

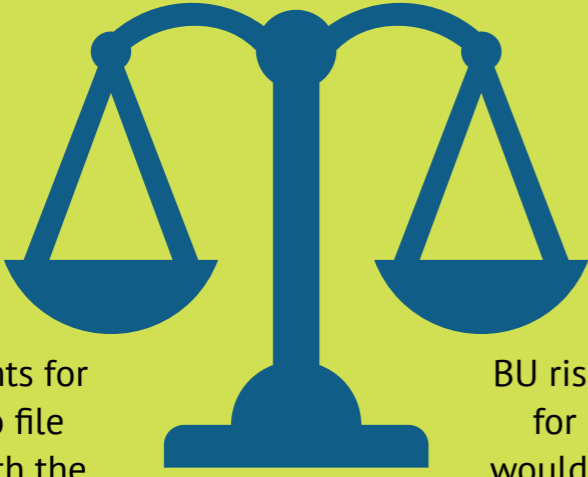
**25**  
May 2018

# General Data Protection Regulation

Be prepared, the GDPR comes into effect May 2018, it has severe implications and penalties for non-compliance.

Applies to **Personal data** - data that allows direct or indirect identification of an individual.

## 1 Serious implications

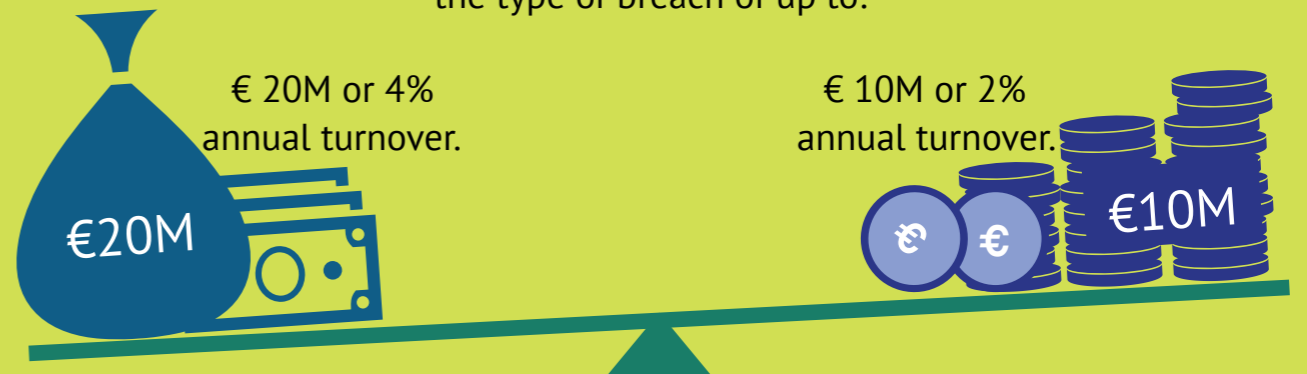


Continued rights for individuals to file complaints with the regulator (the ICO) and to claim compensation.

BU risks reputational damage for breaching GDPR, and would be subject to audit and public noncompliance warnings from the ICO.

## 2 Tough penalties

Fines on a two-tier basis depending on the type of breach of up to:



Source: ICO - <https://goo.gl/DMbz1G>

## What do we need to know?



### Consent

Will require affirmative agreement (opt-in) and explicit consent for sensitive data, must be audible and can be withdrawn by individuals at anytime. [more info](#)



### Audit

Requires audible organisational and technical controls to ensure and demonstrate compliance. BU must maintain records of its data processing activities, such as:

- data subjects, types of data and any third party recipients
- processing purposes
- security standards
- retention periods
- any transfers outside the EEA. [more info](#)



### Subject access requests

Individuals can access their data within 1 month of request. [more info](#)



### Data Protection by Design

Requires Privacy Impact Assessments (a.k.a. Data Protection Impact Assessments) to mitigate risks associated with handling personal data (e.g. pseudonymisation, data minimisation and controls). [more info](#)



### Deletion

Individuals 'right to be forgotten'. [more info](#)  
Data on individuals must not be kept for longer than required.



### Data breaches

Certain types of breach need to be reported to ICO, via the BU Data Breach Management Plan, within 72 hours. [more info](#)



### Data portability

New right for individuals to export their personal data in a structured, commonly used format, such as CSV file. [more info](#)

## What can I do?

Become informed & raise awareness

Audit the data you have access to (physical & digital)

Review your processes / procedures

Decide what to keep and what to securely destroy /delete

Seek guidance on protecting data (e.g. encryption)

Report any concerns, or a data breach incident to [dpa@bournemouth.ac.uk](mailto:dpa@bournemouth.ac.uk) [infosec@bournemouth.ac.uk](mailto:infosec@bournemouth.ac.uk)

## So what is happening at BU?

### WHAT TO DO NOW?

Find more information

<https://goo.gl/8wV0Fr>

[jstevens@bournemouth.ac.uk](mailto:jstevens@bournemouth.ac.uk)

OVC, Poole House, Talbot Campus

### Identify

data sets, locations, owners and processes.

DATA AUDIT

1

2

THIRD PARTY TERMS

### Review

third party terms, and supply chains to determine compliance with GDPR

### Review

policies, privacy notices, and process and procedures relating to consent, deletion and subject access request.

DATA PROTECTION MANAGEMENT

3