Privacy Policy

Table of Contents

1. *Introduction*

Here at IEL we are serious about protecting and safeguarding your privacy rights and ensuring that we work in accordance with data protection legislation (General Data Protection Regulation - GDPR). We are committed, in line with our company values, to being open and honest about how we collect and use your personal data.

This policy explains what we do with your personal data, whether you are our customer, supplier or you work or have worked with us.

It describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal responsibilities.

This policy outlines what processes we have in place for collecting, storing and processing personal data. It tells you how long we will store it for, how we keep it safe, how you can let us know if you want to change or have your personal data deleted.

We have also appointed a Data Protection Officer, who helps us ensure that we meet our data protection obligations.

It's likely that we'll need to update this policy from time to time. We'll notify you of any significant changes. We will do this via email if you are an employee or by publishing an updated version of the policy on our website for you to have a look at.

In this policy, whenever you see the words 'we', 'us', 'our', 'IEL' it refers to Imaging Equipment Limited (registered in the UK number 4189193) a wholly owned subsidiary of Advanced Accelerator Applications, a Novartis company.

2. *Key Definitions*

In this policy we will use and refer to some definitions that you may want to know a bit more about.

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Data subject" means a living individual to whom personal data relates.

"Controller" means the natural or legal person, public authority agency or any other body which alone or jointly with others determines the purpose and means of the processing of personal data.

"Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller, e.g. company providing customer relationship management (CRM) solution or a pension company.

"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.

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she, by a statement or by a clear affirmative action, signifies processing of personal data related to him or her.

3. *What are our responsibilities?*

We are committed to process your personal data in accordance with the following principles:

"Principles relating to processing of personal data"

- IEL processes personal data lawfully, fairly and in a transparent manner.
- IEL collects personal data only for specified, explicit and legitimate purposes and will not further process this personal data in a manner than is incompatible with those purposes.
- IEL processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- IEL keeps accurate, and where necessary, keeps personal data up to date and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- IEL keeps personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- IEL adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

We are also required to implement appropriate technical and organisational measures to comply with the GDPR and be able to demonstrate that we process your data in line with the legislation. We are reviewing and updating these processes regularly.

We will ensure that we only use processors who provide sufficient guarantees that they will comply with GDPR and we set out contracts with those processors.

We also keep up to date records of our processing activities and record the following:

- Name & contact details of the controller (IEL), joint controllers, representative & DPO
- The purpose of collecting
- A description of the categories of data and categories of personal data
- The categories of recipients to whom the personal data will be disclosed to
- Recipients of personal data in third countries or international organisations including identification of the third country or organisation
- The safeguards in place for such transfers
- Retention period and time limits for categories of personal data
- A general description of the technical & organisational security measures in place

In some cases, we will act as a Processor and because of this we keep a record of:

- Name & contact details of the processor (IEL), and the controller that the processor is acting on behalf of
- The categories of processing carried out on behalf of the controllers

"Individual responsibilities"
Our employees are trained to ensure that they know how to handle personal data appropriately and safely. Our employees are aware of their individual responsibilities and they are required to:

- access only data that they have authority to access and only for authorised purposes;
- not disclose data except to individuals (whether inside or outside IEL) who have appropriate authorisation;
- keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not store personal data on local drives or on personal devices that are used for work purposes; and
- report data breaches of which they become aware to Data Protection Officer immediately.

4. What kind of personal data do we collect?

Employees/candidates - depending on whether you are applying to work with us or you are already employed by us, we may collect some or all of the information listed below. The reason for gathering this data is to enable us to make a decision about your application or to comply with laws, regulations and other obligations, e.g. fulfilment of your contract of employment. The personal data that we may gather is:

- Name
- Date of birth
- Sex/gender
- Photograph
- Marital status
- Contact details
- Education details
- Employment history
- Emergency contact details and details of any dependants
- Referee details
- Immigration status
- Nationality/place of birth
- A copy of your passport or Identity Card – to check if you have right to work in UK
- A copy of your driving licence
- National Insurance Number
- Bank details
- Salary, tax, pension and benefits information
- Diversity information including racial or ethnic origin, religious or other similar beliefs, and physical or mental health, including disability-related information

Customers – if you are our customer we need to collect and use information about you, or individuals in your organisation to fulfil our contractual obligations, or to comply with government agencies regulations, e.g. HMRC. We would need to have your contact details or the details of individual

contacts at your organisation (such as their names, job titles, telephone numbers and email addresses) to enable us to ensure that our relationship runs smoothly.

