

ArianeTM

MEDICAL SYSTEMS

Data Privacy Notice

This privacy notice tells you what to expect us to do with your personal information.

Document Owner	Senior Management
Version	1.0
Date issued	19 th March 2026
Review frequency	Annually, or following any substantial change to our data processing activities
Related documents	1039040 – Photo and Video Consent Form 1039041 – Data Protection: Record of Data Processing Activities 1039042 - Data Protection - Personal Data Protection Policy 1039043 - Data Protection - Data Retention Policy 1039044 – Patient Data Access Policy Statement

Table of Contents

2. What Information We Collect, Use, and Why	2
2a. Staff Administration	2
2b. Customer Orders	2
2c. Marketing	3
2d. Finance	3
2e. Compliance with legal requirements	3
2f. Installation, Service & Maintenance Activities	3
2f. Training	4
3. Lawful Basis and Data Protection Rights	4
3a. Your data protection rights	4
3b. Our lawful basis for each processing activity	4
4. Where We Get Personal Information From	5
5. How Long We Keep Information	5
6. Who We Share Information With	6
6a. General third parties	6
6b. Clermont Rayonnement Detection (CLERAD)	6
7. Our Relationship with Clermont Rayonnement Detection (CLERAD)	6
7a. Customers — Sales, Marketing and Commercial Activities	6
7b. Medical Device Traceability	7
7c. Complaints and Customer Feedback	7
7d. Medical Device Vigilance, Field Safety Corrective Actions (FSCAs), and Safety Alerts	7
7e. Service, Maintenance, and Technical Support Activities	7
7f. Joint Marketing and Sales Ventures	7

8. Sharing Information Outside the UK	8
9. How to Complain	8

1. Company Details

Name	Ariane Medical Systems Ltd
Role	Data Controller
Address	151 Mansfield Road, Alfreton, Derbyshire, DE55 7JQ, United Kingdom
Telephone	01332 242258
Email	contact@arianemedicalsystems.com

2. What Information We Collect, Use, and Why

2a. Staff Administration

- Name, address, contact details
- Date of birth, NI number
- Passport / photo ID copies
- Employment & education history
- Right-to-work documentation (e.g. VISAs where applicable)
- Employment references
- Bank Details
- Emergency contact name & phone number
- Health / medical disclosures (special category - allergies, disabilities, conditions relevant to H&S or reasonable adjustments)
- Disciplinary & grievance records
- Sickness, Absence & holiday records
- Training Records

Why we collect emergency contact and health information

Emergency contact details are collected so that we can reach a nominated individual in the event of a workplace emergency, accident, or sudden illness involving an employee. This is a standard and expected part of responsible employment practice.

Medical or health disclosures are collected solely where relevant to health and safety obligations — for example, to ensure we are aware of any allergies, disabilities, or conditions that may require us to take precautionary measures, make reasonable workplace adjustments, or respond appropriately in an emergency.

This information is treated as sensitive personal data (special category data) and is held securely, accessible only to authorised personnel, and used exclusively for the purposes described above.

2b. Customer Orders

- Name, job title, contact details (e-mail, phone)
- Affiliated organisation name & address
- Purchase / order history
- Account information
- Payment / invoicing details
- Device installation site details

- Medical device traceability data (serial numbers, UDI, lot numbers) associated with specific customer/site.
- Delivery and logistics records
- Records of meetings and decisions
- Call recordings

2c. Marketing

- Name, job title, affiliated organisation, contact details (e-mail and phone)
- Marketing preferences and consent records
- Event attendance records
- Photographs and video recordings
- Video interview recordings (KOLs)
- IP addresses, cookie and website analytics data
- Social media profile information (where publicly available)
- Previous orders and purchasing history

2d. Finance

- Name, job title and contact details (e-mail and phone)
- Affiliated Organisation name and address
- Bank and payment details
- Invoice and purchase order records
- Credit reference information
- Financial transaction history
- Signed contracts and purchase agreements

