General Data Protection Regulation
June 2016

Introduction

The General Data Protection Regulation was adopted by the EU in April 2016 and will come into force in May 2018. Although there is a two-year lead-in period, it is vital that universities use all of this time to prepare as the Regulation introduces some significant changes.

The Regulation has an extended territorial reach. It applies to all organisations that process EU residents' personal data – regardless of where those organisations are based. The location of the person whose data is being controlled or processed is now as relevant as the location of the organisation controlling or processing their data.

The Regulation allows organisations to deal with only one supervisory authority. For EU based organisations this will be their home state and for other organisations the authority in the EU state where they do most business. While the UK remains within the EU, the Information Commissioner's Office will be the relevant supervisory authority for British universities.

Non-compliance exposes organisations to a two tier system of significantly increased penalties. Lower tier penalties, defined as fines up to 2% of prior year worldwide turnover or €10 million (whichever is greater), may be incurred for breaches such as: a failure to meet the Regulation's privacy by design provisions; inadequate contracts between data controllers and data processors; or poor record keeping. Upper tier penalties of up to the greater of 4% of worldwide turnover or €20 million can be incurred for poor information security practices; failure to obtain proper consent; or unlawful data transfers to countries outside of the European Economic Area.

Personal Data

The Regulation defines personal data more widely to include any information that relates to an individual and their private, professional or public life. Names, photographs, email addresses, bank details, social network posts, medical information and a computer's IP address all fall within the definition. Genetic and biometric data fall within an extended category of sensitive data which is subject to more stringent control requirements than other forms of personal data. The Regulation encourages the use of pseudonymisation where possible to reduce the risk of sensitive data being linked to individuals.

The legal basis on which personal data is held and processed assumes greater importance under the Regulation. Data may be held and processed because individuals have entered into contracts, for example as employees or as students. Where data is held and processed because individuals have given their consent, then that consent must be given explicitly and actively – pre-ticked boxes, for example, do not meet this threshold. Multi-purpose or blanket consent is not recognised either. Separate consent must be obtained for each processing activity. The nature and purpose of processing activity has to be set out transparently and succinctly. Any request for consent to store personal data must stand out from other terms and conditions and will not be valid if there is deemed

to be an imbalance in power between the organisation seeking consent and the individual providing it.

If personal data relates to a child, their parent or guardian must give consent. Although some jurisdictions may set an age threshold of up to 16, the Information Commissioner's Office, as the UK supervisory authority, will define a child as being under the age of 13 – something that may only rarely apply to universities.

Regardless of the legal basis on which personal data is held, the purposes for which it is to be used, and the length of time for which data will be retained, must be made clear as part of the consent process.

Where data is held on the basis of consent, this can be withdrawn at any time and individuals can request erasure. Processes to allow an individual to withdraw consent cannot be more onerous than the processes that allowed consent to be given in the first place. Erasure can also be requested when the purposes for which the data was originally collected no longer apply. It is important that universities know what personal data is stored, and where, in order to be sure that it is being collected properly. They will also need to ensure data is only used for the stated purposes; is not being retained for longer than it should and can be erased if requested. While these provisions largely exist already under the Data Protection Act, the increased penalties make it essential that universities are managing risks in this area effectively.

Individuals can, as at present, request details of their personal data that is held. Under the Regulation organisations must report clearly on the legal basis on which data is held; and access requests must be fulfilled within one month – rather than 40 days as at present. A charge can only be levied in exceptional circumstances. The right to data portability means that data must be provided in a structured and commonly used electronic format.

Data Protection Officer

The Regulation includes a new requirement for organisations that are public authorities or conduct large scale data processing – including universities – to appoint an independent Data Protection Officer. This person who will help monitor internal compliance with the Regulation is required to have a broad skill set that encompasses both legal requirements and technical IT knowledge. They should have expert knowledge of data protection law and practices; IT processes; technical approaches to cyber security and business continuity. As well as having direct access to an organisation's board or governing body, Data Protection Officers are expected to operate independently from their employing organisations. They will have a legal obligation to notify the supervisory authority of any data breach within 72 hours of becoming aware of it and their performance will be monitored by the supervisory authority.

Data Breaches

There will be a wider obligation to report breaches to the supervisory authority and a further obligation to notify affected individuals if they may suffer an adverse impact from a data breach. Fines will be levied for failure to report a breach, as well as fines for the breach itself. The Information Commissioner's Office advises that organisations ensure they have adequate arrangements in place to detect, report, investigate and manage data breaches.

Privacy by Design and by Default

The Regulation is underpinned by a concern that too often privacy and security are seen as afterthoughts. Data Protection must now be designed into business processes from the outset. In certain situations, for example the introduction of new systems, risk assessments will need to be undertaken and if information processing is considered to be high risk, prior approval must be obtained from the supervisory authority that adequate mitigation measures have been put in place.

Data Controllers and Data Processors

Organisations that collect data are data controllers. They may also be data processors, but where data is stored in a shared cloud, the cloud operator will be a data processor. Under the Regulation it is essential that organisations can demonstrate due care in their selection of data processors and that the respective responsibilities and liabilities of data controllers and third party data processors are set out clearly in contracts. If the third party data processor stores data outside of the EU, additional safeguards are needed.

What You Should Do Now

Universities should assemble the technical and legal expertise to ensure that they are ready to comply with the Regulation. Some steps may involve a considerable lead time, so early action is vital.

- A full understanding what data is held by whom, where and for how long will ensure that universities are able to comply with subject access requests; withdrawals of consent; or requests for data to be corrected or amended. It may also provide an opportunity to move to having a single record for each person – saving both data storage costs and management time.
- In preparation for the Regulation institutions should review their information security and satisfy themselves that they have effective measures to prevent, detect and report security breaches.
- Early review is also important of the disclosure information about data processing and retention and the means by which consent is obtained and recorded. Many universities will need to implement changes to ensure compliance with the Regulation.
- The seniority and breadth of expertise required of the Data Protection Officer may make this post difficult to fill. Universities should give early consideration about how they will do this effectively, but at reasonable cost.
- While universities are already experienced in handling subject access requests, it is worth ensuring that the infrastructure is in place to respond within the shorter timescales allowed by the Regulation and to deliver information in a suitable file format.
- Methodologies for the implementation of new systems and processes need to be reviewed to ensure that the privacy by design requirements of the Regulation are fulfilled.

About Uniac

If you would like to know more, or would like to enlist our help, please contact us:

Ian Musgrave on 0161 247 4697
or imusgrave@uniac.co.uk

finalist
Cyber Security Awards

Certificate Number 13024
ISO 9001, OHSAS 18001, ISO 14001