EMBLA MEDICAL®

Employee Privacy Notice

Personal data, or personal information, is any information that can be used to identify you.

Our goal is to ensure transparency about our data practices and to help you understand your rights and choices regarding your personal data. By providing this notice, we aim to describe how we collect and use personal data about you during and after your working relationship with us.

This privacy notice applies to all current and former employees, as well as to other persons performing work or providing services for us, regardless of the basis of their employment, including interns, contractors and part-time personnel.

We keep our employee privacy notice under regular review. This version was last updated on 30 August, 2026.

Who is the controller of your personal data?

Embla Medical hf. is a “data controller”. This means that we are responsible for deciding how and why your personal data is used. As a data controller, we ensure that all processing of personal data complies with applicable data protection laws, including the General Data Protection Regulation (GDPR).

Embla Medical is made up of different legal entities. This privacy notice is issued on behalf of the Embla Medical group so when we mention “Embla Medical”, “we”, “us” or “our” in this privacy notice, we are referring to the relevant company in the Embla Medical group responsible for processing your data.

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, or our privacy practices, please contact the DPO at:

Embla Medical hf.
Grjóthláls 5, 110 Reykjavík, Iceland
dpo@emblamedical.com

Which types of your personal data are collected?

We may collect, use, store and process different kinds of personal data about you which we have grouped together as provided below.

Embla Medical maintains offices and employs staff across multiple countries, each subject to distinct legal frameworks. Please note that not all jurisdictions require the collection of every data category listed. If you would like to get information about your local conditions, please contact your HR Business Partner or the Global Privacy & Compliance Team.

Identity Data:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependents.
- Next of kin and emergency contact information.
- National Insurance or health insurance number.
- Copy of driver’s license and passport.
- U.S. Veteran’s status.

Financial Data:

- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.

Professional Background Data:

- Recruitment information (including, when necessary, copies of the right to work documentation, references and other information included in a resume or cover letter or as part of the application process).
- Prior work information and education records.

Employment Data at Embla Medical:

- Employment start date and end date.
- Location of employment or workplace.
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history (only your compensation history at Embla Medical, unless we are legally permitted to and do inquire about previous compensation history).
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Information obtained through electronic means, such as records from access cards used to enter or exit the workplace.

Image:

- Footage from security cameras.
- Photographs and videos.

Sensitive Data:

- Information about your race or ethnicity.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Biometric data.
- Information about criminal convictions and offences.
- Disability information.

To begin and maintain your employment, we require certain information from you. Most of the above-mentioned data is essential for fulfilling our employment obligations, including processing your salary and providing workplace benefits. Additionally, some information is necessary for us to comply with legal requirements, such as ensuring workplace health and safety. While certain data may be optional, choosing not to provide required information may affect our ability to proceed with employment-related processes or meet legal obligations.

Please note that the data is only collected if allowed under law, consent has been obtained if required under law, and there is a legitimate need for it, such as to meet regulatory reporting requirements. Some of the information listed above is only collected to provide employee benefits, such as health insurance benefits.

How is your personal data collected?

We collect personal data about you directly from you during and after your working relationship with us, including through onboarding, benefits administration, payroll, performance management, and other employment-related processes.
We may also collect information from third parties where relevant and lawful, such as former employers or background check providers.

Why do we use your personal data (for non-U.S. employees)?

This section applies to employees located outside the United States of America.

We have set out below, in a table format, the purposes for which we may process your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

