Privacy Policy of JOIN

Version 3.0 – September 2026

About us

This privacy policy ("Privacy Policy") explains how we process and protect your personal data when you use this Website or our services provided via https://join.com (together, the "Services").

These Services are operated by JOIN Solutions AG, Eichenstrasse 2, 8808 Pfäffikon SZ (the "Company", "we", "our", or "us"). The Company is the controller for the data processing described below.

Unless otherwise defined in this Privacy Policy, the definitions used in this Privacy Policy have the same meaning as in the Swiss Federal Act on Data Protection (FADP) or the EU General Data Protection Regulation (GDPR).

In Germany, we have appointed an EU representative in accordance with Article 27 GDPR. If you are visiting us from the EU, you can also contact JOIN Solutions GmbH:

- by e-mail to: legal@join.com
- by mail to: JOIN Solutions GmbH, Schönhauser Allee 36, Berlin, 10435, Germany

For all questions on the subject of data protection, you can also contact our data protection officer (DPO) at any time. Our DPO can be reached:

- by e-mail to: dpo@lexr.com
- by mail to: LEXR Law Switzerland AG, Langstrasse 64, CH-8004 Zürich Switzerland

We expressly point out that if you use this e-mail address, the contents will not be exclusively noted by our DPO. If you wish to exchange confidential information, please therefore first contact us directly via: legal@join.com and mark the correspondence with: "F.A.O. data protection officer".

1. Our roles

1.1 As Data Controller

We act as a data controller in relation to the personal data processed when:

- You create, manage, and access your user accounts (candidate and employer logins)
- We process billing and payment data in connection with paid services
- We record personal data processed for a given application to simplify your future applications made via the Services (“Record Feature”).

These activities are governed by this privacy policy. We will provide further details on the nature of the data processed, the purposes of processing, and the corresponding legal bases in section 2 and following.

1.2 As Data Processor

When you apply for a specific job listing published via our platform as a candidate, we act as a data processor on behalf of a recruiting company (in that case the data controller) that has published the job offer ("Recruiting Companies", each a "Recruiting Company").

The Recruiting Company is responsible for the processing of such candidate's personal data (including but limited to contact details, CV, diplomas, certificates, etc.). Please refer to the data protection policy of the Recruiting Company to which you have submitted your application for detailed information on how your personal data is further processed.

As a data processor, we process personal data on behalf of the Recruiting Company and in accordance with our DPA.

2. Personal data we collect as a controller

We may collect or receive personal information for a number of purposes connected with our business operations when you use our Services, namely:

- Usage and analytics information (e.g., identifiers, numbers of clicks, tracking data)
- Contact details (e.g., name, address, phone number, birth date)
- Financial information (e.g., salary, income)
- Geolocation (e.g., your actual location, GPS data)
- Login details (e.g., password, username, session)
- Payment details (e.g., billing information, credit card details)

- Recruitment details if you apply to work at JOIN or for the Record Feature (e.g., CV, letter of motivation)
- Request details (e.g., details and content of your inquiries)
- Website visitor details (e.g., IP address, logfiles, terminal ID)

There is no obligation to provide your personal data. However, please note that our Services cannot be provided if you do not provide the required data strictly necessary for performing the contract between you and us.

3. How we collect personal data

We collect information about our users when they use our Services, including taking certain actions within it.

Directly

- Via our Website and electronic communication
- When you use our Services
- When you provide services to us
- When you correspond with us by electronic means using our Services
- When you browse, complete a form or make an inquiry while using our Services

Indirectly

- Through public sources
- From public registers (such as commercial registers), news articles and internet searches
- When our business customers engage us to perform professional services which involve them sharing personal data they control with us as part of that engagement

4. Legal Basis and purposes

Our legal basis for collecting and using the personal data described in this Privacy Policy depends on the personal data we collect and the specific purposes for which we collect it.

