General Data Protection Regulation (GDPR) fact sheet number 6

Notification of data breaches under the GDPR

The Information Commissioner's Office (ICO) used to encourage organisations to voluntarily disclose to them that a data breach had occurred, in order to encourage transparency in how personal data was processed. Article 33 of the GDPR now makes notification of a personal data breach **compulsory** in many cases, as explained below.

What is a data breach?

The definition of a data breach can be quite broad and includes:

- access by someone who wouldn't usually have access to it
- loss of the personal data e.g. loss of mobile devices / paper files destroyed
- disclosure to the wrong person e.g. addressing an email containing personal data to the wrong person
- no longer being able to access the personal data.

GDPR requirements

The differences between the voluntary notification under the Data Protection Act 1998 and the compulsory notification under the GDPR are that

- **all** breaches should be notified to the ICO, *unless* the breach is unlikely to result in a risk to the right and freedoms of the individuals whose personal data was part of the breach.
- in any case where the ICO is not notified of a data breach, a record must be kept of the internal investigation and the decision not to inform the ICO for, at least, audit purposes, (a supplementary purpose, not set out in the GDPR, will be to identify any trends in breaches across the organisation and to deal with that trend).
- if the breach has occurred at the premises of, or was caused by, a data processor, the data processor is obliged to inform the data controller (the University's data protection officer) as soon as possible – this would then be the point at which the 72 hours notification period would begin.
- the data processor is then required to provide the data controller with as much help as is required to resolve the breach.
- Article 34 of the GDPR requires that in cases where the data breach is likely to result in a *high risk* to the rights and freedoms of those people whose personal data has been disclosed / lost / accessed, the controller (the University) must inform these individuals of
  - the fact of the breach,
  - who is dealing with it within the University,
  - what the consequences of the breach might be,
  - what is being (has been) done to stop the breach, and
  - what is being done to resolve any issues arising from the breach.
- The requirement to notify the individuals whose personal data might be affected may not be necessary if the data affected is actually inaccessible to anyone else as a result of encryption / password protection, where steps have already been taken to ensure a high risk to the individuals' rights and freedoms is unlikely (anonymisation of the data), or where it would involve disproportionate effort to inform everyone individually, but in this last case the data controller must make a public announcement of the breach and provide contact details for concerned individuals to contact the controller.

- Failure to notify a breach to the ICO when it is appropriate to do so could result in a notification fine, the limit to which is 2% of annual turnover or €10 million, whichever is the larger.

Breach reporting

A data breach must be reported to the relevant competent supervisory authority within 72 hours of being made aware of the breach. In the University's case this will be the ICO in all cases unless the data breach happens in a third country. This may not be the same as 72 hours from the breach occurring, so it is important to be clear when the 72 hours begins.

The ICO has issued guidance on what to do when dealing with a personal data breach based on its original voluntary notification guidance (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) and the University has its own Data Breach Notification policy available at [insert link].

For more information on how to handle a personal data breach, please contact the University's Data Protection Officer, Samantha Hill, on ext 3642 or information-matters@port.ac.uk , or Robbie Walker, Information Security Architect on ext 3279 or Robbie.walker@port.ac.uk .