PRIVACY POLICY

Version 4 - 13 November 2025

1. About This Privacy Policy

- **Who we are**: ARTHRO ID (Borsbeeksebrug 34, Suite 520, 2600 Antwerpen, Belgium – Crossroad Bank number BE1011.212.429).

  ARTHRO ID is the "**Controller**" of your personal data (data) that determines the purpose and means of the processing of your personal data. ARTHRO ID, to ensure its functioning, collaborates with a "**Joint-Controller**" who is your treating doctor in control of your medical file. ARTHRO ID further collaborates with "**Processors**," like the treating hospital or online platforms (e.g., Google Platform) or consultants, who process data on behalf and per the instructions of the "**Controller**."

- **Our commitment**: Protecting your personal data is very important to us. This Privacy Policy (Policy) explains how we collect, use, and protect your information, and the choices you have.
- **Where to find it**: This Policy is always available on our website homepage (https://arthroid.ai/), and wherever we ask for personal data.
- **Definitions and abbreviation**: in section 13 of this Policy commonly used words and abbreviations are defined enduring your proper understanding of this Privacy Policy.
- **Children's data**:
  Our research and services are **not intended for anyone under the age of 18**.
  We do not knowingly collect children's personal data.
  If you are a parent/guardian and believe your child has shared data with us, please contact us.
  If we discover we have collected children's data without parental consent, we will delete it.

2. General terms

This Policy explains how ARTHRO ID collects and uses your personal data, and what rights you have.

- It does not replace any contract you have with us or your legal rights.
- Please read it carefully before joining our research or using our services.
- If you do not agree, stop using our website, app, services, or participation in our research right away.
- If you have questions, contact us at dataprivacy@arthroid.ai

3. What personal data do we collect and how do we process it?

Research

For research purposes related to the ARTHRO ID medical device called 'KNEE ID,' we use your personal data in a pseudonymized way (your first and last name is replaced with a code so you cannot be directly identified). The data may include (depending on the test plan/protocol):

- First and Last Name
- Gender
- Age
- Race
- Height

- Weight
- Medical history
- Diagnosis
- Medication list
- Surgery notes (e.g., implant type and size)
- Test results (e.g., pre-, and post- surgery scans like X-rays, CT scans, MRIs, blood tests results)
- Recovery outcomes

This information is collected and processed through your orthopaedic surgeon's hospital system and, when needed, further processed in ARTHRO ID's secure electronic system for the design and development of KNEE ID. We take strong measures to protect your data from breaches (see section 9 on data security).

Products & Services

To provide and improve our products and services, we may collect the following personal data either directly or through third parties:

- First and Last Name
- Address (full details)
- Email
- Phone and mobile numbers
- Fax number
- Account number

For business partners (customers, consultants, suppliers, or collaborator companies), we process the same contact details for professional purposes.

To find new business customers, we may use external sources (like address managers) and then contact potential customers. They can review, update, or remove their data at any time.

We also use your contact details for **marketing**, such as sending you updates or offers. This is **opt-in only**—you choose whether to receive these communications.

For **job applicants**, we collect the personal data you provide when applying for a role (see section 6 on job applicants in this Policy).

All personal data is processed in ARTHRO ID's secure electronic systems to reduce the risk of data breaches (see section 10).

Note: If you follow links to other websites, their privacy policies apply—we are not responsible for them.

4. Why do we collect such information and what is the legal basis?

Research

- We use anonymized or pseudonymized health data to test and develop our medical software '**KNEE ID**' for ultimate market access and for market maintenance until the end of the medical device lifecycle.
- This includes exploratory, verification, and validation tests and clinical evaluations needed for performance and safety checks per intended use, and regulatory approvals and maintenance (e.g., CE-mark, FDA).
- Test results will be used for regulatory, market access and maintenance purposes, for publishing peer reviewed scientific articles and for presenting at conferences.

