



2026
September

Candidate privacy policy

VERSION	DESCRIPTION	PREPARED	REVIEWED

1. Who we are

Members of Gunvor Group ('we', 'our', 'us') will always aim to be in compliance with the EU General Data Protection Regulation 2016/679 ('GDPR'), the Swiss Federal Act on Data Protection ('FADP') and other applicable privacy laws. We use Workday, an online application provided by Workday Inc., to assist with our recruitment process. We use Workday to process personal information as a data processor on our behalf. Workday is only entitled to process your personal data in accordance with our instructions. If you wish to have more information about Workday's privacy policy, please click on the page 'Privacy Statement | Workday'. This Privacy Policy only applies to the personal data of job applicants and potential candidates for employment. We also use Tradermath B.V. ("Tradermath"), where applicable, to provide online candidate screening and assessment services, including assessment delivery, scoring and remote proctoring. Tradermath processes candidate personal data on our behalf and in accordance with our instructions and applicable contractual and data protection safeguards.

2. For what purpose and on what legal basis do we collect your personal data?

We process your personal data to recruit and select staff for Gunvor and to compile a pool of potential future candidates before the employment contract. Our processing of your personal data for the purposes mentioned above is based on the following legal basis:

- » in part, on our legitimate business interest in evaluating your application and managing online assessments, to manage our relationship with you, to ensure that we recruit appropriate employees, and to evaluate and maintain the efficacy of our recruiting process more generally;
- » in part, on the performance of contractual and precontractual measures relating to our potential employment relationship with you and online candidate assessments;
- » in part, on our compliance with applicable law with regard to personal data necessary to satisfy our legal or regulatory obligations
- » in part, on your consent, if we offer you the opportunity to participate in our optional recruiting programs or if we collect sensitive personal data, to the extent permitted by applicable law.

We may also process your personal data to run certain background checks designed to verify the information provided to us by you.

3. What kind of personal data do we collect and why?

Personal data is any information relating to an identified or an identifiable natural person who can be directly or indirectly identified by reference to an identifier. We may process the following categories or types of personal information about you:

- » Name
- » Address
- » Phone number
- » Email address
- » Legally allowed to work in the country
- » Highest academic qualification
- » Salary expectation
- » Motivation
- » LinkedIn Address
- » HuKou Address
- » Reference information and/or information received from background checks (where applicable), including information provided by third parties
- » All the information that you choose to share with us via your CV
- » Any other information in your application that you choose to share with us – such as previous work experience or previous job application with us or the existence of any relatives working for us.

Where you participate in an online assessment, we may additionally process:

- » assessment responses, including answers to questions and coding exercises
- » scores, rankings and assessment results
- » webcam video and audio recordings where remote proctoring is used
- » technical information such as IP address, browser and device information, timestamps and activity logs

- » assessment integrity indicators, such as tab-switching events, plagiarism indicators and other signals of potential assessment irregularities. Video and audio recordings are not intended to be used for facial recognition, biometric identification or to infer sensitive characteristics about candidates.

4. How do we collect your personal data?

Your personal data is obtained via Workday and, where applicable, the Tradermath assessment platform, as well as from the attachments and information that you choose to share during your application and assessment.

5. Do we share your personal data with third parties?

We may share within the Gunvor Group the personal data you provide us with for purposes connected with your job application. We may perform some of our operations by relying on third-party suppliers. The personal data that you provide may be shared with these suppliers in order to enable them to perform the required tasks. However, these suppliers are required to exclusively use the received information for the respective services on our behalf and as instructed by us and they are obliged to comply with the applicable data protection regulations. Third parties may have access to your personal data without your consent if there is a legal basis for it.

6. How do we transfer your personal data?

Where a data transfer may be necessary, we will take necessary steps to ensure that your personal data has the level of protection required by applicable data protection laws, including, where applicable, the GDPR and the Swiss FADP. We will notify you and seek your consent to processing, in each case if required. In any situations where a job application is received for another location outside of our job vacancy designated jurisdiction, that application will be transferred via email to the appropriate location for processing. In case of transfer to an entity located outside the European Economic Area, we will act appropriately to ensure the personal data has the level of protection as required by the GDPR and local data protection laws. Some of our recruitment service providers or their sub-processors may process or access personal data from countries outside Switzerland, the European Economic Area or the country in which you applied. Where such transfers occur, we implement appropriate safeguards in accordance with applicable data protection laws.