Suppliers – if you are one of our suppliers we need to collect some personal data to ensure a smooth working relationship. We will have details of our contacts within your organisation, such as names, telephone numbers and email addresses. We also collect your bank details, so that we can pay you.

5. *How do we collect your personal data?*

We collect personal data about you from the following sources:

Employees/candidates – the majority of personal data we will have will have been received from yourself. We may ask others about you if you nominate them as your employment referees.

Clients – we would mainly receive personal data about you from yourself, either through:

- ✓ you contacting us proactively, usually by phone or email; and/or
- ✓ us contacting you, either by phone or email, or through meetings with our Account Managers

Where appropriate, and in accordance with government regulations, we may seek more information about you or your colleagues from other sources, e.g. market intelligence including:

- ✓ From third party market research and by analysing online and offline media (which we may do ourselves, or employ other organisations to do for us);
- ✓ From delegate lists at relevant events

Suppliers – we would mainly receive personal data about you from yourself during the course of working with you.

6. *Why we collect your personal data and how we use it?*

Whether you work with us or you are our client or supplier, personal data that we collect about you will always be processed in line with GDPR Data Protection Principles (Paragraph 3). There are many reasons why we hold data about you and we are transparent about it.

Employees/Candidates – we collect personal data about you in order to comply with legal obligations (e.g. we are required to let HMRC know your NI number), to enter or fulfil a contract between you and us (e.g. we need your bank details to pay you), because of our legitimate interests (e.g. to prove that we have been fulfilling your contract if there are any disputes or, in rare circumstances, defend against legal claims) and in some cases, it will be necessary to carry out obligations or exercise rights under employment law (e.g. to prove that we work in line with equality and diversity principles).

Sensitive Personal Data **–** in line with GDPR, information about racial or ethnic origin, political opinions, religious beliefs or other similar beliefs, trade union membership, physical or mental health, sexual life, and criminal allegations, proceedings or convictions are classed as sensitive personal data.

In certain limited circumstances we may legally collect and process sensitive personal data without requiring the explicit consent of an employee.

- we will process data about an employee's health where it is necessary, for example, to record absence from work due to sickness, to pay statutory sick pay, to make appropriate referrals

to the Occupational Health Service, and to make any necessary arrangements or adjustments to the workplace in the case of disability. This processing will not normally happen without the employee's knowledge and, where necessary, consent.

- we will process data about, but not limited to, an employee's racial and ethnic origin, their sexual orientation or their religious beliefs only where they have volunteered such data and only for the purpose of monitoring and upholding our equal opportunities policies and related provisions.

Customers – we collect personal data about you or others in your organisation to enter or fulfil contracts with you, due to legal obligations (e.g. to comply with regulations from Medicines and Healthcare products Regulatory Agency - MHRA), to tell you about our products, marketing activities or educational events, or because we have some legitimate reasons.

If you are our customer, we will store information about you in our CRM system.

CRM - Customer relationship management is an approach to manage a company's interaction with current and potential customers; it uses data analysis about customers' history with a company to improve business relationships with customers, specifically focusing on customer retention and ultimately driving sales growth.

The CRM is a set of software applications that help our organisation determine the needs and preferences of our customers by managing, organising, tracking and storing customer details and interactions.

Our CRM support provider is Wattle (https://www.wearewattle.com) and all information is stored on the Cloud. The Could is protected from any breach by our IT security company Westgate (https://westgateit.co.uk).

Our CRM is provided by Microsoft and is called 'Dynamics 365'. Dynamics 365 is a product line of enterprise resource planning and customer relationship management applications announced by Microsoft in July 2016 and on general release November 1, 2016, as a part of the Microsoft Dynamics product line. Microsoft confirms they have mandatory processes and encryption restrictions within Dynamics 365 both Online / Cloud and on-premise to comply with GDPR. Some of these include:

Security Development Lifecycle: a mandatory Microsoft process that embeds security requirements into every phase of the development process. Dynamics 365 is built using the Security Development Lifecycle.
Encryption: in transit between your users' devices and Microsoft data centers, as well as while at rest in a Microsoft database. This helps protect your Dynamics 365 data at all times according to Microsoft. This restriction particularly applies to Dynamics CRM Online / Azure Cloud.

In some circumstances we are only be able to contact you if you give us permission to do so. This is when consent is our basis for processing and concerns mainly marketing activities. When this applies, IEL will process your personal data in line with GDPR regulations:

- Where processing is based on consent, IEL will be able to demonstrate that the data subject has consented to the processing of his or her data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, IEL will present the request for consent in a manner clearly distinguishable from other matters.