PURPOSE/ACTIVITY	TYPES OF DATA	LAWFUL BASIS FOR PROCESSING
Determining the terms on which you work for us.	▪ Professional background data. ▪ Employment data. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records).	▪ Legitimate interest – workforce management (establishing appropriate working conditions and responsibilities based on your data). ▪ Condition for processing sensitive data: processing is necessary for the assessment of the working capacity of the employee.
Checking if you are legally entitled to work in the applicable country.	▪ Identity data. ▪ Professional background data. ▪ Image.	▪ Legal obligation.
Paying your salary and deducting tax and the required fees.	▪ Identity data. ▪ Financial data. ▪ Employment data. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records; trade union membership).	▪ Legal obligation. ▪ Condition for processing sensitive data: processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment, social security and social protection law.
Providing the applicable benefits to you.	▪ Identity Data (e.g.: age, marital status). ▪ Financial Data. ▪ Employment Data. ▪ Sensitive Data (information about your health, including any medical condition, health and sickness records).	▪ Performance of a contract with you. ▪ Condition for processing sensitive data: Processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment, social security and social protection law.
Liaising with your pension provider.	▪ Identity data. ▪ Financial data.	▪ Legal obligation.
Administering the contract we have entered with you.	▪ Identity data. ▪ Financial data. ▪ Employment data.	▪ Performance of a contract with you.
Business management and planning, including accounting and auditing.	▪ Financial data. ▪ Employment data.	▪ Legitimate interest – operational efficiency (using your data to optimize workforce planning and resource allocation).

PURPOSE/ACTIVITY	TYPES OF DATA	LAWFUL BASIS FOR PROCESSING
Conducting performance reviews, managing performance and determining performance requirements.	▪ Employment data.	▪ Legitimate interest – workforce assessment (evaluating your performance to ensure alignment with business goals).
Making decisions about salary reviews and compensation.	▪ Financial data. ▪ Employment data.	▪ Legitimate interest – fair compensation (ensuring salaries align with industry standards and employee contributions).
Assessing qualifications for a particular job or task, including decisions about promotions.	▪ Professional background data. ▪ Employment data.	▪ Legitimate interest – merit-based decision-making (evaluating qualifications to ensure promotions and job assignments are fair and based on skills).
Gathering evidence for possible grievance or disciplinary hearings.	▪ Employment data. ▪ Image.	▪ Legitimate interest – ensuring workplace fairness (investigating complaints and grievances to ensure a fair and respectful work environment).
Making decisions about your continued employment or engagement.	▪ Financial data. ▪ Professional background data. ▪ Employment data. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records; trade union membership)	▪ Legitimate interest – workforce planning (using objective criteria to assess employee performance and suitability for continued employment). ▪ Condition for processing sensitive data: processing is necessary for the assessment of the working capacity of the employee.
Making arrangements for the termination of our working relationship.	▪ Identity data. ▪ Employment data.	▪ Legitimate interest – ensuring an organized offboarding (using your data to optimize processes regarding terminating the working relationship).
Education, training and development actions.	▪ Professional background data. ▪ Employment data.	▪ Legitimate interest – workforce development (enhancing employee skills to meet business needs and keeping them updated with the latest industry trends and technologies).

PURPOSE/ACTIVITY	TYPES OF DATA	LAWFUL BASIS FOR PROCESSING
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	▪ Identity data. ▪ Employment data. ▪ Image. ▪ Sensitive data (trade union membership).	▪ Legitimate interest – legal defense and pursuing claims (dealing with legal disputes in order to take care of the company's interests). ▪ Condition for processing sensitive data: processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.
Ascertaining your fitness to work.	▪ Employment data. ▪ Professional background data. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records).	▪ Legal obligation. ▪ Condition for processing sensitive data: processing is necessary for the assessment of the working capacity of the employee.
Managing sickness absence.	▪ Employment data. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records).	▪ Legal obligation. ▪ Condition for processing sensitive data: processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment, social security and social protection law.
Complying with health and safety obligations.	▪ Identity data. ▪ Employment data. ▪ Image. ▪ Sensitive data (information about your health, including any medical condition, health and sickness records).	▪ Legal obligation. ▪ Condition for processing sensitive data: processing is necessary for the purposes of carrying out the obligations and exercising specific rights in the field of employment, social security and social protection law.
To monitor your use of our information and communication systems.	▪ Identity data. ▪ Employment data.	▪ Legitimate interest – assuring relevant levels of cybersecurity (protecting company systems from unauthorized access, malware, and cyber threats, as well as ensuring compliance with our IT policies).
To ensure network and information security, including preventing unauthorized access to our computers and electronic communications systems and preventing malicious software distribution.	▪ Identity data. ▪ Employment data.	▪ Legitimate interest – assuring relevant levels of cybersecurity (protecting company systems from unauthorized access, malware, and cyber threats, as well as ensuring compliance with our IT policies).

