Information on Personal Data Processing for Applicants

(Last updated: March 2026. We reserve the right to amend this notice where necessary to reflect legal or operational changes.)

At Solaris SE, we are committed to protecting your personal data and processing it responsibly and transparently in accordance with the General Data Protection Regulation.

1. Data Controller

   Solaris SE Cuvrystraße 53 10997 Berlin, Germany acts as the data controller within the meaning of Art. 4(7) GDPR.

   You can contact us at: recruitment@solarisbank.de

   You can contact our Data Protection Officer at: dataprotection@solarisgroup.com

2. Purposes and Legal Bases of Processing

   2.1. Recruitment Process

   When you apply for a position with us, we process your personal data for the purpose of:

   - assessing your suitability for the role,
   - communicating with you during the recruitment process,
   - arranging interviews, and
   - taking steps at your request prior to entering a potential employment or service contract.

   We process your personal data based on Article 6(1)(b) of the General Data Protection Regulation ("GDPR"). This provision permits the processing of personal data where it is necessary to take steps at your request prior to entering a potential employment contract. The processing of your personal data is necessary to assess your application and, where applicable, to take steps toward concluding an employment contract. If you do not provide the personal data required for the application process, we may be unable to properly assess your application or proceed with the recruitment process. The personal data processed may include:

   - First and last name
   - Contact details (email, telephone, address)
   - CV (education and professional history)
   - Cover letter
   - Certificates and references
   - Photo (if voluntarily provided)
   - Interview notes

- Offer and expectation letters
- Position, level, proposed start date

Where necessary, we also process applicant data based on Art. 6(1)(f) GDPR, which allows us to use your personal data to pursue our legitimate interests. These legitimate interests include:

- ensure an efficient and secure recruitment process,
- prevent fraud and safeguard company assets,
- defend and exercise legal claims,
- retain documentation for evidentiary purposes,
- improve recruitment processes.

We have conducted a balancing test and determined that our legitimate interests do not override your fundamental rights and freedoms. You have the right to object to this processing at any time (Art. 21 GDPR). This means that you can ask us to stop processing your personal data if you believe that our interests should not override your rights and freedoms. If you object, we will review your request and will stop processing your data unless we can demonstrate compelling legitimate grounds for continuing the processing that override your interests, rights, and freedoms, or unless the processing is necessary for the establishment, exercise, or defence of legal claims. You can exercise your right to object by contacting us using the contact details provided in Section 7.

2. Background Checks 2.2 Background Checks

If you reach the final stage of our recruitment process, we may carry out background checks where this is required or permitted by law, particularly for regulated roles in the financial sector. These checks help us verify the information you have provided and ensure that we meet our legal and regulatory obligations. Depending on the role, the checks may include:

- Verification of your professional and educational history
- Reference checks
- Identity verification
- Screening against sanctions lists
- Adverse media searches

For certain positions, we are required by Section 6(2) no. 5 of the German Money Laundering Act (Geldwäschegesetz – GwG) to carry out specific checks to verify your identity and ensure the integrity of our operations. The legal basis for this processing is Article 6(1)(c) GDPR, which allows us to process personal data to comply with a legal obligation.

Where background checks are not based on a specific statutory obligation but are necessary for the establishment of the employment relationship, the legal basis is § 26(1) of the German Federal Data Protection Act (BDSG) in conjunction with Article 6(1)(b) GDPR, which allows us to process personal data to take steps at your request prior to entering a potential employment contract. If, in exceptional cases, information relating to criminal convictions is processed, this will only take place where legally permitted and in accordance with Article 10 GDPR and applicable German data protection law. Such data will be handled with particular care and accessed only by authorised personnel. The personal data processed in this context may include:

- name and contact details
- identification documents
- educational background
- employment history
- references

3. Suitability Assessments for Regulated Functions

For certain regulated roles (e.g., Management Board members, Supervisory Board members, key function holders), we are legally required to conduct suitability assessments under Sections 25d and 25e of the German Banking Act (KWG) and applicable supervisory guidelines. The legal basis for this processing is Art. 6(1)(c) GDPR (legal obligation). If this is the case for you, you will be informed of this requirement in advance, and dedicated forms will be provided to collect the necessary information.

4. Special Categories of Personal Data

Some types of personal data are considered particularly sensitive under data protection law. This includes information such as health data, information about racial or ethnic origin, religious beliefs, or trade union membership. We do not actively request this type of information. If such data is included in your application documents, we will only process it where this is legally permitted, for example, where necessary to comply with employment law obligations or other regulatory requirements. Sensitive data is handled with special care, strict access controls, and enhanced security measures.

5. Employee Referral Program

We operate an employee referral program through which employees recommend potential candidates. If you are referred to us, we receive your personal data directly from the referring employee before you apply. The data received includes your name, contact details, CV, cover letter, and information relating to the referral. The source of the data is the referring employee. We process this data to identify and contact you and to assess your suitability for employment. The legal basis for this processing is Art. 6(1)(f) of the General Data Protection Regulation. Our legitimate interest lies in conducting an efficient recruitment process and filling vacancies through employee recommendations. Because we obtain your personal data from a third party, we provide you with information about this processing within

one month of receiving your data. This information includes the source of the data, the purposes of processing, the applicable retention period, and your data protection rights. You have the right to object to this processing at any time. If you apply, your personal data is processed based on Art. 6(1)(b) GDPR for the purpose of taking steps prior to entering a potential employment contract. The referring employee is informed whether the recruitment process has been completed. No evaluation details are disclosed.

