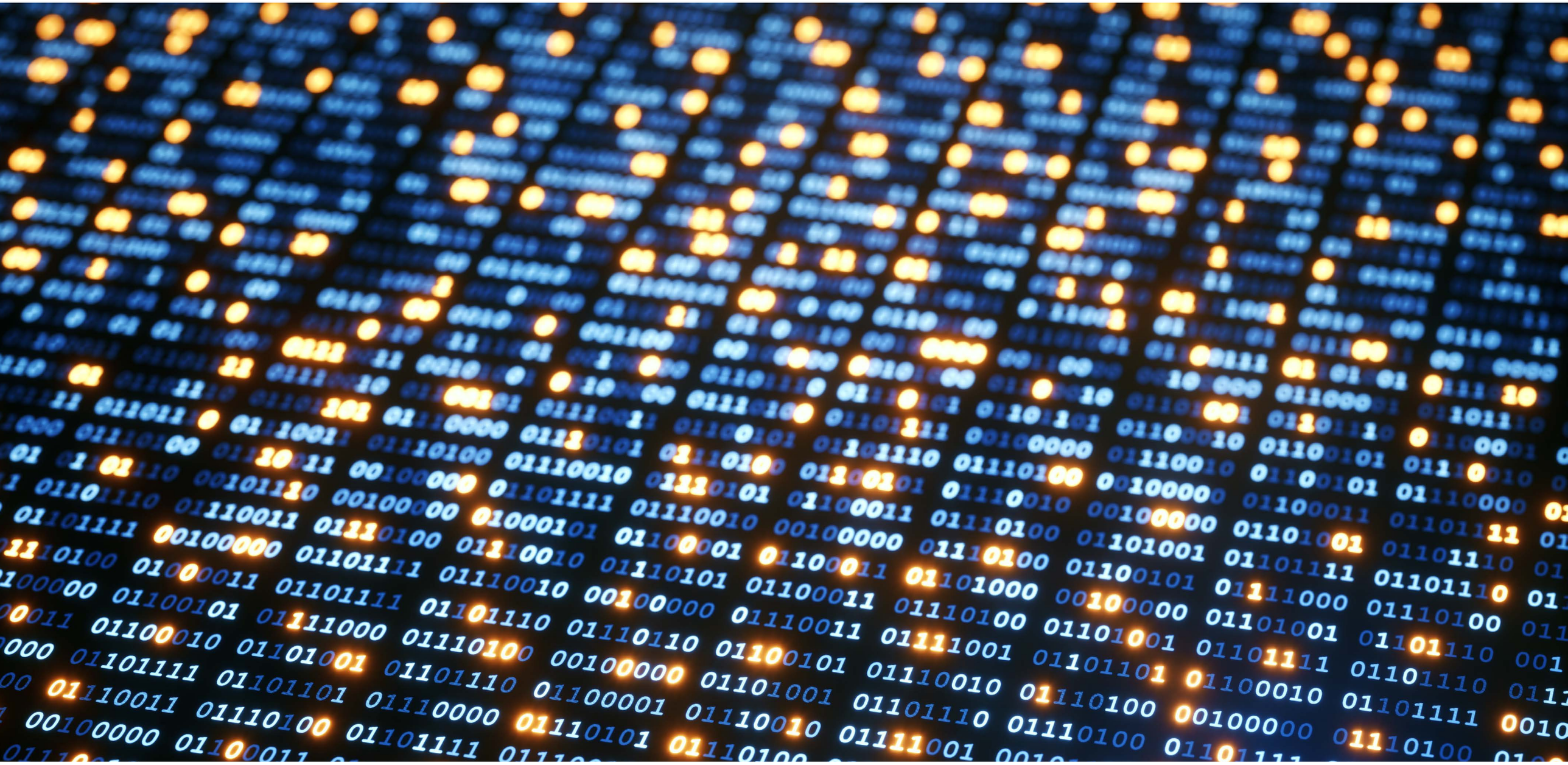
NHS
South Western
Ambulance Service
NHS Foundation Trust



# GDPR for beginners

http://intranet.swast.nhs.uk/information-governance.htm

# Introduction

The General Data Protection Regulation (GDPR), coming into force on 25 May 2018, is an overhaul of data protection law designed to produce a single set of data protection rules for the entire EU. The focus will be on the responsibilities around individuals' data protection, including patients and staff.