PURPOSE/ACTIVITY	TYPES OF DATA	LAWFUL BASIS FOR PROCESSING
To conduct workforce analytics studies, using employee data where necessary and, where possible, aggregated or anonymized results, to review and better understand employee retention and attrition rates.	▪ Identity data. ▪ Professional background data. ▪ Employment data.	▪ Legitimate interest – workforce optimization (identifying trends in employee retention to improve hiring and retention strategies).
Equal opportunities monitoring (where allowed by law).	▪ Identity data. ▪ Professional background data. ▪ Employment data.	▪ Legitimate interest – ensuring workplace diversity (assessing hiring and promotion trends to ensure equal opportunities).
For work related travel arrangement.	▪ Identity data.	▪ Legitimate interest – workforce mobility (enabling employee movement for meetings, training, or third-party engagements).
Providing required employee information as part of participating in tenders and applying for grants.	▪ Employment data.	▪ Legitimate interest – applying for grants and participating in tenders.
Managing access to technology systems and infrastructure. Monitoring for and managing information security, privacy, and cybersecurity threats and incidents.	▪ Geolocation information. ▪ IP address information.	▪ Legitimate interest – assuring relevant levels of cybersecurity (protecting company systems from unauthorized access, malware, and cyber threats, as well as ensuring compliance with our IT policies).
For optional technical features, such as voice recognition in Microsoft Teams.	▪ Identity data. ▪ Sensitive data (biometric data, such as your voice).	▪ Consent. ▪ Condition for processing sensitive data: explicit consent.

The technical features which use biometric data, including voice recognition in Microsoft Teams or facial recognition on iPhone devices, are completely voluntary. Employees may choose whether to provide biometric data for purposes such as creating a voice profile or using facial scanning to unlock their phone. Choosing not to enroll in these features will not limit access to core systems or employment-related tools, nor will it result in any discrimination or unequal treatment.

Why do we use your personal data (for U.S. employees)?

This section applies to employees located in the United States of America. The table below outlines the categories of personal data we collect (and have collected over the past twelve months), examples of personal data we collect, and the purposes for which such data may be processed.

CATEGORY OF PERSONAL DATA	EXAMPLES OF PERSONAL DATA WE COLLECT	PURPOSE
Identifiers.	▪ A real name. ▪ Alias. ▪ Postal address. ▪ Internet protocol address. ▪ Email address. ▪ Social Security number. ▪ Driver's license or other government identification number. ▪ Passport number. ▪ Employee identification number, or other similar identifiers.	▪ To onboard personnel; enroll and administer benefits; enter into contracts; and carry out general human resource purposes. ▪ To build required skills in the workforce through needs assessments, deployment and delivery of learning solutions, and measurement of skill adoption. ▪ To provide training and short- and long-term professional development, and to manage employee performance, including establishing performance plans, monitoring and reviewing performance, and providing counselling. ▪ To review Personal Information provided by a whistleblower and information collected as part of investigations into whistleblowing concerns, including any necessary follow-up actions. ▪ To collect and review relevant information, such as emails, attendance records, performance notes, CCTV footage, or witness statements, in order to understand the circumstances surrounding a grievance or alleged misconduct.

CATEGORY OF PERSONAL DATA	EXAMPLES OF PERSONAL DATA WE COLLECT	PURPOSE
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	▪ A name. ▪ Signature. ▪ Social Security number. ▪ Physical characteristics or description. ▪ Address. ▪ Telephone number. ▪ Passport number. ▪ Driver's license or state identification card number. ▪ Insurance policy number. ▪ Education. ▪ Employment, employment history. ▪ Bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. ▪ Some personal data included in this category may overlap with other categories.	▪ To process job applications; onboard personnel; enroll and administer benefits; enter into contracts; and support general human resource activities. ▪ To process pay-related information, including pay rates, payroll deductions, banking details for direct deposit, and credit card details for expense reimbursement, in order to pay employees and comply with applicable laws. ▪ To carry out activities related to the development and management of centralized or regional business strategy and operations through third parties supporting business travel, meetings, and events for legal entities or organizational units. ▪ To record and manage sickness absence details, including dates of absence, reported reasons, and supporting documentation such as medical or fit notes.
Characteristics of protected classifications under state or federal law.	▪ Age. ▪ Race. ▪ Ancestry. ▪ National origin. ▪ Immigration status. ▪ Citizenship. ▪ Marital status. ▪ Disability. ▪ Gender identity. ▪ Veteran or military status.	▪ To collect equality and diversity information, such as minority, veteran, or disability status, through voluntary self-disclosure or other lawful sources, and to use such information only where and to the extent permitted by applicable law, including compliance with legal obligations and support of lawful diversity or equal opportunity initiatives. ▪ To collect and process health and safety information in order to maintain a safe workplace, assess working capacity, administer occupational health and workers' compensation programs, and comply with applicable laws. ▪ To collect and process information necessary for benefits enrollment and benefits administration purposes.

