Imaging Equipment Ltd

Privacy Policy

IEL Global Privacy Policy

Effective: 22nd June 2018

Version: 2.0

Version History

Dated	Author	Version
22 June 2018	Magda Schroeder	Version 1.0
08 May 2019	Thomas Love	Version 2.0

Contents

1. Introduction

1.1 Purpose

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.

1.2 Scope and Applicability

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. 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. Principles

Data privacy is receiving increased societal attention and scrutiny, it is an emerging field of law with varying local maturity and evolving interpretation by the courts. We therefore need to apply a principles based approach to our decision making.

All Processing of Personal Information shall comply with the 7 fundamental principles as set out below. The 7 principles are embedded in our commitment to abide by a high standard of ethical business conduct:

Principle 1 - Lawfulness, Fairness and Transparency

Principle 2 - Purpose Limitation

Principle 3 - Data Minimisation

Principle 4 - Accuracy

Principle 5 - Storage Limitation

Principle 6 - Integrity and Confidentiality (security)

Principle 7 - Accountability

3.1 Principle 1 - Lawfulness, Fairness and Transparency

We are transparent about what Personal Data we process, how and why we collect it, use it, and who we share it with. We explain this in clear and simple language. We are lawful and have identified valid grounds for collecting and using Personal Data and have ensured that we do this without breaching other laws. We process personal data in a fair way and are clear, open and honest about how use an individuals Personal Data.

3.1.1 Background

Similar to the first principle of the Data Protection Act 1998, organisations must process personal data fairly and lawfully, with the requirement to be transparent receiving greater emphasis. This important principle both enhances our accountability for our practices and in handling personal data and builds trust and confidence amongst our suppliers, employees, Health Care Professionals, stakeholders and patients.

3.1.2 Implementation

Associates must:

- Provide information to individuals about how their personal data will be used at the time of collection or as soon as possible afterwards. This can be in the form of privacy notices, consent forms, etc.
- Focus on the individuals personal needs and what they need to know and provide specifics about handling of their personal data.

3.1.3 Examples

Employees and/or 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.

3.2 Principle 2 - Purpose Limitations

We connect all collection and use of Personal Data to specific purposes and are clear about what the purpose is for processing from the start. We record our processes as part of our documentation obligation and specify them in our privacy documents. We are aware that we can only use Personal Data for a new purpose if either this is compatible with the original purpose, we have consent or have clear lawful basis.

3.2.1 Background

We will only collect personal data if we have specific and legitimate reasons or lawful requirements to do so. We will only collect the minimum amount necessary for the specific purpose. This will reduce risks associated with the processing of personal data, while demonstrating a responsible use of personal data.

3.2.2 Implementation

Associates must:

- Identify the business objective and legitimate reason for collecting personal data.
- Explore whether alternatives are available to collecting personal data to meet the specific purpose, understand that there may be additional Data Privacy requirements when collecting Sensitive Personal Data.

3.2.3 Examples

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.

3.3 Principle 3 - Data Minimisation

We process Personal Data only in ways compatible with the purposes for which it was collected. We facilitate individuals to exercise their rights with regards to their Personal Data. We use and demonstrate data minimisation practices in line with new accountability obligations, and have noted the links to the new rights of erasure and rectification.

3.3.1 Background

We will only collect the minimum amount necessary for the specific purpose. This will reduce risks associated with the processing of personal data, while demonstrating a responsible use of personal data. We have sufficient personal data to properly fulfil the collection purposes and we periodically review the data we hold, deleting data that we do not need.

3.3.2 Implementation

Associates must:

- Take appropriate steps to use personal information only for specific business purposes described in the Privacy Notice, with legitimate justifications.
- Take appropriate steps to only collect the necessary amount of personal data for the purpose.
- Periodically review stored personal data to ensure accuracy and delete data which is no longer in use.

3.3.3 Examples

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 data 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.

3.4 Principle 4 - Accuracy

We take all reasonable steps to ensure the Personal Data we hold is not incorrect or misleading as to any matter of fact. We keep Personal Data updated where necessary and if we discover incorrect or misleading data, we take reasonable steps to correct or erase it as soon as possible. We carefully consider any challenges to the accuracy of Personal Data.

3.4.1 Background

We ensure the accuracy of any personal data we collect and have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. We take reasonable steps to ensure we delete or correct inaccurate personal data and have noted that the GDPR does not explicitly distinguish between personal data that we create and personal data that someone else provides us.

3.4.2 Implementation

Associates must:

- Take appropriate steps to keep personal data accurate and up to date through the information lifecycle, i.e. from collection through to destruction.
- Keep personal data only as long as necessary for the purpose or as required by law.
- Follow the processes put in place to identify when we need to keep the data updated properly.
- Comply with the individuals right to rectification and carefully consider the challenges to the accuracy of personal data.

