

IMT MEDICAL TRANSPORT LIMITED - DATA PROTECTION AND UK GDPR. (16 MARCH 2023)

This Micro Data is updated with regards the law enforcing process.

The Guide to Law Enforcement Processing is part of a guide towards Data Protection. It is for those who have day-to-day responsibility for data protection in companies with law enforcement functions.

It explains the data protection regime that applies to those authorities when processing personal data for law enforcement purposes. It covers part 3 of the Data Protection Act 2018 (DPA 2018), which is separate from the UK GDPR regime.

It explains each of the data protection principles, rights and obligations. It summarises the key points you need to know and answers frequently asked questions.

Where relevant, this guide also links to more detailed guidance and other resources, including ICO guidance and relevant European guidance published by the European Data Protection Board (EDPB). EDPB guidelines are no longer directly binding to the UK regime, but are included as a useful reference resource.

At a glance.

- Part 3 only applies to competent authorities (or their processors) processing for criminal law enforcement purposes.
- Processing for other general purposes such as HR will fall under the general processing regime in part 2 of the DPA 2018.
- It applies to processing of personal data, which is information about identifiable living individuals.
- Controllers determine how and why the data is processed. Processors process data on their behalf, but may share some accountability for the processing.
- There are additional rules which apply to 'sensitive processing' of some specified types of particularly sensitive data.

What is the UK GDPR?

The UK General Data Protection Regulation (UK GDPR) is part of the data protection landscape that includes the Data Protection Act 2018 (the DPA 2018). The UK GDPR sets out requirements for how organisations need to handle personal data.

What information does the UK GDPR apply to?

The UK GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

There are additional rules in the UK GDPR for organisations processing special category data. This includes information about an individual's health.

Does the GDPR still apply?

The GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside an amended version of the DPA 2018. The government has published a 'Keeling Schedule' for the UK GDPR, which shows the amendments.

The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to:

- Offering goods or services to individuals in the UK; or
- Monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing, but the way we interact with European data protection authorities has changed.

The UK GDPR sets out the information IMT Medical should supply and when individuals should be informed.

The information IMT Medical supplies about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

The Information Commissioner's Office (ICO)

The ICO are the UK's independent authority created to uphold information rights in the public interest, promote openness in public bodies and data privacy for individuals. IMT Medical is registered with ICO.

The ICO provides free and independent advice on your privacy rights.

You can contact the ICO for advice or log a complaint via:

- Website: www.ico.org.uk
- Helpline :0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers). If you're calling from outside the UK, you may not be able to use the 03 number, so please call +44 1625 545 700.
- Welsh speaking service: 029 2067 8400.
- Rydym yn croesawu galwadau yn Gymraeg ar: 029 2067 8400.
- Normal opening hours are Monday to Friday between 9am and 5pm.

Post:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

What we have done at IMT Medical?

Accountability: We maintain an up-to-date register of our data processing activities.

Data Security: We have strengthened the protection of personal data in the processes and systems of our Company and have passed our annual ISO 27001 accreditation which provides many responsible actions to support data security. We are NHS Digital accredited.

Privacy Impact Assessments: We have reviewed our data processing activity to safeguard the privacy rights of the data subject.

Transparency: We maintain transparency about how data is processed and convey it in a clear and comprehensive manner.

Compliance: We have appointed a Data Protection Officer to monitor internal compliance, to advise and to inform about DPA and UK GDPR and we have taken advice from our insurers and their solicitors.

To keep people informed: We have published a number of updates on our website about the collection and use of their personal data and our staff undertake annual training on matters of confidentiality and DPA.

To have access: We have ensured that to have access to personal data, all are aware of and are able to verify the lawfulness of the processing of the data.

To rectification: We check and monitor if personal data is inaccurate or incomplete.

To erasure/deletion: Of personal data if a compelling reason for its continued processing is missing (also called 'right to be forgotten').

To restrict (or block) processing of personal data.

To data portability to allow personal data to be easily moved, copied or transferred in a safe and secure way.

To object to persons personal data being used for direct marketing and for the purposes of scientific/historical research (We never provide data to anyone for such use).

To have rights in relation to automated decision making and profiling decisions being made about them.