Contract: To perform our contractual obligations or take steps linked to a contract with you. In particular:

- To provide you with customer support
- To set up and manage your account, as well as to verify your credentials when logging in
- To recruit you for working at JOIN (and not at one of the Recruiting Companies)

- To provide our Services

Consent: We may rely on your freely given consent at the time you provided your personal data. In particular:

- To analyse, improve, personalise and monitor the usage of our Services and communication
- To place non-essential cookies and other tools on your browser
- To provide users with news, special offers, newsletters, and general information about goods and services which we offer
- For specific features of our Services that involve the sharing or extended processing of your personal data (such as the processing of sensitive data) your explicit consent may be required and will be obtained prior to such processing

Legitimate interests: We rely on legitimate interests based on our assessment that the processing is fair and reasonable and does not override your interests or fundamental rights and freedoms. In particular:

- To place essential cookies and other tools on your browser that are technically necessary for our Services
- To develop new services
- To maintain and improve our Services, as well as to detect, prevent, and address security threats

Necessity for compliance with legal obligations: To meet regulatory and public interest obligations. In particular:

- To notify you about changes to our Services and our Privacy Policy
- To comply with applicable regulations and legislation.
- For the legal enforcement of claims and rights.

5. Data retention

We retain personal data for so long as it is needed for the purposes for which it was collected and in line with legal and regulatory requirements or contractual arrangements. For the avoidance of doubt, such a purpose exists at least, for as long as you have an account with us. After this period, we delete or fully anonymize your personal data.

6. Data recipients

We engage third-party companies ("Service Providers") to facilitate the operation of our Services, assist in analysing the usage of the Services, or perform necessary

services, such as payment and the provision of IT services. These third parties have access to your personal data only to the extent necessary to perform these tasks.

Type(s) of Service Providers who might access your personal data:

- Job platforms posting job ads
- Professional advisers that we use, such as accountants and lawyers
- Third parties that are engaged in the course of your matter, such as counsels, banks and other payment providers, KYC/AML service providers, and postal or courier providers
- Other group entities that are involved in your matter
- Insurers
- Third parties who provide IT and software services
- Third parties who help us with client insights and marketing

In particular, we use the customer communication platform Front as a Service Provider to manage messages in our inboxes in order to streamline our internal operations. Front uses AI to suggest draft replies for our team to review and send, and can automatically send standardised replies to certain enquiries (rules-based AI replies). We do not use fully autonomous AI or make automated decisions with legal or similarly significant effects on you.

7. Data transfers

We and/or our Service Providers may transfer your personal data to and process it in the following countries:

- EU and EEA
- USA

We may use Service Providers partly located in so-called third countries (outside the European Union or the European Economic Area or Switzerland) or process personal data there, i.e., countries whose level of data protection does not correspond to that of the EU or Switzerland.

We safeguard your personal data per our contractual obligations and applicable data protection legislation when transferring data abroad.

Such safeguards may include:

- The transfer to countries that have been deemed to provide an adequate level of protection according to the Federal Council, as well as to countries where there is an adequacy decision by the European Commission in place

- Applying standard data protection model clauses, binding corporate rules or other standard contractual obligations that provide appropriate data protection

If a third country transfer takes place and there is no adequacy decision or appropriate safeguards, it is possible and there is a risk that authorities in the third country (e.g. intelligence services) can gain access to the transferred data and that the enforceability of your data subject's rights cannot be guaranteed.

8. Data disclosure

We may disclose your personal data in the good faith belief that such action is necessary:

- To comply with a legal obligation (i.e., if required by law or in response to valid requests by public authorities, such as a court or government agency)
- To protect the security of our Services and defend our rights or property
- To prevent or investigate possible wrongdoing in connection with us

9. Data Security

We take reasonable technical and organisational security measures that we deem appropriate to protect your stored data against manipulation, loss, or unauthorised third-party access. Our security measures are continually adapted to technological developments.

We also take internal data privacy very seriously. Our employees and the service providers that we engage are required to maintain secrecy and comply with applicable data protection legislation. In addition, they are granted access to personal data only insofar as this is necessary for them to carry out their respective tasks or mandate.

The security of your personal data is important to us but remember that no method of transmission over the internet or electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security. We recommend using antivirus software, a firewall, and other similar software to safeguard your system.

10. Your rights

10.1 Against the Company

When we act as a data controller (as outlined in Section 1.1), you have the below data protection rights. To exercise these rights, you may contact the above address or send an e-mail to: legal@join.com. Please note that we may ask you to verify your identity before responding to such requests.