3.4.3 Examples

We have introduced periodic reviews of the data stored and have put in place processes to update and delete data.

We store consent forms on our SharePoint in order to provide proof of consent and to ensure that we can go back and ensure the data on the system is correct.

3.5 Principle 5 - Storage Limitation

We do not keep Personal Data longer than we need it, and can justify the length of time we keep Personal Data for. We have a policy setting standard retention periods and also periodically review the data we hold. We carefully consider the challenges to our retention of data and have put in necessary procedures for individuals to have their data erased.

3.5.1 Background

We note that the storage limitation principle is broadly similar to the fifth principle of the Data Protection Act 1998. We also note that under the GDPR we are allowed to keep anonymised data for as long as we need. In other words, we are able to either delete or anonymise personal data once we no longer need it. Documentation provisions mean that we now must have a policy setting out standard retention periods where possible. We have noted clear links to the right to erasure (right to be forgotten).

3.5.2 Implementation

Associates must:

- Know what personal data we hold and why we keep it.
- Carefully consider and justify how long we keep the personal data.
- Use appropriate processes to comply with individuals' requests for erasure under 'the right to be forgotten'.

3.5.3 Examples

Retention Periods

Bank Details	6 Years after employee leaves
Details of Expenses	6 Years after employee leaves
Customer details	6 Years after employee leaves
Ethnicity	6 Years
Supplier Details	6 Years

The basic retention period at IEL unless stated otherwise on our Data Register in 2 years.

3.6 Principle 6 - Integrity and Confidentiality (security)

We protect Personal Data by using reasonable safeguards to prevent its loss, unauthorised access, use, alteration or unauthorised disclosure and take appropriate steps to keep Personal Data accurate and up to date. We ensure the correct security measures are in place to protect the Personal Data that we hold.

3.6.1 Background

A key principle of the GDPR is that you process personal data securely by means of appropriate technical and organisational measures, which was the same under the Data Protection Act 1998. IEL is responsible for personal data which it has been entrusted with and takes reasonable steps to protect that information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. The nature of the personal data, and the risk of a security incident occurring, will guide the level of protection needed. Sensitive Personal Information requires a higher standard of protection, security risk management should be taken into account when assessing the appropriate level. Security measures may be physical such as padlocks and access cards for building, electronic, such as passwords and encryption, or organisational, such as restricting access to information to only those who require it. We will regularly assess the protocols and verify that the personal data is secure.

3.6.2 Implementation

Associates must:

- Safeguard personal data so that it is not shared with others who do not have a valid business reason to access the information.
- Report any actual or suspected personal data security incident, including loss or unauthorised access, to the relevant persons.
- Consider, with the assistance of the DPO, anonymisation or pseudonymisation of personal data as an appropriate security measure.

3.6.3 Examples

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.

3.7 Principle 7 - Accountability Principle

We take responsibility for what we do with Personal Data and how we comply with the other principles. We have appropriate measures and records in place to demonstrate our compliance.

3.7.1 Background

The accountability principle is one of the biggest changes introduced by the GDPR and says that organisations must take responsibility for, and be able to demonstrate compliance with, the other principles. It includes a number of measures that we can, and in some cases must, take. We have implemented the relevant measures to comply with this principle including:

- Adopting and implementing data protection policies
- Taking a 'data protection by design and default' approach
- Maintaining documentation on our processing activities
- Appointing a data protection officer (DPO)
- Adhering to relevant codes of conduct

3.7.2 Implementation

Associates must:

- Consider all instances where personal data is at risk and take appropriate measures to ensure the security of the data
- Take responsibility for their actions wherever personal data is involved, taking precautionary measures to avoid security breaches.
- Ensure knowledge of all relevant data privacy documents and review training documents provided by IEL.
- Report any actual or suspected personal data security incidents, including loss or unauthorised access, to the relevant persons.

3.7.3 Examples

During the process of becoming compliant with the GDPR when it was announced, we appointed a Data Protection Officer to oversee the process and implement changes. You can contact them below:

Via email: data@imagingequipment.co.uk

Or write to us at:

Data Protection Officer, IEL, The Barn, Church Lane, Chilcompton, Somerset, BA3 4HP

We have created all the relevant policies to ensure personal data is treated with the care and caution that the GDPR requires.

4. Implementation

4.1 Subject Access Request's (SAR's) and Opting Out

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, Manor Farm, Church Lane

Chilcompton

Somerset

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.

4.2 Training of this Policy

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.

4.3 Third Parties

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 European Economic Area (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).

4.4 Breach of this Policy

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.

4.5 The IEL Website

We track cookies using Google Analytics. When you first go on the IEL website a pop up will appear allowing you to accept or decline cookie tracking.

4.6 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.

5. Contacting IEL

5.1 How to get in touch

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

5.2 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

Privacy Policy

IEL Global Privacy Policy