Although the regulation comes into force nine months before the UK is scheduled to leave the EU, SWASFT will need to prepare for compliance with the GDPR as while the UK remains in the EU, it will have to abide by the new law. The UK Information Commissioner's Office (ICO) and the government have both indicated that the UK is likely to retain equivalent provisions to the GDPR in whole or in part after Brexit.

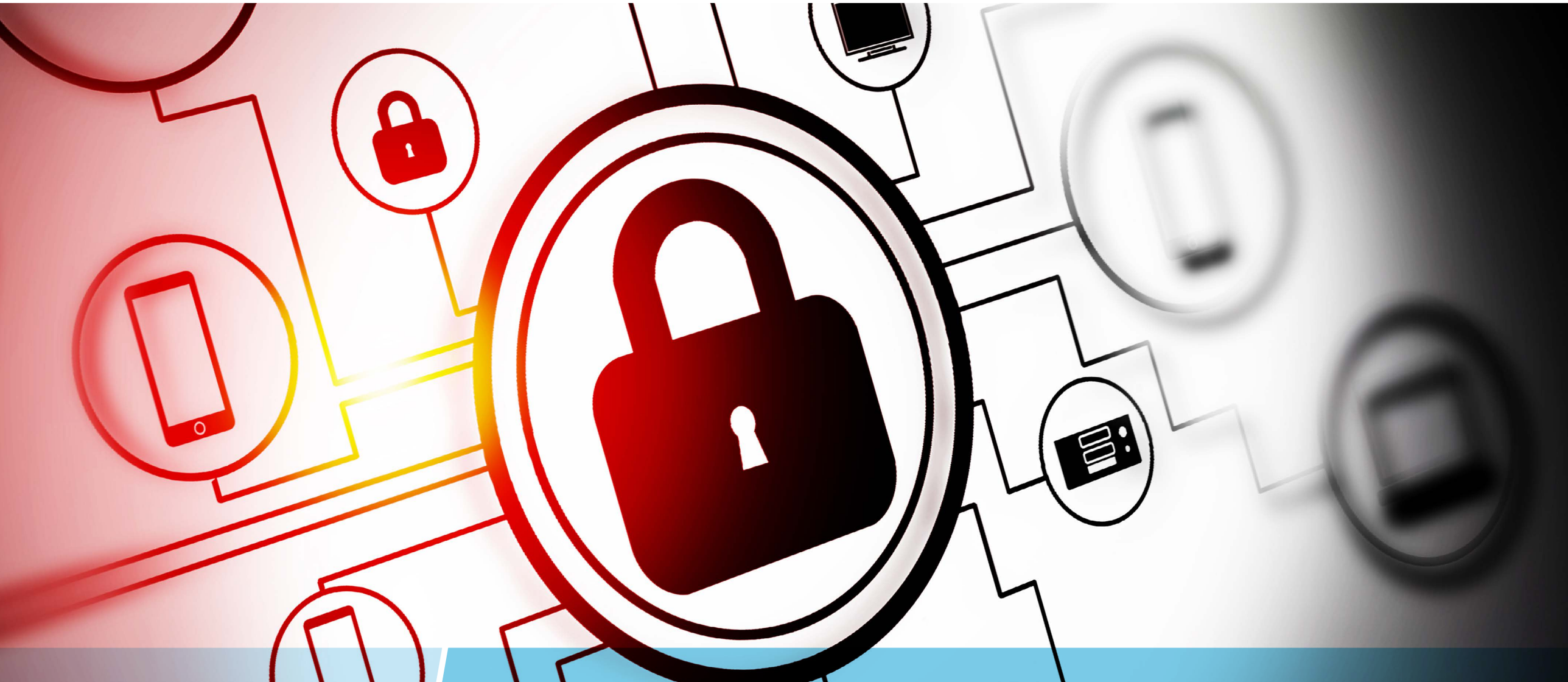
## What personal data is covered?

Personal data means data which relates to an identifiable living individual and includes any expression of opinion about that individual. So personnel records, including sickness absence, performance appraisals, recruitment notes, patient care records etc. are all personal data.