- You will not be directly identifiable in any documentation nor in the scientific articles and conference presentations. The only person who can identify you is the doctor who keeps a research subject (meaning you) ID list at the hospital where the subject code is linked to your first and last name. This is called indirect identification. The subject code is used as a pseudonym for you. The subject ID list never leaves the hospital and is only visible to the doctor, his/her assigned team or any auditors or inspectors that are all bounded to confidentiality.
- We process, store, and reprocess your personal and sensitive personal data for research purposes as described in the informed consent, which you personally sign and date before any onset of research activities.
- **Legal basis:**
    - **Anonymized data** (cannot identify you): no legal basis needed. The GDPR does not apply.
    - **Pseudonymized data** (can still identify you indirectly) used for:
        - **Academic research:** only used when the scope of research is **public interest**.
        - **Usability testing and clinical investigations:** only used if you give your **consent**. Your doctor will explain how your personal data is processed and re-processed before you decide. You have the right to refuse and to withdraw your consent. This will not affect your doctor-patient relationship nor your treatment. (See also section 9 on your rights in this Policy).

Providing Our Services

- We need your personal details (e.g., name, contact info, payment details) to set up your account, process payments, provide services, and offer customer support.
- **Legal basis**: **Contract** (we need this data to deliver the services you signed up for).

Customer Management

- We use your contact details to maintain our relationship with you and provide a better customer experience.
- This may include sending you newsletters or service updates.
- **Legal basis**: **Legitimate interest** (balanced with your rights). You can unsubscribe anytime by emailing dataprivacy@arthroid.ai or clicking the unsubscribe link in our emails.

Compliance

- We keep certain personal data to meet legal requirements, respond to authorities, and maintain business records.
- **Legal basis**: **Legal obligation**. Example: keeping records after a contract ends or when you close your account.

Service Development & Improvement

- We may use your contact details to analyse and improve our services, or for statistical purposes.
- We use functional cookies on our website (required for basic site features)
- **Legal basis**: **Legitimate interest** (balanced with your rights).You can opt out anytime by emailing dataprivacy@arthroid.ai
- We may use analytical (–measure performance and usage or other cookies e.g., advertising, or cross-site tracking. (See section 10 covering cookies in detail)
- **Legal Basis: Consent.**

Job Applicants

- If you apply for a job with us, we use the personal data you provide to evaluate your application. See Section 6 in this Policy for details.
- **Legal basis: Legitimate interest** (balanced with your rights).You can opt out anytime by emailing dataprivacy@arthroid.ai

5. Protecting your privacy

How we use your data

We will only use your personal data when one or more of the following legal bases apply:
- **Consent**: You have given us permission (e.g., for prospective research using personal and sensitive data, or for using analytical cookies).
- **Public interest**: for the conduct of academic research.
- **Contract**: To provide services, support, or to set up an account with you.
- **Legal obligation**: Required to follow laws or regulations.
- **Legitimate interest**: To improve our services, fix technical issues, or understand current and future customer needs—always in a way that is proportionate and respects your rights.

Your data is processed in a secure electronic system designed to protect against hacking, viruses, and other risks (see Section 9 on data security).

How Long We Keep Your Data

- We keep your data only as long as needed to conduct research; to provide services; to publish and present at conferences or to ensure compliance with applicable regulations.
- Sometimes we keep it longer if required by law (e.g., invoices) or for legitimate reasons (e.g., handling disputes or reactivating subscriptions).
- When data is no longer needed, we either anonymize it or delete it securely.
- A retention Policy is maintained to personal data in our care. You can request information on specific retention for your personal data by emailing dataprivacy@arthroid.ai