2e. Compliance with legal requirements

- Name and contact details of complainant or reporter
- Affiliated organisation and site address
- Device identification data (serial number, UDI, lot number, installation date) attributed to customer/site
- Description of complaint, adverse event, or near-miss
- Clinical or patient context (where relevant to a complaint or vigilance report - may include special category data)
- Correspondence and investigation records
- Corrective and Preventive Action (CAPA) records
- FSMA / Field Safety Notice distribution records
- Training and competency records (employees)
- Audit records (internal and external)

2f. Installation, Service & Maintenance Activities

We collect the following information for recruitment, employment administration, and to fulfil our legal obligations as an employer:

- Contact details (e.g. name, address, telephone number or personal email address)
- Date of birth
- National Insurance number
- Copies of passports or other photographic identity documents
- Employment history (e.g. job application, employment references, or details of secondary employment)
- Education history (e.g. qualifications and professional registrations)
- Right to work information

- Emergency contact details (name, relationship, and contact number of a nominated next of kin or emergency contact)
- Medical and health information disclosed for health and safety purposes (e.g. known allergies, disabilities, or conditions relevant to workplace safety or reasonable adjustments)

2f. Training

- Name, job title, and contact details of site contact(s)
- Date of training and date of certificate issue
- Training assessment outcomes / competency sign-off records
- Certificate expiry date and renewal records (where applicable)
- Trainer name and credentials

3. Lawful Basis and Data Protection Rights

Under UK data protection law, we must have a 'Lawful Basis' for collecting and using your personal information. The lawful bases available under UK GDPR are published on the ICO's website. Which lawful basis we rely on may affect your data protection rights, which are summarised below.

3a. Your data protection rights

We respect that individuals whose personal data we hold have rights under UK GDPR. We are committed to honouring these rights as promptly as possible – your rights include:

- Right of access – you have the right to ask us for copies of your personal information, including details about where we get it from and who we share it with.
- Right to rectification – you have the right to ask us to correct or delete personal information you think is inaccurate or incomplete.
- Right to erasure – you have the right to ask us to delete your personal information in certain circumstances.
- Right to restriction of processing – you have the right to ask us to limit how we use your personal information.
- Right to object to processing – you have the right to object to our processing of your personal data, including where we rely on legitimate interests.
- Right to data portability – you have the right to ask us to transfer personal information you provided to us, to you or another organisation.
- Right to withdraw consent – where we rely on consent as our lawful basis, you may withdraw that consent at any time.

We must respond to any data rights request within one month. To make a request, please contact us using the details in Section 1.

3b. Our lawful basis for each processing activity

Staff Administration

- Contract
- Legal obligation
- Legitimate interests (emergency contacts & health disclosures for H&S duty of care)

Emergency contact details: it is in the legitimate interests of both the employee and the Company to hold next-of-kin contact information to enable a prompt and appropriate response in a workplace emergency or medical incident. Employees are made aware of this at the point of collection, and the information is not used for any other purpose.

Employee health and medical disclosures for health and safety: it is in the legitimate interests of the Company and the employee to hold relevant medical information (such as allergies, disabilities, or health conditions) where this is necessary to fulfil our statutory duty of care under the Health and Safety at Work Act 1974, to enable appropriate risk assessments, and to make reasonable adjustments under the Equality Act 2010. This information is treated as special category data, held securely, and access is restricted to those with a genuine need to know.

- Consent (voluntary disclosures e.g. health/medical information)

Customer Orders

- Contract
- Legal obligation
- (UK MDR 2002 / EU MDR 2017/745 traceability / 21 CFR Part 820 traceability requirements)

Service updates or marketing purposes

- Consent (marketing communications, photographs, video recordings, web tracking and cookies)
- Legitimate interests (prospecting, event follow-up, analytics)

Finance

- Contract
- Legal obligation (HMRC, Companies House, financial regulations)

Dealing with queries, complaints, or claims

- Legal obligation (UK MDR 2002 / EU MDR 2017/745 / 21 CFR Part 820 / ISO 13485)
- Legitimate interests (patient safety, product quality)
- Vital interests (where patient safety is at immediate risk – vigilance and adverse event reporting)