There is extra protection for certain types of personal data (special category data) which includes information about the data subject's race, ethnicity, biometrics, politics, religion, trade union status, health, sex life or sexual orientation. Such data should be treated with particular care.

## Current Data Protection Legislation

The current UK legislation governing data protection is the Data Protection Act 1998 (DPA). The Trust already complies with the current Data Protection Act and so are 85% there in terms of compliance with the GDPR. GDPR emphasises that need for users of data to take more care with the data that they use and keep.




## What are the key changes under the GDPR?

### GDPR Principles (ICO 1)

A significant addition to the GDPR is the principle of accountability. Staff and managers should put in place measures to ensure they are complying with the GDPR and have evidence to demonstrate their compliance.

Conducting an internal audit of processing activities to identify what processing staff actually carry out is critical to compliance and will provide knowledge and understanding of what personal data is processed. Changes could include changing data protection statements in contracts with suppliers, updating or putting in place new data protection policies for clinical data, or implementing a new data protection training regime. The key here is to review all existing practices to ensure they comply with the GDPR.

### Information you hold and process (ICO 2)

Staff are being invited by their departments to conduct a data-mapping exercise. This should be completed by the middle of April. The point of this exercise is to determine what person identifiable data or corporately sensitive data you process and why, where you send it and who you share it with.

You should also identify your processors, such as payroll providers, review the contractual terms, and check the written agreements you have with them meet compliance requirements.

### Special Categories of Data (ICO 2)

GDPR outlines special categories of data which are outlined in ICO2. Under schedule 1, part 1 of the Data Protection Bill we can process this data in accordance with our obligations as a provider of health care or employment. This includes health and equality data.

Systems such as CAD and ePCR also hold special category data; so we need to reconsider if we are handling this data according to GDPR.

## Communicating Privacy Information (ICO 3)

Under the GDPR patients and staff must be provided with much more detailed information about the personal data that we, as an ambulance service and an employer, hold. For example, employers must tell employees the purpose for which any personal data is processed and what the legal basis is for doing so. Similarly we need to explain to patients how their data will be used in their care and by the service more generally.

Amongst other things, any relevant data retention policy must be explained, along with the individual's rights in relation to their personal data, their right to withdraw consent to processing and their right to lodge a complaint with a supervisory authority. All details must be provided in a manner that is concise, transparent, intelligible and easily accessible.

The recommended way to convey this information is to issue privacy notices to staff and patients, which are easily understandable and accessible. Notices will also need to be kept under review to ensure they accurately capture any new types of data collected or any changed uses for that data.

## Individual Rights (ICO 4)

Under GDPR, individuals, or data subjects, will have more control over the data we hold and how we use it. They may ask that their personal information is only shared with named professionals, such as their GP or A&E Consultant, but can request that it is not shared more widely. Data subjects can also request for some or all of their data to be deleted from our systems and for us to ensure that we do not retain any of their data.

There are exceptions in law where a patient's wishes for data sharing and deletion can be overridden. Please contact the Information Governance (IG) team (**information.governance@swast.nhs.uk**) if you have any questions around Individual Rights.

## Subject Access Requests (ICO 5)

The Trust receives subject access requests mainly through Information Governance (IG) and HR. The 40-day time limit for responding to data subject access requests ("DSARs") is being reduced to one calendar month (can be extended for a further two months where request is complex/there are numerous requests). HR and IG will have to deal with DSARs in a shorter timescale, as well as providing additional information.

The data held by the Trust in relation to individuals can be held in a variety of different ways, from formal HR or ePCR records to more informal e-mails among managers or health care providers. Retrieving all the relevant data within the new timescale could be challenging for employers that have not set out clear processes for dealing with DSARs which deal with every step of the process. A fee for making a request will be abolished. This could potentially open the floodgates to an increase in the number of DSARs made by individuals or their legal representatives which may have an impact on our teams to support.

Responding to a DSAR is often complex and the Trust will need to ensure people are trained to recognise and handle them, to apply consistent principles where objections

are made and to ensure that third party data is handled appropriately.

It may also be timely to consider both whether IT systems are "smart" enough to retrieve data (at the right time) and whether staff or patients should be able to access more personal data online (you do not have to supply information the data subject already possesses, or information they can readily access themselves say through a staff portal).