6. Talent Pool

If your application is not successful, we may offer you the opportunity to join our talent pool. The legal basis is Art. 6(1)(a) GDPR (consent). If you provide consent, we will process your application data specified in section 2 to identify and contact you regarding future job opportunities. You may withdraw your consent at any time with effect for the future by contacting us, as described in section 7. Withdrawal does not affect prior processing. Providing consent is voluntary and does not affect your current application.

3. Data retention

- *Unsuccessful applications:* If your application is unsuccessful, your personal data will generally be deleted six (6) months after the conclusion of the recruitment process, unless you have consented to the talent pool.
- *Referral program data:* If we process your data in the context of the referral program and no further contact occurs, the referral data will be deleted six (6) months after receipt.
- *Talent pool consent:* If you have consented to the talent pool, your data will be stored for eighteen (18) months from the date of consent. If no suitable position is identified within this period, your data will be deleted unless longer statutory retention periods apply or you renew your consent.
- *Legally required background checks:* Where background checks are carried out to comply with a legal obligation (e.g., under Section 6(2) no. 5 of the German Money Laundering Act – GwG), documentation is retained in accordance with statutory requirements. Section 8 GwG generally prescribes a retention period of five years, unless longer retention is required in specific cases.
- *Background checks without statutory retention obligation:* Documentation of the outcome of such checks will generally be retained for up to one year from the date of acceptance of the employment offer, for compliance, audit, and documentation purposes, as well as for the establishment, exercise, or defence of legal claims.
- *Criminal record checks:* The certificate itself is retained only for the time necessary to complete verification. Generally, only a note that the check was completed and satisfactory is kept, for up to one year from the date of acceptance of the offer, unless longer retention is required by law.
- *Employee personnel files:* If you are hired as an employee, relevant recruitment data will become part of your personnel file and will be retained in accordance with our employee retention schedule. As a rule, personnel file documentation is retained for three years after termination of the employment relationship. However, longer retention periods may apply where required by statutory provisions, under commercial and tax law (between six and ten years pursuant to the German Commercial Code (Handelsgesetzbuch – HGB) and the German Fiscal

Code (Abgabenordnung – AO)), under social security law, or where documentation is relevant for pension entitlements. In addition, personal data may be retained for longer periods where necessary for the establishment, exercise, or defence of legal claims. Data will be deleted once the applicable retention obligation or limitation period has expired and no further legitimate purpose for retention exists.If your application is unsuccessful, your data will generally be deleted six (6) months after conclusion of the recruitment process, unless you have consented to the talent pool.

4. Data Sharing and International Transfers

Your personal data is shared internally only with employees involved in the recruitment process and with service providers. We use service providers acting as processors pursuant to Art. 28 GDPR, including:

- **Greenhouse Software Inc:**

  Greenhouse Software, Inc. provides our applicant tracking system. Applicant data, including CVs, cover letters, interview notes, and recruitment documentation, is processed and stored on Greenhouse servers located in the European Union. Greenhouse Software, Inc. is headquartered in the United States and is covered by adequacy decision provided by the EU Commission by being registered in the EU–US Data Privacy Framework. This is an administrative agreement that allows U.S. companies to receive personal data from the EU with GDPR-level protections.

- **Zinc Work Ltd**

  Zinc Work Limited provides background screening services. Personal data required for screening is processed and stored within the United Kingdom and the European Union. The United Kingdom benefits from an adequacy decision adopted by the European Commission pursuant to Art. 45 GDPR.

- **Egnyte Inc**

  Egnyte, Inc. provides secure document storage services. Egnyte, Inc. is headquartered in the United States. Personal data is stored on servers located within the European Union. Any international transfer is based on Standard Contractual Clauses pursuant to Art. 46 GDPR.

- **Personio SE & Co. KG**

  Personio SE & Co. KG provides human resources management services. Personal data is processed and stored in data centres located in Germany and within the European Union. No transfer to third countries takes place in this context.

- **Amazon Web Services (AWS, Frankfurt am Main, EU)**

  Amazon Web Services provides cloud infrastructure services. Personal data is stored in the AWS data centre located in Frankfurt am Main, Germany.

  Amazon Web Services, Inc. is headquartered in the United States and is certified under the EU–US Data Privacy Framework adopted under the European Commission adequacy decision pursuant to Art. 45 GDPR. Where required, transfers are additionally safeguarded by Standard Contractual Clauses pursuant to Art. 46 GDPR.

- **Solaris Digital Solutions Private Limited**

  Solaris Digital Solutions Private Limited provides support at running the employee referral program. Personal data is processed in India.

  India does not benefit from an adequacy decision under Art. 45 GDPR. Transfers are therefore based on Standard Contractual Clauses adopted by the European Commission in accordance with Art. 46 GDPR, supplemented by technical and organizational measures to ensure an adequate level of protection.

5. Automated Decision-Making

We do not use automated decision-making, including profiling, within the meaning of Art. 22 GDPR that produces legal effects or similarly significant effects. All recruitment decisions involve meaningful human review.

6. Information Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure, or destruction.

7. Your Rights

You have the rights of access, rectification, erasure, restriction of processing, data portability, objection, and the right to lodge a complaint with a supervisory authority.

You may lodge a complaint with the Berlin Commissioner for Data Protection and Freedom of Information:

Address: Alt-Moabit 59-61, 10555 Berlin, Germany

Email: mailbox@datenschutz-berlin.de

Website: https://www.datenschutz-berlin.de

For exercising your rights, you can contact us according to the information provided in Section 1.