Installation, Service & Maintenance

- Contract (Service contract)
- Legitimate interests (maintaining safety and performance of medical devices in clinical use)
- Legal obligation (FSCA records)

Product Training

- Contract (Service contract, commercial/distributor agreements)
- Legitimate interests
- (ensuring patient safety and device performance through documented competency)

4. Where We Get Personal Information From

- Publicly available sources
- Directly from you
- Previous employers (employment references)
- Suppliers and service providers
- Clermont Rayonnement Detection (CLERAD) — our associated company, Legal Manufacturer, and product development partner (see Section 6)

5. How Long We Keep Information

Medical device records (including traceability, installation, service, maintenance, complaint, and vigilance records relating to a specific device) are retained in active files for the full-service lifetime of the product, with a minimum retention period of ten years from the date of supply. When an individual product is removed from service, the associated records are transferred to archive and retained for a further minimum of ten years starting from the date of decommissioning.

Employee records (including recruitment, employment, and payroll records) are retained for up to five years following the end of employment (or in the case of contractors end of contractual engagement).

All other categories of personal data held by Ariane Medical Systems — including customer account records, marketing records, correspondence, and general business records — shall be retained for up to ten years, after which it is securely deleted or anonymised unless a specific legal or regulatory obligation requires otherwise.

When data reaches the end of its retention period, it is securely deleted or anonymised. Paper records containing personal data are disposed of by secure shredding.

If you have any questions about how long we retain your specific information, please contact us using the details in Section 1.

6. Who We Share Information With

We share personal data with third parties only where necessary and to the extent required.

6a. General third parties

- Professional or legal advisors
- Relevant regulatory authorities (e.g. MHRA, HSE)
- External auditors or inspectors
- Professional consultants
- Organisations we are legally obliged to share personal information with (HMRC, MHRA, HSE)
- Suppliers and service providers
- Publicly, via our website, social media, or other marketing and communications channels (where prior consent has been obtained)

6b. Clermont Rayonnement Detection (CLERAD)

Our primary third-party data sharing relationship is with the French (EU) company Clermont Rayonnement Detection (CLERAD), our associated company based in France. Sharing of personal information is performed in connection with our role as subcontract manufacturer, UK Responsible Person, UK importer, and international sales/marketing partner and distributor of CLERAD products. Full details of this relationship and data sharing arrangements are covered in section 7.

7. Our Relationship with Clermont Rayonnement Detection (CLERAD)

About our relationship with Clermont Rayonnement Detection ('CLERAD')

Clermont Rayonnement Detection ('CLERAD') is a company based in France. CLERAD and Ariane Medical Systems Ltd are part of the same group of companies under common ownership.

The nature of our commercial and regulatory relationship with CLERAD is multi-faceted:

- Ariane Medical Systems and CLERAD are engaged in joint business operations
- CLERAD is the Legal Manufacturer of the medical devices we represent, sell, and distribute.
- Ariane Medical Systems is designated as the UK Responsible Person (UK RP) for CLERAD devices placed on the UK market
- Ariane Medical Systems is the subcontract manufacturer of certain CLERAD products
- Ariane Medical Systems distributes CLERAD products in agreed territories including the United Kingdom

As a result of these roles, significant data sharing between our companies is necessary and legally required in certain circumstances, as described below.

7a. Customers — Sales, Marketing and Commercial Activities

We share customer contact details and account information with CLERAD for the following purposes:

- Processing and fulfilling product orders and managing customer accounts
- Coordinating joint sales and marketing campaigns, product launches, and promotional activities
- Managing customer relationships where both companies have a commercial interest (e.g. customers purchasing products from the wider group)
- Sharing marketing preferences and customer records to ensure consistent and appropriate communications

The lawful basis for this sharing is contract (where necessary to fulfil our obligations to you) and, where applicable, consent (for marketing communications).

7b. Medical Device Traceability

As the UK Responsible Person, Importer and Distributor of CLERAD products, we are required under the UK Medical Devices Regulations 2002 and associated MHRA guidance to maintain and share records that enable full traceability of medical devices throughout their lifecycle. This includes:

- Customer and end-user details (name, organisation, address, installation site)
- Device identification information (serial numbers, lot numbers, Unique Device Identifiers / UDI)
- Purchase, supply, and delivery records
- Installation and commissioning records

This information may be shared with CLERAD as Legal Manufacturer to maintain the device traceability records they are required to hold under EU MDR 2017/745 and applicable French national regulations. The lawful basis for this sharing is legal obligation.