## Lawful Basis for Processing (ICO 6)

Many of our processes currently rely on staff or patients consent to justify all their data-processing activities by including a clause in the employment contract or disclaimer at the outset of the relationship.

Signing an employment contract with a consent clause or a disclaimer on the website will not amount to consent which is freely given so we will, in most cases, be required to find an alternative basis for lawful processing of some data.

We would expect the Trust to rely more heavily on alternative lawful basis, other than consent, for processing in future, these will be:

- public task of the business (for example: performance management of staff or the operational delivery);
- contractual necessity (for example: processing for the purposes of paying employees, sharing patient details for their care);
- necessary for the compliance with a legal obligation (e.g. when you have concerns around safeguarding or criminal activity); or
- vital interests (where the processing of information is necessary to protect someone's life).

Note: The lawful basis only applies to the original purpose for processing. If you want to use that personal data in the future for another reason, then you will need a lawful basis for that or seek consent (e.g. for public relations).

## Staff Monitoring and Surveillance (ICO 6)

The GDPR may make monitoring of staff or vehicles and premises more difficult and there will be more for the Trust to do to demonstrate GDPR compliance.

One of the main recommendations is that the Trust should undertake impact assessments before undertaking surveillance which should, among other things, consider whether the surveillance is necessary and proportionate.

Legitimate interests will be a useful lawful basis among staff as usually the employee surveillance will be undertaken to prevent or detect crime or to detect or stop abuse of the Trusts resources, for example vehicles, internet and email facilities.

## Consent (ICO 7)

Subjects must be informed about the lawful basis for the processing of their personal data.

Consent is one way to comply, but it is not the only want and may health care settings this may not be possible. We do not have to obtain consent where we have an alternative basis for lawful processing for GDPR purposes, and the trust are encouraged to use these alternatives. However, we should consider the different individuals rights under GDPR and what we are processing for. Individuals will have more control over their data where consent is used as the lawful basis for processing under GDPR.

If consent is needed, then the consent should be acquired with the highest of standards:

- freely given and unambiguous;
- as easy to withdraw as it was to give; and
- available to the subject in an accessible format if requested

## Data on Children (ICO 8)

The GDPR contains provisions intended to enhance the protection of children's personal data and to ensure that children are addressed in plain clear language that they can understand. Transparency and accountability are important where children's data is concerned.

It is also consistent with the UN Convention on the rights of the child which provides at Article 12 that every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.

## Data Breaches (ICO 9)

Part of the approach to prevention of data breaches is to ensure that the entire workforce is trained and data aware and to keep records of who has received training. Those with specific responsibilities to handle personal data should receive enhanced training.

## Privacy Impact Assessments (ICO 10)

This GDPR principle aims to put data protection and privacy

at the heart of organisations' policies and procedures. To comply with this, the Trust will consider data protection at the outset when implementing new procedures and policies, for example, outsourcing HR administration or functions or putting data in the Cloud.

Data Privacy Impact Assessments (DPIAs) will be required wherever there is new technology or new processes introduced that may have a privacy implication, for example, the introduction of a new clinical system like ePCR then this would require a DPIA to be conducted.

## Data Protection Officer (ICO 11)

The Trust has an obligation to have a named Data Protection Officer (DPO) because of the special characteristics data that we process. The DPO is also responsible of the management of any data breaches should they occur.

The Trust have appointed DPAS to act as our DPO for 2018/19. They are independent of the Trust Management and can provide impartial advice and monitoring of our compliance with GDPR.