CATEGORY OF PERSONAL DATA	EXAMPLES OF PERSONAL DATA WE COLLECT	PURPOSE
Professional or employment-related information.	▪ Current or past job history or performance evaluations. ▪ Corporate expense information. ▪ Salary information. ▪ Tax rates. ▪ Retirement fund information, compensation information, bonus information, benefits information, or stock option information.	▪ To manage the relationship with personnel. ▪ To forecast human capital needs and manage workforce-related metrics and workforce information. ▪ To verify, document, and securely store evidence of work-authorization checks, including copies of reviewed documents and verification dates, in order to comply with immigration and employment laws. ▪ To analyze performance data, managers' feedback, and documented achievements to support fair and evidence-based decisions regarding career progression or advancement opportunities. ▪ To monitor compliance with safety procedures, track completion of required certifications, and share relevant information with managers or safety officers to meet legal and organizational health and safety requirements.
Internet or other electronic network activity information.	▪ IP address information. ▪ Logs of activity on company systems - such as software usage, internet browsing records, access to shared drives, or login times.	▪ To protect the company, customers, and personnel, including property, equipment, and confidential information, and to ensure company systems are used appropriately and securely. ▪ To monitor for and manage information security, privacy, and cybersecurity threats and incidents.

CATEGORY OF PERSONAL DATA	EXAMPLES OF PERSONAL DATA WE COLLECT	PURPOSE
Biometric Information.	▪ Fingerprints. ▪ Facial geometry. ▪ Voice recordings.	▪ To process fingerprint data where required by law and for legally permitted background-check purposes. ▪ To process fingerprint data in certain locations for timekeeping and attendance purposes, including the use of physical time clocks for hourly employees as an alternative to manual time entry systems. The time clock fingerprint data is encrypted and stored by the timeclock system as mathematical templates, and we only see a digital value - the raw images are never stored. ▪ To enable optional technical features, such as voice recognition or live transcription tools in Microsoft Teams, by processing audio input to convert speech into text during meetings or calls, where such features are voluntarily activated. ▪ To enable optional facial recognition features on work-issued devices, such as Face ID, where chosen by the user.
Geolocation Data.	▪ Geolocation information. ▪ GPS information. ▪ IP address information.	▪ To manage internal and external access to technology systems and infrastructure. ▪ To monitor for and manage information security, privacy, and cybersecurity threats and incidents.
Legal and Contractual Information.	▪ Name. ▪ Contact information. ▪ Employment information. ▪ System activity logs. ▪ Social Security Number.	▪ To comply with legal and contractual requirements and to establish, exercise, or defend legal and contractual rights or claims. ▪ To obtain legal advice including compliance with legal, regulatory, tax, and reporting obligations.

CATEGORY OF PERSONAL DATA	EXAMPLES OF PERSONAL DATA WE COLLECT	PURPOSE
Emergency Contact Information.	▪ Name and contact information. ▪ Relationship to Employee.	▪ To contact designated emergency contact persons in the event of an emergency involving an employee.
Beneficiary Information.	▪ Name and contact information. ▪ Relationship to the Employee. ▪ Birth date. ▪ Social Security Number. ▪ Information necessary to process benefits claims.	▪ To enroll and administer benefits programs for employees' beneficiaries and dependants.