- IEL will ensure the data subject has a right to withdraw his or her consent at any time.

The ICO suggest a double opt in as best practice for gaining consent. We will use the *double opt in* process if we are required to obtain your consent. Double opt in is a two-stage process:

- Stage 1 – we send you an email, either because you have contacted us and you would like some information about our products and services, or because we already have your contact details and would like to check that you are still happy for us to keep in touch with you. This email will have the option to either Opt in or Opt out to receiving marketing communications from IEL. Clicking on Opt in in will open IEL's preference centre in your browser.
- Stage 2 – Is to go through the marketing communication options of what you want to hear from us about and enter any personal information you want to give. There is also the option to opt out on this form. The details will then be updated in our CRM.

Suppliers – we collect personal data about you or others in your organisation to enter or fulfil contracts with you, due to legal obligations, various UK regulations or because we have some legitimate reasons.

7. Who do we share your personal data with?

The personal data that we collect about you is mainly processed by us. There are some situations when we may have to share it with other organisations or individuals. We would only share it with trusted third parties and we would ensure that:

- We provide only the information they need to perform their specific services.
- They may only use your data for the exact purposes we specify in our contract with them.
- We work closely with them to ensure that your privacy is respected and protected at all times.
- If we stop using their services, any of your data held by them will either be deleted or anonymised.

Employees/Candidates - where appropriate and in accordance with legal requirements, we may share your personal data with the following:

- Our parent companies – Advanced Accelerator Applications and Novartis.
- Individuals and organisations who hold information related to your employment references and/or recruitment agencies.
- Tax, audit, or other authorities, when we believe in good faith that the law or other regulation requires us to share this data (for example, because of a request by a tax authority or in connection with any anticipated litigation).
- Third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems);
- Third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place;

Customers – where appropriate and in line with legal requirements and other obligations, e.g. our contract with you, we may share your personal data with:

- Courier companies
- Suppliers
- Government organisations, e.g. Medicines & Healthcare products Regulatory Agency (MHRA)
- Third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems).
- Third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place.

Suppliers - where appropriate and in line with legal requirements and other obligations, e.g. our contract with you, we may share your personal data with:

- Our customers
- Government organisations
- Third party service providers who perform functions on our behalf (including external consultants, business associates and professional advisers such as lawyers, auditors and accountants, technical support functions and IT consultants carrying out testing and development work on our business technology systems).
- Third party outsourced IT and document storage providers where we have an appropriate processing agreement (or similar protections) in place.

8. How do we safeguard your personal data?

We know how much data security matters to everyone. With this in mind we treat your data with the utmost care and take all appropriate steps to protect it. We are committed to taking all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures. These include measures to deal with any suspected data breach.

Access to your personal data is password-protected, encrypted where necessary and access limited to only appropriate and trained personnel.

If you suspect any misuse or loss of or unauthorised access to your personal information, please let us know immediately by emailing: data@imagingequipment.co.uk

9. How long do we keep your personal data for?

Whenever we collect or process your personal data, we'll only keep it for as long as it is necessary and for the purpose for which it was collected.

At the end of that retention period, your data will either be deleted completely or anonymised, for example by aggregation with other data so that it can be used in a non-identifiable way for statistical analysis and business planning.

Unsuccessful Candidates – we keep your personal date for 6 months after the rejection date.

Employees – the retention period will depend on the category of your personal data. Majority information about you we will keep for the duration of your employment and for 6 years after the end of your employment with us.

Customers - depending on the category of the personal data the retention period will vary. Majority data we will keep for 6 years after the end of the contract but some, e.g. Pharmacovigilance information we will keep for 10 years.

Suppliers - depending on the category of the personal data the retention period will vary. Majority data we will keep for 6 years after the end of the contract.

In some situations, we may keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons.

10. How can you access, amend or take back the personal data you have given us?

It's important to remember that even if we already hold your personal data, you still have various rights in relation to it. If you would like to get in touch with us about any of these, please contact:

Data Protection Officer
IEL
The Barn
Church Lane
Chilcompton
BA3 4HP
or email **data@imagingequipment.co.uk**

We will seek to deal with your request as soon as reasonably possible, and in accordance with any law requirements. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

To protect the confidentiality of your information, we will ask you to verify your identity before proceeding with any request you make under this policy. If you have authorised a third party to submit a request on your behalf, we will ask them to prove they have your permission to act.

