4.4 Retention

We will retain your Personal Data:

- Raw analytics and log data: maximum 12 months from collection.

Retention periods are defined in accordance with ISO 27001 control requirements for information lifecycle management.

## 4.5 Cookies and Similar Technologies

We use cookies and similar technologies in compliance with the ePrivacy Directive and GDPR. Cookies may include:

- Strictly necessary cookies
- Functional cookies
- Analytics technologies
- Consent management cookies (read more about our cookies in the [Cookies setting](#))

## 5. Business Contact Data

### 5.1 Purpose of Processing

When we enter into an agreement with the company you represent, we process your personal data in order to administer the agreement and communicate with you, in particular for the purpose of:

- Commercial discussions and marketing activities
- Inform of our services
- Contract fulfilment
- Customer relationship management
- Surveys and newsletters

### 5.2 Categories of Personal Data

We may process:

- Name
- Business email
- Business phone
- Title
- Employer organisation
- Professional profile links

### 5.3 Legal Basis

The processing is based on:

- Art. 6(1)(f) — Legitimate interest (when the processing is necessary for our legitimate interests to communicate with you and fulfil the agreement with the company you represent, maintain good customer relations or inform about our business and services)
- Art. 6(1)(b) — Contract performance (to fulfil the agreement when we enter into an agreement with you directly)
- Art. 6(1)(a) — Consent (for surveys/newsletters)

## 5.4 Retention

We will retain your Personal Data:

- Personal data is retained for the duration of the active business relationship and 1 year thereafter or until you inform us that you no longer shall be the contact person under the agreement.
- For processing based on your consent you may withdraw the consent at any time. If you opt-out or unsubscribe from our marketing, we will no longer process your personal data for this purpose.

# 6. Recruitment

## 6.1 Purpose of Processing

If you submit a job application, we will process your Personal Data in order to administer your application and assess whether to proceed with your application and potentially offer you employment.

## 6.2 Categories of Personal Data

We may process:

- Name, address, phone number, e-mail address
- CV and application documents including work experience and education background and other information voluntarily provided by you.
- Assessment notes

## 6.3 Legal Basis

The processing is based on:

- Art. 6(1)(a) — Consent (if you consent to be included in a candidate pool)
- Art. 6(1)(b) — Pre-contractual steps

## 6.4 Retention

We will retain your Personal Data:

- During active recruitment
- Up to 12 months for candidate pooling (unless consent is withdrawn)

## 7. Authorized Users of our services

### 7.1 Purpose

When we enter into an agreement with the company that you represent, we process your Personal Data in order to deliver the contracted services and in particular for the purpose of:

- Provide and manage access to our systems and services, including support services
- Ensure security and compliance with internal policies
- Monitor and audit usage to prevent unauthorised access or misuse

### 7.2 Categories of Personal Data

We may process:

- IP addresses
- Usernames
- Business Emails
- Business Phone
- Any potential Personal Data you voluntarily share with us

### 7.3 Legal Basis

The processing is based on:

- Art. 6(1)(f) - Legitimate interest (when the processing is necessary for our legitimate interests to communicate with you and fulfil the agreement with the company you represent and our legitimate interest to ensure secure systems and prevent unauthorised access or misuse)
- Art. 6(1)(a) - Consent
- Art. 6(1)(b) - Contractual Necessity (to fulfil the agreement when we enter into an agreement with you directly)
- Art. 6(1)(c) - Legal Obligation

## 7.4 Retention

We will retain your Personal Data:

- Personal Data is retained for the duration of your engagement with us, and maximum 1 year thereafter.
- We store and process your Personal Data in support matters for the period necessary for us to resolve your support matter.
- Duration of engagement plus 7 years for financial reporting

## 8. Recipients and International Transfers

To fulfill the purposes described above, we may need to share personal data with suppliers when they perform services on our behalf, mainly to provide and maintain IT systems and partners for recruitment. See the list below of our engaged processors.

Your personal data is generally only processed within the EU/EEA. In the event the data is transferred to a country outside the EU/EEA, as set out in the list below, we ensure that such transfer is lawful. If the European Commission does not consider that the country ensures an adequate level of protection, the transfer to the third party will be supported by the Commission's standard contractual clauses and, where applicable, supplemented with additional safeguards. Finally, your personal data may also be transferred to the United States, where applicable, and such transfers are based on the recipient being certified under the EU-US Data Privacy Framework Program.

| Name of processor             | Location of Processing        | Description of Processing         | Corporate Location | DPA                                  |
|-------------------------------|-------------------------------|-----------------------------------|--------------------|--------------------------------------|
| Atlassian (JIRA)              | Global                        | Ticketing System                  | USA                | <a href="#">Atlassian DPA</a>        |
| NextCloud                     | Sweden                        | File workspace and storage        | Germany            | <a href="#">NextCloud Privacy</a>    |
| Runbox                        | Norway                        | Email Communication               | Norway             | <a href="#">Runbox Privacy</a>       |
| IssTech AB                    | Sweden                        | Backup Administration and Support | Sweden             | Stored Internally                    |
| Hailey HR                     | Finland, Sweden               | ATS used to evaluate candidates   | Sweden             | <a href="#">Hailey HR DPA</a>        |
| LinkedIn – Recruitment        | USA, EU operations in Ireland | Used to link candidate CVs to ATS | USA                | <a href="#">LinkedIn DPA</a>         |
| Slack Technologies (optional) | USA, EU Operations            | Communication tool                | USA                | <a href="#">Slack Privacy Policy</a> |

## Optional Use of Shared Slack Workspace

We may offer access to a shared workspace in Slack as an optional way to communicate. Use of Slack is voluntary and it is not required to receive our services, which are available through other communication channels.

If you create an account with Slack and use the shared workspace, you may share your Personal Data, such as account information and contact details, with a third party. For information on how your Personal Data is processed by the third party, please see the privacy policy for Slack on its website.

Our processing will still be in accordance with this privacy policy or in accordance with an applicable data processing agreement.

## 9. Information Security Measures

We follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it. We maintain appropriate administrative, technical and physical safeguards to protect your personal data against accidental or unlawful destruction, accidental loss, unauthorized alteration, unauthorized disclosure or access, misuse, and any other unlawful form of processing of the personal data in our possession.

In accordance with ISO/IEC 27001, we maintain an Information Security Management System (ISMS) and apply appropriate technical and organisational measures, including:

- Risk assessment and risk treatment processes
- Access control based on least privilege
- Encryption in transit (TLS)
- Encryption at rest where appropriate
- Logging and monitoring
- Supplier security assessments
- Incident response procedures
- Business continuity planning
- Regular internal audits and management reviews

Personal data protection is integrated into our security governance framework.

Records of processing activities (ROPA) are maintained in accordance with GDPR Art. 30.

## 10. Automated Decision-Making

We do not engage in automated decision-making or profiling within the meaning of GDPR Art. 22, unless explicitly stated and legally permitted.

## 11. Third-Party Websites

Our website may contain links to third-party websites. Our processing will still be in accordance with this privacy policy, but when you have used these links to leave our site, you should exercise caution and inform yourself of the privacy statement applicable to the website in question. We are not responsible for their data processing practices.

## 12. Contact Us

If you have any questions about your rights, please feel free to contact us at [gdpr@safespring.com](mailto:gdpr@safespring.com)