- **Right of access:** You have a right to request a copy of your personal data, which we will provide to you in an electronic form.
- **Right to amendment:** You have the right to ask us to correct our records if you believe they contain incorrect or incomplete information about you.
- **Right to withdraw consent:** If you have provided your consent to the processing of your personal data, you have the right to withdraw your consent at any time with effect for the future. This includes cases where you wish to opt-out from marketing communications. 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 initially consented to unless there is another legal basis for processing. To stop receiving emails from us, please click on the 'unsubscribe' link in the email you received or contact us at legal@join.com.
- **Right to erasure:** You have the right to request that we delete your personal data when it is no longer necessary for the purposes for which it was collected or when it was unlawfully processed.
- **Right to restriction of processing:** You have the right to request the restriction of our processing of your personal data where you believe it to be inaccurate, our processing is unlawful, or where we no longer need to process it for the initial purpose, but where we are not able to delete it due to a legal obligation or because you do not want us to delete it.
- **Right to portability:** You have the right to request that we transmit your personal data to another data controller in a standard format such as Excel, if this is data which you have provided to us and if we are processing it on the legal basis of your consent or to perform our contractual obligations.
- **Right to object to processing:** Where the legal basis for our processing of your personal data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have a compelling legal basis for the processing which overrides your interests or if we need to continue to process the personal data for the exercise or defence of a legal claim.
- **Right to lodge a complaint with a supervisory authority:** You have the right of appeal to a data protection supervisory authority if you believe that the

processing of your personal data violates data protection law. The competent data protection authority in Switzerland is the Federal Data Protection and Information Commissioner (www.edoeb.admin.ch). In the EU and EEA, you can exercise this right, for example, before a supervisory authority in the Member State of your residence, your place of work or the place of the alleged infringement. You can find a list of the relevant authorities here: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en.

10.2 Against Recruiting Companies

For personal data we process solely as a data processor, your rights must be exercised against the relevant Recruiting Company. For more information, please consult the respective Recruiting Company's privacy policy.

11. Social Media and Links to Third-Party Apps and Websites

Our Services contain links to websites or apps that are not operated by us. When you click on a third-party link, you will be directed to that third party's website or app. We have no control over the content, privacy policies, or practices of any third-party websites or services.

We maintain online presences on social networks to, among other things, communicate with customers and prospective customers and to provide information about our products and Services. If you have an account on the same network, it is possible that your information and media made available there may be seen by us, for example, when we access your profile. In addition, the social network may allow us to contact you. As soon as we transfer personal data into our own system, we are responsible for this independently. This is then done to carry out pre-contractual measures and to fulfil a contract. For the legal basis of the data processing carried out by the social networks under their own responsibility, please refer to their data protection declarations. Below is a list of social networks on which we operate an online presence:

- LinkedIn: Privacy Policy

12. Newsletter

We may send newsletters and other notifications by email and through other communication channels and may deliver them with the help of third parties.

In principle, you must expressly consent to receive newsletters and other notifications from us, unless this is permitted for other legal reasons. We use "double opt-in" for any consent in the case of e-mails, i.e., you will receive an e-mail with a web link that you must click to confirm, so that no misuse by unauthorized third parties can take place. We may log such consents including Internet Protocol (IP) address, date and time.

Newsletters and other notifications may contain web links or tracking pixels that record whether an individual newsletter or notification has been opened, and which web links were clicked (performance measurement). Such web links and tracking pixels record the use of newsletters and other notifications. We use this statistical recording of usage, including success and reach measurement, in order to be able to offer newsletters and other notifications effectively and in a user-friendly manner, as well as permanently, securely and reliably, based on the reading habits of the recipients.

You can unsubscribe from newsletters and other notifications at any time and thereby object in particular to the aforementioned collection of usage. You can do so by contacting us directly or following the link included in the footer of each newsletter we send you.

13. Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We therefore encourage you to review this Privacy Policy periodically for any changes.

Changes to this Privacy Policy are effective when they are posted on this page.

14. Contact us

If you have any questions about this Privacy Policy, do not hesitate to get in touch with us at:

JOIN Solutions AG, Eichenstrasse 2, 8808 Pfäffikon SZ, legal@join.com.