Some of the Personal Data listed above are considered Sensitive Personal Information under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CPRA"). You have the right, at any time, to direct us to limit the use and disclosure of your Sensitive Personal Information to uses permitted by the CPRA.

CPRA defines Sensitive Personal Information to include, not by way of limitation: social security information, driver's license, state identification number, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; health information; sex life or sexual orientation, genetic information; or biometric information.

To whom may we disclose your personal data?

We only share your personal data when it is necessary and appropriate to the purposes for which it was collected. This may include sharing information with the entities within Embla Medical and with third parties such as service providers who support our operations, provide IT and system administration services, provide employee benefits, and professional advisers who provide consultancy, banking, legal, insurance and accounting services.

When we share your data with third parties, we ensure that they are contractually required to protect your information, use it only for agreed purposes and comply with data protection laws.

How do we protect your data?

We have a range of technical and organizational measures in place to protect your personal data from loss, misuse, or unauthorized access.

Access to our digital systems is carefully controlled. They are protected by role-based access controls, meaning employees can only access the information they need to carry out their work.

We also use secure networks, encryption, and regular data backups to protect your information during storage and transmission. Employees receive training on data protection and confidentiality, and we regularly review our security practices to ensure they remain effective.

How long do we keep your data?

We keep your personal data only for as long as necessary to fulfil the purposes for which it was collected, such as for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. In some cases, we may need to retain your data for longer, for example if there is an ongoing complaint, legal claim, or audit.

When deciding how long to keep your data, we consider factors such as the type and sensitivity of the data, the potential risks of keeping it too long or not long enough, and any legal and professional rules that apply.

What are your rights regarding processing of your personal data?

You may exercise any of the rights described in this section by contacting us at dpo@emblamedical.com. To make sure your information stays secure, we may ask you to prove your identity before we continue.

You have the right to:

- **Request access** to your personal data. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data in certain cases. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Please note that we may not always be able to comply with your request for erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data when we are relying on a legitimate interest and you want to object to the processing because you feel it impacts your fundamental rights and freedoms.
- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data if needed.
- **Request the transfer** of your personal data to you or to a third party. We will provide you, or a third party you have chosen, with your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to information kept in an electronic form which you initially provided with consent for us to use or where we used the information to fulfill a contract with you.

You can **withdraw your consent at any time** where we are relying on that consent to process your personal data.

Please note that this will not affect the lawfulness of any processing of personal data that was carried out before you withdrew your consent.

You have the right to **make a complaint** at any time to your country´s supervisory authority for data protection issues. We would, however, greatly appreciate the chance to deal with your concerns before you approach the supervisory authority, so please reach out to us in the first instance.

Being that Embla Medical's headquarters are in Iceland, the company's main supervisory authority for data protection issues is the Icelandic Data Protection Authority (Persónuvernd) - Data Protection Authority. The Icelandic Data Protection Authority with its seat at Laugavegur 166, 105 Reykjavík, Ísland, can be contacted by e-mail: postur@personuvernd.is. If you reside in the European Economic Area, you may also lodge a complaint directly with your local supervisory authority.

If you would like to get information about your local conditions, please contact your HR Business Partner or the Global Privacy & Compliance Team.

Where is your data kept, and is it ever transferred?

We generally store and process your data either in the country where you work, in the country where your HR information system is based, or - if you are located in the European Economic Area (EEA) - within the EEA. Together, these locations are referred to as your “Data Residence Area”.

In some cases, we may use service providers located outside the Data Residence Area, for example for secure cloud-based systems or technical support. When this happens, we ensure that appropriate safeguards are in place to protect your data, such as strict confidentiality obligations as well as approved data transfer agreements encompassing the Standard Contractual Clauses.

Information about the Standard Contractual Clauses can be obtained by visiting the website Standard Contractual Clauses (SCC) - European Commission.

Are there supplemental privacy notices that apply to my data?

Depending on where you live, different rules may apply regarding how we notify you and the rights you hold under privacy laws. If additional privacy notices relate to your region, those will take precedence in case of any discrepancies.

If you would like to get information about your local conditions, please contact your HR Business Partner or the Global Privacy & Compliance Team.