7. Where is your personal data stored?

We store your personal data in Workday data centers (software as service – SaaS) and our data centers (that may be provided by service providers i.e. external data centers). Candidate assessment data may also be stored in systems operated by Tradermath and its authorised sub-processors in accordance with the applicable contractual, security and international-transfer safeguards.

8. How long will your data be stored for?

As a matter of principle, personal data is retained

- (i). for as long as needed to achieve the purposes as described in this policy, or
- (ii). for a longer period if we have a specific legal basis that requires such longer storage period.

We will delete or anonymise personal data (or equivalent) once they are no longer necessary to achieve the purposes for which they have been collected, subject however

- (i). to any applicable legal or regulatory requirements to store personal data for a longer period, or
- (ii). to establish, assert, exercise and/or defend actual or potential legal claims, investigations or similar proceedings, including legal holds.

Specific retention periods apply to candidate assessment information: audio and video recordings generated for assessment proctoring are retained for up to three months, and assessment data and results are retained for up to twelve months. Such data is deleted or anonymised following expiry of the applicable retention period, subject to any legal requirements or the need to establish, exercise or defend legal claims.

9. Your privacy rights

You have the right, subject to the applicable local data protection legislation, to:

- » request access to, and receive a copy of, the personal data we hold about you (Right to access, Art. 15 GDPR);
- » if appropriate, request rectification or erasure of the personal data that are inaccurate (Right to rectification, Art. 16 GDPR);

- » request the erasure of the personal data, subject, however, to applicable retention periods (Right to be forgotten, Art. 17 GDPR);
- » request a restriction of processing of the personal data where the accuracy of the personal data is contested, the processing is unlawful or if the data subjects have objected to the processing (Right to restriction of processing, Art. 18 GDPR);
- » object to the processing of the personal data (Right to object, Art. 21 GDPR);
- » receive the personal data in structured, commonly used and machine readable format (Right to data portability, Art. 20 GDPR);
- » complain in relation to the processing of the personal data and, absent a satisfactory resolution of the matter, file a complaint in relation to the processing of the personal data with the competent data protection supervisory authority, including the competent Swiss authority where the Swiss FADP applies.

If you object to the processing of your personal data, we will no longer process the personal data unless we have compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. Subject to the limitations set forth herein and/or in applicable local data protection laws, you can exercise the above rights free of charge by contacting us at: privacy@gunvorgroup.com Where an assessment score, AI-assisted result or integrity indicator has materially influenced the recruitment process, you may contact us if you have concerns about the result and request that the circumstances be reviewed by an appropriate member of the recruitment team. No hiring or rejection decision should be based solely on an AI-generated result or an integrity flag without appropriate human involvement.

10. How do we protect your personal data?

We have established the security of your personal data in accordance with applicable data protection principles, including the GDPR and Swiss FADP where applicable. The measures taken are technical and organisational measures relating to data security in order to guarantee an adequate level of protection regarding confidentiality, integrity, availability of the data and resilience of the systems. Technical measures are those that directly involve the IT system. Organisational measures, on the other hand, are related to the system's environment and processes and particularly to the people using it. The combination of both types of measures is designed to prevent (i) data from being destroyed or lost by mistakes and (ii) fakes and unauthorised access from occurring. These measures are part of the life cycle of our organisation and are implemented at every level of the system. Furthermore, security is an ongoing process, not a static element. In this perspective, the technical and organisational measures are subject to technical progress and further development as risks and threats do.

11. Cookies Our website use cookies.

A cookie is a small text file placed on your computer or mobile device when you visit a website or use an app. Cookies collect information about users and their visit to the website, such as their Internet protocol (IP) address, how they arrived at the website (for example, through a search engine or a link from another website) and how they navigate within the website or app. We use cookies and other technologies to facilitate your internet sessions, track use of our websites and apps and to compile statistics about activities carried out on our websites and. A pixel tag, also known as a web beacon, is an invisible tag placed on certain pages of our website but not on your computer. Pixel tags are usually used in conjunction with cookies and are used to monitor the behavior of users visiting the website. You may set up your web browser to block cookies which will in turn disable the pixel tags from monitoring your website visit. You may also remove cookies stored from your computer or mobile device. However, if you do block cookies and pixel tags, you may not be able to use certain features and functions of our websites.