7c. Complaints and Customer Feedback

Where a complaint relates to a medical device for which CLERAD is the Legal Manufacturer, we are required to forward that complaint — including all relevant personal data — to CLERAD for investigation and response. This is because, under applicable medical device regulations, the Legal Manufacturer holds ultimate responsibility for product complaints, corrective actions, and post-market surveillance.

Information shared with CLERAD in this context may include:

- Complainant name and contact details
- Details of the affected device (serial number, UDI, installation location)
- A description of the complaint or adverse event
- Any supporting correspondence, photographs, or records

The lawful basis for this sharing is legal obligation and, where applicable, legitimate interests (ensuring patient safety and regulatory compliance).

7d. Medical Device Vigilance, Field Safety Corrective Actions (FSCAs), and Safety Alerts

We may be required to share personal data with CLERAD in connection with:

- Medical Device Vigilance (MDV) reporting — where a serious incident or adverse event involving a device requires reporting to the MHRA and/or other competent authorities, and CLERAD as Legal Manufacturer must be notified and involved in the investigation
- Field Safety Corrective Actions (FSCAs) — where CLERAD initiates or we identify a need for a recall, safety notice, or field correction, and we must communicate with affected customers and share their details with CLERAD to coordinate corrective action
- Safety alerts and hazard notices — where CLERAD issues Field Safety Notices (FSNs) and we must identify and contact affected customers on their behalf

The lawful basis for this sharing is legal obligation. In some circumstances, vital interests may also apply where patient safety is at risk.

7e. Service, Maintenance, and Technical Support Activities

Where devices require planned or reactive maintenance, calibration, or technical support, we may share customer details with CLERAD to coordinate service visits, remote support, or device updates. Information shared may include:

- Customer name and contact details
- Site address and access arrangements
- Device identification and service history
- Records of maintenance or repair activities

The lawful basis for this sharing is contract (where service obligations exist under a contract with the customer) and legitimate interests (maintaining the safety and performance of medical devices in clinical use).

7f. Joint Marketing and Sales Ventures

From time to time, we may undertake joint marketing campaigns, attend trade events, or pursue sales opportunities collaboratively with CLERAD. In those contexts, contact details and marketing preferences for

prospects and customers may be shared between us in accordance with applicable consent. We will always ensure that any joint marketing use of personal data is consistent with the preferences and consent you have provided.

8. Sharing Information Outside the UK

Where necessary, we transfer personal information outside the UK to CLERAD in France. When doing so, we comply with the UK GDPR, ensuring that appropriate safeguards are in place. France, as a member of the European Economic Area (EEA), benefits from UK adequacy regulations, meaning that the level of data protection is recognised as equivalent to that provided under UK law.

For further information or to request a copy of the appropriate safeguards for any transfer, please contact us using the details in Section 1.

Organisation name	Clermont Rayonnement Detection (CLERAD)
Category of recipient	Associated company — Legal Manufacturer, joint commercial partner
Country of transfer	France (European Union, European Economic Area)
Legal mechanism for transfer	UK Adequacy Regulations — France/EEA is recognised as providing an adequate level of protection under UK data bridge arrangements

9. How to Complain

If you have any concerns about how we use your personal data, please contact us in the first instance using the details in Section 1. We will aim to resolve your concern promptly.

If you remain unhappy after raising a concern with us, you have the right to complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office (ICO)

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113

Website: ico.org.uk/make-a-complaint

Data Controller: Ariane Medical Systems Ltd | 151 Mansfield Road, Alfreton, Derbyshire, DE55 7JQ, United Kingdom | contact@arianemedicalsystems.com | 01332 242258

This document is prepared in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This document is confidential and intended for internal use. It should be made available to the Information Commissioners Office upon request.

Last updated: 19th March 2026