You have the right to request:

- Access to the personal data we hold about you. This would be free of charge in most cases.
- The correction of your personal data if it's incorrect, out of date or incomplete.
- To have your personal data erased in some circumstances, e.g. when you withdraw consent, or object and we have no legitimate overriding interest, or once the purpose for which we hold the data has come to an end.
- That we stop using your personal data for some or all forms of direct marketing. You can decide how you would like us to keep in touch with you.
- That we stop any consent-based processing of your personal data after you withdraw that consent.
- To have your personal data transferred between us and other companies.
- Not to be subject to a decision based solely on automated processing which significantly affects you (including profiling). **We do not use automated decision making at IEL.**

Subject Access Request
You have the right to request a copy of any information that we hold about you, at any time. We will ask you to let us know what personal information you want to access and the date range of the information you wish to access.
Once we have all the information necessary to respond to your request we'll provide your information to you within one month. This timeframe may be extended if your request is particularly complex. If the request is deemed as excessive or unfounded a fee may be charged.

Your right to withdraw consent
Whenever you have given us your consent to use your personal data, you have the right to change your mind at any time and withdraw that consent. Please let us know about it by emailing data@imagingequipment.co.uk.

Where we rely on our legitimate interest
In cases where we are processing your personal data on the basis of our legitimate interest, you can ask us to stop for reasons connected to your individual situation. We must then do so unless we believe we have a legitimate overriding reason to continue processing your personal data.

Direct marketing
You have the right to stop the use of your personal data for direct marketing activity through all channels, or selected channels. We must always comply with your request.

11. What to do if you are not happy?

In the first instance, please talk to us directly and we will do our best to resolve your problem or query. You also have the right to contact the Information Commissions Office (ICO) if you have any questions about Data Protection. You can contact them using their help line:

0303 123 113 or at www.ico.org.uk.

12. Do we store and transfer your data internationally?

Our parent company, Advanced Accelerator Applications (AAA) is a French Radiopharmaceutical Company with Headquarters in Saint-Genis-Pouilly and offices in 13 countries including some executive offices in New York, USA.

Advanced Accelerator Applications is owned by Novartis, based in Basel, Switzerland. Novartis is a multinational company with offices across the world.

We may share, at times, some limited personal data about our employees with AAA and/or Novartis and subsequently transfer it outside of the UK and EEA. We would only do it in order to fulfil contractual obligations, because of law requirements or because we have some legitimate interests.

We may also share our customers details with our suppliers, who are based outside of UK and vice versa. This will be done as a part of a contract, because we have legitimate interests to do so or because of government agencies requirements, e.g. pharmacovigilance or post sales customer care.

In every situation where we transfer any personal data internationally we ensure that the data is transmitted in a safe and secure way. We also only share it when we are certain that those parties

have adequate protections and procedures in place (e.g. US Privacy Shield or Standard EU contractual clauses).

13. IEL website

Please note, we don't track cookies. If we decide to start tracking them, we will update this section of policy and tell you how and which cookies we track if you choose to allow us.

14. What are our Legitimate Interests?

In certain situations, we will process your personal data because of our legitimate interests. General Data Protection Regulation outlines legitimate interests as: "*processing that is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection.*" (GDPR, Rec.47, 48; Art.6(1)(f))

If we choose to rely on legitimate interests, we will always fully consider and protect your rights and interests.

For example, we may rely on legitimate interests when establishing the length of period of retention of our employees' personal data. We keep the majority of employee information for 6 years after the end of employment even if it's not required by law. This is because, in rare situations, we may need to use this data to defend legal claims. This personal data will be appropriately and safely stored and access to it will be very limited in line with this policy and law obligations. Impact on employees' rights and freedoms is very low.

We may rely on legitimate interests for marketing activities too. We would ensure that our use of your data is proportionate, has a minimal privacy impact, and we would only send information that we believe, you would not be surprised to receive or be likely to object to receiving.

15. What would we do in the case of a Data Breach?

If we discover that there has been a breach of any personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner's Office within 72 hours of discovery and notify everyone who could have been affected by the breach. We will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

16. How you can get in touch with us?

We hope that this Privacy Policy has helped you to understand the way we handle your personal data as well as your rights to control it.

If you have any questions that haven't been covered please contact our Data Protection Officer who will be pleased to help you:

Via email: data@imagingequipment.co.uk

Or write to us at Data Protection Officer, IEL, The Barn, Church Lane, Chilcompton, Somerset, BA3 4HP.

17. Our Training

We ensure that everyone at IEL knows and understands their data protection responsibilities. We provide training during induction and a regular refresher as and when required.