Where Your Data Is Stored and Shared

- Your personal data is stored in a validated electronic environment within the ARTHRO ID organization.
- We may share your data with trusted third parties (e.g., hosting providers, e-marketing services) to help us deliver our services. Google platform is a hosting provider used by ARTHRO ID upon electronic system validation.
- **We never sell your personal data**.
- If data is transferred outside the European Economic Area (EEA), we ensure it is protected according to approved legal safeguards. For instance, no transfer of personal date will occur with an organization of another country unless we are ensured through adequate controls of the security of your personal date. When ARTHRO ID shares your personal information with its colleagues or partners in the United States, your data is protected under the EU-US **Data Privacy Framework (DPF)**. This means it is only shared with US companies that are officially **certified** to handle your data safely. In addition, ARTHRO ID uses **legal agreements** (called *Standard Contractual Clauses*) and regularly updates **risk checks**

(called *Transfer Impact Assessments*) to make sure your information stays secure. You can request a copy of these safeguards by emailing dataprivacy@arthroid.ai

6. ARTHRO ID job applications

Job Applicants – How We Handle Your Information

- **Applying**: If you are interested in a job at ARTHRO ID, you can send us your contact details and CV through our website and/or by email.
- **Use of your data**: We only use your information for recruitment purposes, such as:
  - Identifying and evaluating applicants
  - Making hiring decisions
  - Contacting you by phone or in writing
- **How long we keep it:**
  - We keep applicant information for up to one year after a position is filled or closed.
  - This allows us to:
    - Reconsider you for other roles
    - Refer back to your application if you apply again
    - Use it for employment purposes if you are hired

Your rights:

- You can ask us to access, update, or delete your information at any time. To do so, please contact us at dataprivacy@arthroid.ai

7. Share personal data with third parties

How We Share and Protect Your Personal Data

Internal use only

- Your personal data is mainly used inside ARTHRO ID.
- Employees, consultants, and suppliers only see the data they need to do their job.
- All stakeholders are trained on the limits of handling personal data.

Exceptions

We may share your data outside ARTHRO ID only when:

- Required by law, court order, or a supervisory authority.
- Needed to prevent or investigate crimes such as fraud.
- Necessary in emergencies where safety is at risk.
- Part of a business change (e.g., merger, acquisition, or sale of assets).

Third-party services

- We work with trusted service providers (e.g., hosting, payment processing, security, analytics, email, legal and financial advisors):
  - Google analytics

  - Google platform
- These providers may access your data only as needed to deliver their services per the contract we have with them and must use it only for that purpose.
- If you follow links to other websites, their privacy policies apply—we are not responsible for them.

Law enforcement and legal duties

- We may share your data if required by law or legal process (e.g., subpoena, court order).
- We may also share it if we believe it is necessary to safeguard your safety.

8. Your rights in relation to your Personal Data

If you live in the EU or your data is processed in the EU, you have the following rights regarding your personal data (with some exceptions depending on the situation):

- **Transparency and information**: You have the right to receive information about the purpose, recipients, identification of the controller and processors, legal basis, and retention period of your personal data.
- **Access and portability**: Ask for a copy of the personal data we hold about you, including where it came from, why we use it, who controls it, and who it may be shared with. You also have the right to transmit your personal data to another controller.
- **Stop processing**: Ask us to stop using your data, in whole or in part, unless we are legally required/allowed through a genuine legal basis to continue. For research purposes, even after you withdraw your consent, ARTHRO ID may retain and process your pseudonymized personal data collected before you withdrew your consent to ensure the validity of the results.
- **Restrict use**: Ask us to limit how we use your data if:
  - you dispute its accuracy,
  - the processing is unlawful, but you do not want it deleted, or
  - we no longer need it, but you require it for legal claims.
- **Erase**: Ask us to delete your data when it is no longer needed for the purpose it was collected, providing no legal objections.
- **Challenge**: Object if we use your data based on "legitimate interest."
- **Marketing**: Ask us not to share your data with third parties for marketing or change how we contact you.
- **Correct/Update**: Ask us to fix errors or update your data. You can also update or delete parts of your data yourself through your account settings.
- **Transfers outside the EU**: Request a copy of the safeguards we use when transferring your data outside the EU. Your personal data may be transferred to the US, where your personal data is equally well protected as in the EEA under the EU-US "Data Privacy Framework" (see section 6 in this Privacy Policy for details).
- **Complain:** File a complaint with your local data protection authority:

  Gegevensbeschermingsautoriteit
  Drukpersstraat 35, 1000 Brussel

  +32 (0)2 274 48 00
  +32 (0)2 274 48 35

  Link:
  https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen

Important to know:

- We may ask for proof of identity before fulfilling your request.
- In rare cases we may charge a fee if your request is clearly unfounded or excessive.

9. Commitment to data security

How We Keep Your Data Safe

We take strong steps to protect your personal data. This includes:

- **Physical safeguards** – secure facilities and controlled access.
- **Electronic safeguards** – protected systems to prevent hacking or unauthorized access.
- **Managerial safeguards** – clear rules and trained staff to handle data responsibly.

All information we collect online is stored in a **validated secure system** to reduce the risk of data breaches. Note no electronic processing of personal data is 100% secure. We however strive for ensuring protection per the current State of The Art (SoTA).

To increase your data security, you can set the preference in your setting or preference page of "Do Not Track" in your web browser to inform websites you prefer not to be tracked.

10. Use of Cookies or Other Tracking Technologies

Use of Cookies and Tracking Technologies

ARTHRO ID, together with trusted partners, uses cookies and similar technologies (such as pixels, tags, and scripts) to:

- Keep your session active and remember your preferences
- Improve security and fix technical issues
- Understand how our services are used (user trends, campaign effectiveness)
- Improve website performance and your overall experience

Third-party services (e.g., analytics or marketing providers) may also place cookies. Their practices are covered by their own privacy policies, not ours.

What Are Cookies?

Cookies and similar files help us distinguish you from other users and improve your browsing experience.

- Some are set by ARTHRO ID, others by third parties.
- Some last only while your browser is open, others stay longer.

Types of cookies we use:

- **Functional cookies** – required for basic site features and site security (do not need consent).
- **Analytics cookies** – measure performance and usage (need your consent).
- **Other cookies** – e.g., advertising, or cross-site tracking (need your consent).

Your Choices

- You can manage or block cookies in your browser settings.
- Blocking all cookies may limit access to parts of our website.

Cookies We Use

- **Google Analytics** – helps us understand how the site is used (kept 30 minutes to 2 years).
- **AddThis** – allows sharing content on social media (kept up to 2 years).

11. Changes

Updates to This Privacy Policy

- We may update this Privacy Policy as our services and website develop.
- We will let you know about changes by posting the update Privacy Policy on our website, and by frequent reminders via e-mail.
- With each change the effective date will be updated on the website. The updated Privacy Policy becomes effective once it is available on the Arthor ID website.
- You are advised to review this Privacy Policy periodically for any changes.
- By continuing to use our website or services after updates are made, you accept the revised Privacy Policy.

12. Contact information

Questions or Complaints

- If you have questions about this Privacy Policy or want to use any of your rights (see Section 8), please contact us at dataprivacy@arthroid.ai.
  This request is free of charge. A fee can be charged in case of unfounded or excessive requests (e.g., in case of unfounded repeated requests).
- We will verify your identity before responding to such requests.
- We will do our best to resolve any concerns about how we process your personal data.
- If you live in the EU, you also have the right to file a complaint with your national data protection authority at any time:
  - Gegevensbeschermingsautoriteit
    Drukpersstraat 35, 1000 Brussel

    +32 (0)2 274 48 00
    +32 (0)2 274 48 35

  - Link:
    https://www.gegevensbeschermingsautoriteit.be/burger/acties/klacht-indienen

  However, we encourage you to contact us first at dataprivacy@arthroid.ai so we can try to resolve the issue directly.