## Processing data by 3rd parties (ICO 12)

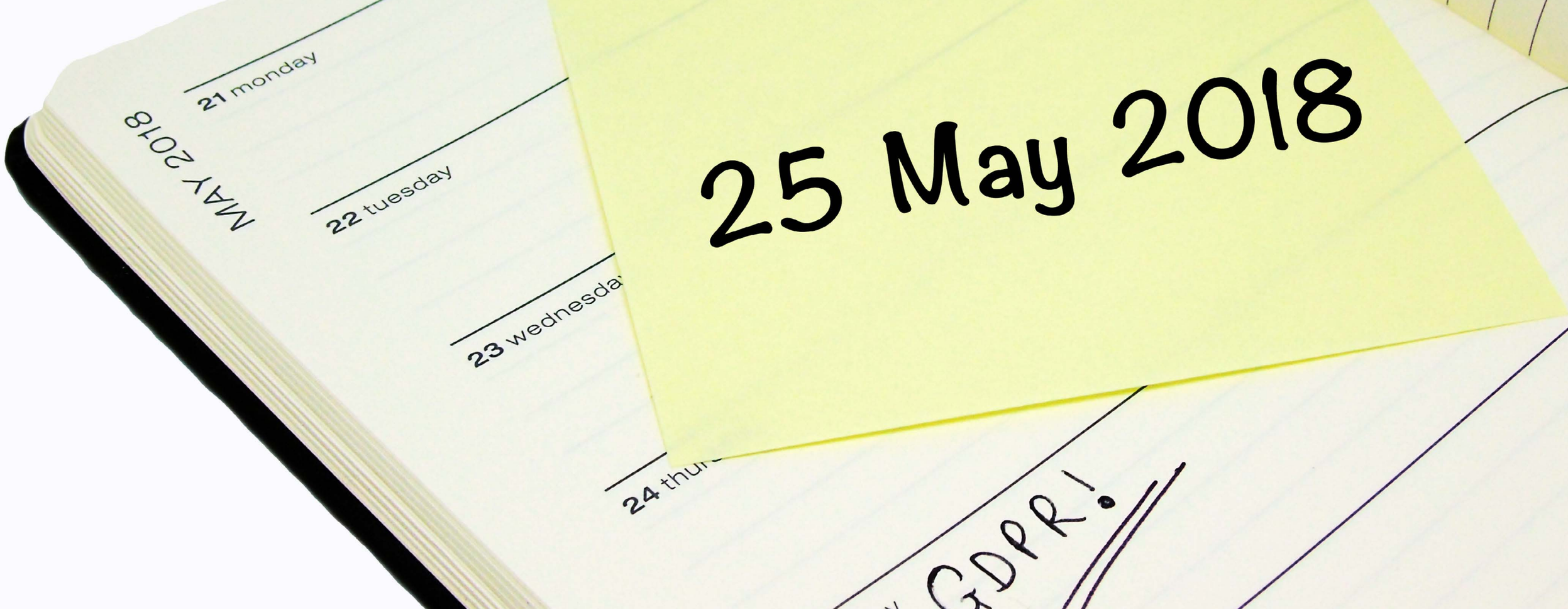
The Trust holds a number of contracts with external suppliers, some of them, such as in IT have access to systems with personal information on them.

The Trust also shares data with other public bodies, for example, safeguarding and serious investigations. For these data flows the Trust will need to ensure that there are information sharing agreements in place that cover the minimum data fields and the purpose for sharing with these other agencies, and that they are compliant.

The Trust is updating the data security and sharing clauses in the contracts and agreements we hold to ensure compliance.

You will also consider the mechanism that data is transferred e.g. securing paper files in lockable boxes, encrypted email and safe haven faxes.

In Summary - GDPR affects all of us in and out of work. The Trust will need every department to help build compliance by 25 May 2018.




## Here are 10 things to remember

- It is not our data, so treat it as if it were your own.
- It is illegal to collect and hold onto personal data without a lawful basis to do so, every time you collect a new piece of information just ask yourself "why" do I need this?
- Sharing is not caring: Personal data is not yours to share, think twice before you hit send.
- People have a right to say "no thanks" so give people the choice and opportunity to say "no thanks".
- If you don't think you need it, the likelihood is you are right. Check the Trust's Retention and Disposal Schedule and if it's not required press delete!
- Change happens for the better; before we change the way we process patient or employee data, think twice about the privacy impacts.
- Partners who look after our systems, IT, websites, payroll and estates - all have the same obligations as we do so let's build a new way of working with a collective approach to keeping data safe.
- If you do not understand it then our patients/ staff will not either. Explain in simple terms what we do with their data and why.
- No means no. Yes means yes. In most cases if someone says stop using my personal data then STOP!
- Data is like oil, used correctly it can enable us to go a long way, but used incorrectly it can leak and become toxic. Hold it and use it safely.

### Guidance provided by

DPAS DATA PRIVACY ADVISORY SERVICE

**info@dataprivacyadvisory.com**
**www.dataprivacyadvisory.com**
**Telephone: 01392 914019**