MANCHESTER 1824
The University of Manchester

GDPR YOUR FIVE MINUTE GUIDE

25 MAY 2018

What is the General Data Protection Regulation (GDPR)?

New General Data Protection Regulations (GDPR), accompanied by a new UK Data Protection Act, will come into force on Friday, 25 May 2018.

The new law is all about person identifying information (PII) and the way that this is collected, stored and used.

It requires organisations that use PII to be transparent in explaining each of these uses to people; to provide choices about these where appropriate to do so; to keep it securely; to only collect and retain the minimum amount of PII necessary to carry out their functions and to only retain it for as long as required.

What is Person Identifying Information (PII)?

PII is any information relating to an identified or identifiable person – this could include reference to their name, identification number, location/address, or other factors relating to their identity.

For example this could be:

- a list of contact addresses eg for marketing or events purposes
- candidates CVs or application information
- correspondence with staff relating to HR matters

The 'To/From' addresses and signatures in emails will generally not be considered to be PII.

If you're not sure if something is classed as PII contact your ***Information Governance Guardian***.

What is a data protection incident?

The University holds the personal data of thousands of staff, students, alumni, research participants and others who have an association with the University. If that data is lost, stolen, corrupted or released to unauthorised persons, the Information Governance Office must be informed immediately.

A potential breach could be:

- lost or stolen devices containing personal data, such as USB devices, laptops, and smart phones
- a successful phishing attempt via email
- paper documents that have been lost or stolen from home, your car or on the train.

What does that mean for you?

GDPR reinforces much of the current Data Protection Act but there some things you'll need to do before 25 May, 2018:

1 Mandatory Data Protection training

All staff are expected to undertake mandatory Data Protection training every two years – this is a condition of access to University IT systems

2 Delete obsolete or duplicate emails, paper or electronic files containing PII

Everyone is responsible for the University data (information) files or documents they store either on their computer, email or as a physical copy in their offices, labs or even at home.

3 Report any data protection breaches straight away

You are also responsible for reporting any incidents to the University where personal data may have been compromised.

1

Mandatory Data Protection training for all members of staff

Have you completed your Data Protection training? Did you know it is a mandatory requirement for all staff members with access to University IT systems to complete Data Protection Training every two years?

You can check when you last completed the course ***here***: ***https://app.manchester.ac.uk/myprofile/training/default.aspx***

If you need to complete the course visit My Manchester and complete the ***online Data Protection e-learning course***.

2

Delete obsolete or duplicate emails, paper or electronic files containing PII

In order for the University to be prepared for the new changes in regulations, we must be able to demonstrate that we are compliant and only keeping the information we need.

All staff members are responsible for the University files or documents they store either on their computer, email or as a physical copy in their office, labs or even at home.

You will have to declare that you are applying the records retention schedule and not retaining person identifying information (PII) longer than necessary.

Check your desks and cupboards for physical copies of information containing PII

Shred any personal, duplicate or obsolete information, especially anything containing PII. Unless there's a legitimate reason for keeping PII, such as that we've been given consent to use it for a particular purpose (eg lists of external email addresses used for marketing/events) then we shouldn't keep it.

You can find out how long different types of records should be kept from the ***Records Retention Schedule***.

Check Outlook for emails containing information as described as above

You should delete all emails which contain PII outside of the period defined in the ***Records Retention Schedule*** as keeping these is unlawful. Going forward it is advisable that you move any emails which contain significant PII (e.g. mitigating circumstances information) into a separate email folder so that they're easier to find. If you find other information, not containing PII, that you do need to keep you might also choose to move this to a separate email folder so that you can find it more easily in future. Remember, most HR information should not be ***retained locally*** but if there is something that needs to be kept privately, such as information relating to a current formal HR process, this should be moved to a separate email folder, moved out of email and saved to a password protected folder on a shared drive, or moved to a P drive and deleted as soon as it is no longer required.

Check the shared drive, your P and C drives

Delete files containing information as described above. You should not be using your C drive in any circumstances as this is susceptible to theft and not automatically backed up like a network drive.

3

Report any data protection breaches straight away

Under the new General Data Protection Regulation (GDPR) we are obliged to report data breaches within 72 hours of becoming aware. The clock starts from the moment we know something has occurred. For example, this could be someone telling their line manager about an email sent containing sensitive person identifying information (PII) to an incorrect recipient.

What do I need to do?

As soon as you are aware of an incident involving PII, or if you're unsure about whether you need to report an incident, you should telephone the Information Governance Office (IGO) on 0161 275 7789 or email ***infosec@listserv.manchester.ac.uk*** in line with the ***incident reporting procedure***.

This is so they can assess whether it needs to be reported to the Information Commissioner's Office on behalf of the University within the 72 hour deadline. If the University does not meet this deadline it could face a six figure fine.

ARE YOU READY?

www.staffnet.manchester.ac.uk/gdpr

datamatters

The University of Manchester
Oxford Road
Manchester
M13 9PL

Royal Charter Number RC000797
M2227 04.18