13. Definitions

- **Anonymous data**: personal data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.
- **Clinical Investigation**: systematic investigation in one or more human subjects, undertaken to assess the clinical performance, effectiveness, or safety of a medical device. Synonymous with "clinical trial" or "clinical study."
- **Controller / Joint-Controller**: means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Cookies**: are small text files that websites store on your device (like your computer or phone) when you visit them. They help websites remember who you are and what you have done—like keeping you logged in, saving your preferences, or tracking your activity for analytics or ads.
- **Data Privacy Framework (DPF)**: the current agreement that allows personal data to be transferred from the European Union to certified companies in the United States.
- **Data Subject**: an identified or identifiable natural person.
- **EEA**: European Economic Area. EU countries + Iceland, Liechtenstein, and Norway (Switzerland is not part of the EEA but has bilateral agreements with the EU instead).
- **EU**: European Union
- **Consent**: of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Exploratory testing**: refers to early-stage evaluations that aim to gather initial insights about a device's safety, performance, and usability—and this (most often) before formal clinical trials or full verification testing begin.
- **GDPR**: stands for **General Data Protection Regulation**. It is a **European Union (EU) law** that came into effect on **May 25, 2018**, designed to **protect the privacy and personal data** of individuals within the EU and the European Economic Area (EEA).
- **Legal basis**: the lawful reason that allows an organization to process personal data. You must identify and document this basis before you begin processing.
- **Legitimate interest**: allows organizations to process data when it is necessary for their own or a third party's legitimate interests—unless those interests are overridden by the rights and freedoms of the individual.
- **Market access**: the entire process of making a medical device available for use in a specific country or region—legally, safely, and economically. It is about regulatory approval and about ensuring the device can actually reach patients and be reimbursed or funded.
- **Market maintenance**: the entire process of keeping a medical device available for use in a specific country or region—legally, safely, and economically. It is about regulatory approval and about ensuring the device can actually reach patients and be reimbursed or funded.
- **Personal data:** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

- **Processing**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Processor:** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
- **Public interest:** a principle in law that allows governments, public bodies, or certain private entities to take actions or make decisions that are justified by the **need to protect or promote the general welfare of the public**, even if such actions may limit individual rights or private interests.
- **Pseudonymization:** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
- **Regulatory**: refers to the rules, processes, and authorities that ensure devices are safe, effective, and legally allowed to be sold and used.
- **Research**: the systematic investigation and development process aimed at creating, improving, and validating medical technologies that diagnose, treat, or monitor health conditions.
- **Sensitive personal data** are data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Examples are medical data, race, gender.
- **SoTA:** State of the Art. It refers to the current and generally accepted level of development, safety, and performance based on consolidated scientific, technical, and/or clinical knowledge—not necessarily the most advanced or newest technology.
- **Standard contract clauses (SCCs):** pre-approved legal agreements issued by the European Commission that allow organizations to transfer personal data from the EU/EEA to countries outside the EU/EEA that do **not** have an adequacy decision under the GDPR.
- **Subject code**: the code provided to you as a data subject to pseudonymise your personal data and held by the doctor to identify you indirectly.
- **Third party**: means a natural or legal person, public authority, agency or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- **Transfer Impact Assessment (TIA):** a required evaluation under the GDPR when personal data is transferred from the EU/EEA to a country that does not have an adequacy decision. It helps ensure that the data will be protected to a level essentially equivalent to EU standards—even outside the EU.
- **Validation**: proving that the device actually works for its intended purpose and meets the needs of users in real-world conditions.
- **Validated electronic environment**: in the context of medical devices refers to a digital system (software, hardware, or cloud-based platform) that has been formally tested and documented to ensure it consistently performs as intended—especially when used for regulated activities like design control, document management, or clinical and other personal data handling.
- **Verification**: checking whether the device has been built correctly according to its design specifications. It is about confirming that the technical requirements have been met—before the device is used by real patients