

Privacy Notice for Recruitment

Effective Date: 12 March 2025

1. Who is responsible for your personal data?

The company in the Cellmark group to which you apply is the controller of your personal data for the purposes of recruitment. As the controller, it determines why and how your personal data is processed.

CellMark AB, Swedish corporate identity number 556244-2433, with address PO Box 11927, SE-404 39 Gothenburg, Sweden, telephone number +46(0)31-100 300 acts as a processor on behalf of the group company mentioned above. This means CellMark AB processes your personal data according to the instructions of that entity and only for the purposes outlined in this Privacy Notice.

If you have questions about who is the controller for the specific position you have applied for, or how CellMark AB assists with processing your data, please contact our Data Protection Coordinator as indicated in section 6 below.

2. Details on the data we process about you

Below is a consolidated overview of why we process your data, what categories of data are involved, the legal basis for processing, and how long we typically keep it.

Purpose	Data Categories	Legal Basis	Retention Period	Source
A. Administer Your Application - Evaluate your skills and experience, communicate with you, arrange interviews and tests	Contact details (name, email, phone, address). Information from your CV and cover letter. Interview notes. Test results (if any). Background checks, if applicable – see details below. Information from	Contract necessity - steps prior to entering an employment contract (GDPR Art. 6.1.b)	Active Recruitment/ Hired: Data retained for the duration of the process, and if successful data is transferred to the employee file. Not Hired / Withdrawn: Erased 6 months after application date, unless consent is given to be kept in the database for future opportunities	You - when you apply for one of our jobs. Recruitment agencies we use – when your application data is given to us by a recruitment agency you have given your data to. Test providers. People that act as your references.

Purpose	Data Categories	Legal Basis	Retention Period	Source
	your references, e.g. about your personal characteristics and qualifications.		(see D below).	Background check companies.
B. Background checks	<p>For employees with access to sensitive information – identity documents, employment history, professional references, criminal records (where allowed under the law).</p> <p>For sensitive or high risk positions we additionally perform a financial audit and check previous board positions.</p> <p>In the United States a criminal record check is conducted for all positions</p>	Your consent (GDPR Art. 6.1.a), unless applicable national law provides another basis.	<p>Active Recruitment/ Hired: Data retained for the duration of the process, and if successful data is transferred to the employee file.</p> <p>Not Hired / Withdrawn: Outside of the US - erased 6 months after application date, unless consent is given to be kept in the database for future opportunities (see D below). In the US: 1 year from application.</p>	Background check companies, and you directly.
C. Defend Against Claims - Handle legal disputes (e.g., discrimination claims)	Same categories as under “A”	Legitimate interest in defending legal claims (GDPR Art. 6.1.f)	Retained for 6 months after the recruitment process, or until the dispute is resolved if arisen.	Same as under “A”
D. Match You to Future Positions - Keep your data on file for upcoming or open positions that might suit your profile	Same categories as under “A”.	Your consent (GDPR Art. 6.1.a), which is requested at the end of the recruitment process and renewed every 6 months.	6 months on a rolling basis, provided you renew your consent.	Same as under “A”

With the exception of the USA where we criminal records for all employees, we perform background checks for the final candidates in some of our positions – namely sensitive or high-risk positions, and employees with access to sensitive information. During the background checks we verify identity, employment, professional references, criminal records (where allowed under the law). For sensitive or high risk positions we additionally check criminal records and we perform a financial audit and check previous board positions. We do this as a risk-based approach, to prioritize and maintain a safe workplace.

We do not take automated decisions with legal or other significant effect in the course of our processing and we do not sell data.

3. Who can gain access to your personal data?

- **Sharing Within Our Group**

- We share your data with group entities if relevant to your application (e.g., the position is based in another group company), as well as for administration of recruitment. As mentioned previously, CellMark AB is a processor for all companies in the group.

- **Recruitment companies**

- We work with recruitment companies that source candidates for our job openings. They operate as separate controllers, and as such have access to the data you give to them.

- **Test Providers**

- Some of our roles involve tests. If you complete a test, the company administering the test processes your data on our behalf and is a data processor for us. However, we don't have access to your answers but only the general outcome of the test, which we use to determine compatibility with our company culture and environment.

- **Background check companies**

- If you are a final candidate for a position that requires background checks, we will use reputable background check companies depending on the jurisdiction. These are limited in their data processing to the purposes instructed by us (as processors), and have robust security measures in place.

- **IT Service Providers**

- Our IT services providers are processors which process your data as instructed by us and under confidentiality.
- We use digital communication and productivity tools (like Microsoft 365), as well as the recruitment platform Teamtailor.

- **Legal or Regulatory Disclosure**

- We may disclose data if required by law or a binding legal request.

4. Transfers

The controller processes your data in their own jurisdiction, as well as in the European Economic Area through CellMark AB as processor. Our use of IT services providers includes transfers of personal data from the EEA to The United States, which are performed under the Data Privacy Framework.

5. Security measures

We apply technical and organizational measures to protect your data, such as access controls, secure servers, and encryption (where appropriate). We also regularly review and update our security practices.

6. Your rights with regard to the processing of your personal data

- **Access:** Request a information about or a copy of the personal data we hold about you.
- **Rectification:** Correct or update inaccurate/incomplete data.
- **Erasur:** Ask us to delete data no longer needed or unlawfully processed.
- **Restriction:** Limit the processing of your data under certain conditions (e.g., if accuracy is contested).
- **Objection:** Object to processing based on legitimate interests; we will stop unless we have compelling grounds.
- **Portability:** Receive data you provided in a structured, commonly used format (for processing based on contract or consent).
- **Withdraw Consent:** If processing is based on your consent, you can withdraw consent at any time with effect for the future, without affecting prior processing.
- **Complaint:** Lodge a complaint with the data protection authority in your country.

To exercise any of these rights you can use the form available at <https://www.cellmark.com/about/privacy-law/>. Alternatively, you can contact us at dataprotection@cellmark.com. We generally respond within one month, unless legally required to respond faster.

7. Updates to This Notice

We may update this Notice to reflect changes in our data practices or legal requirements. We will post any revised Notice on our website and indicate the “Effective Date” date at the top.

8. Contact Us

If you have questions about this Notice or wish to exercise any rights, feel free to contact us:

Email: dataprotection@cellmark.com

Phone: +46(0)31-100 300

Thank you for your interest in joining CellMark!
