GDPR Update Jan 2018

Introduction

The General Data Protection Regulation (GDPR) will come into force on May 25th 2018. This new legislation will apply across the EU and replaces the current Data Protection Act 1998. Broadly speaking the new legislation will build on the existing requirements of the Data Protection Act but with more stringent requirements for collecting and processing data and harsher punishments available for those breaking deemed to be in breach of the law.

More detailed guidance and information can be found at the Information Commissioner's Office website.

GDPR Overview

In its fundamental approach to Data Protection, GDPR doesn't differ much from the existing Data Protection Act. It is important to note that there are very few new additions in GDPR and many of the elements have always been legal requirements or best practice encouraged by the ICO.

Key areas of GDPR

'Personal data' is defined under the GDPR as

> *...meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.*
>
> *This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.*

The main principles of GDPR specify that personal data must be:

> *a) processed lawfully, fairly and in a transparent manner in relation to individuals;*
>
> *b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;*
>
> *c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

To summarise a little more briefly, the expectation that is formalised in the GDPR is that you only collect the personal data that you need as you require it and keep it only for as long as you are using it. This data should be collected and used transparently (with permission of the data subject where applicable), accurate and up-to-date and held securely.

There are various other elements to the GDPR including the various rights a data subject has which I would recommend reading into further if possible.

ICU's Data commitments

As part of Imperial College, ultimate responsibility for our use of data lies with the College Data Controller. This would mean that Imperial College would be liable if we or another department were found to be in breach of the GDPR legislation. In the worst cases, fines under GDPR can be up to £20million or 2% of turnover, whichever is higher. However, the risk of this is minimal – as mentioned in a blog by the Information Commissioner, far more likely are warnings and sanctions which are more likely to present a reputational risk rather than financial. Adhering as closely as possible to best practice is essential going forward.

We have been working closely with the GDPR Coordinator in College to work towards meeting full compliance. While we have some work to improve our processes and handling of data, we are perhaps not as much of a concern as other departments or faculties (the Faculty of Medicine is currently recruiting a full time GDPR Coordinator, for example).

Generally, we are in a good position and manage our data well. Our main challenges lie in ensuring good stewardship of data by staff and particularly student Clubs, Societies and Projects.

Our Data

We have a good idea of the data we hold and for the most part we are holding data in centrally managed databases with highly restricted access. The data we receive from College on students and staff is shared with ICU as part of the College T&Cs.

However, there are many processes that need to be considered with regards to Data Protection such as HR, retail and commercial, casual staff management etc. These will all be considered and addressed as we move forward with the process. We also hold various historical data sets on physical and digital media

Actions for Jan - May

ICU will be continuing to approach GDPR compliance across several major areas:

- Data auditing
- Governance and Process
- Training and stewardship
- Systems and Security

Below I will briefly outline these and highlight a few of the actions we will be or are already taking to tackle these. A more detailed plan can be found in the accompanying document.

Data Auditing
An important first step is to understand what data we hold, where it is kept and how we are dealing with it.

- Categorising and cataloguing the data we currently hold
- Auditing Shared drives, emails, databases and websites to understand what data we hold and what should be removed
- List any external organisations that we are sharing data with, if any

Governance and Process
This part of the work is designed to demonstrate an ongoing commitment to upholding the principles of GDPR and ensure Data Protection is a key consideration for the organisation

- Ensuring retention policies are in place for all necessary activities
- Ensuring Privacy Notices are displayed as appropriate
- Reviewing College Data policy and T&Cs
- Put data sharing agreement into place with external organisations if required
- Ensure Data Protection considerations are embedded into the organisation at every level, particularly in project planning.

Training and stewardship
Good stewardship of data is everyone's responsibility. Ensuring staff, officers and students are aware of their responsibilities is a legal requirement of GDPR as part of accountability and governance.

- Ensure staff are properly aware of issues and trained accordingly
- Provide clear guidance on practical approaches to Data Protection
- Formalise policies for CSPs around Data Protection and provide adequate training to ensure compliance

Systems and Security

We will be undertaking various smaller scale development projects to assist with GDPR compliance. These are high priority for the Systems team and include:

- Refactoring how we ingest data from the College Registry feed and how this data is stored
- Adding a more robust emailing preferences module to the website to manage various email subscriptions
- looking in to ways to keep data anonymised and limit transfer of data including managing Club and Society mailing lists.
- As part of our work on our Online Shop, ensuring the highest levels of security are in place and we are not directly handling or storing customer card details

Questions and Discussion

What are the biggest risks posed to the Union around Data Protection and GDPR?

Are there any areas or implications that we have not considered in regards to Data Protection?

What implication will the changes we are making have on our business processes and ability to achieve our strategic plan?

How will we ensure that we maintain best practice into the future?