General Data Protection Regulation (GDPR) fact sheet number 1

The differences between the Data Protection Act 1998 (DPA) and the GDPR

The DPA will be repealed on 25 May 2018 and replaced with the GDPR and the Data Protection Act 2018.

The new GDPR have come about because of the changes in data use since the DPA was written (pre-Internet days) with the intention to bring transparency to the processing of personal data. The main differences are as follows:

- **Technology neutral** - the legislation is now *technology neutral*, so it applies to personal data held and used / recorded in any *format* whether paper or electronic, whether on laptops, phones, USBs, cameras, video tapes, audio recordings, tablets etc,

- **Location data and online identifiers** - the *definition of Personal Data* has changed to include location data (including radio frequency identification tags or information collected as part of 'swiping' an ID card for entry into a building) and online identifiers (Internet Protocol addresses)

- **Sensitive now special** - the term *Sensitive Personal Data* itself changes to Special Categories of Personal Data (SCD)

- **Genetic and biometric data** - the *definition of what constitutes Special Categories of Personal Data* has been extended to include genetic and biometric data but only for the purpose of uniquely identifying a living individual. *Genetic data* is personal data which give unique information about the physiology or the health of that individual. *Biometric data* is personal data which allow or confirm the unique identification of an individual (e.g. fingerprints)

- **Criminal data** - whilst the GDPR has removed *criminal conviction and offence data* from the definition of Special Categories of Personal Data, section 10(5) of the forthcoming Data Protection Act 2018 returns this type of data to the definition

- **Data subject rights -** in addition to the existing *data subject rights,* the following changes have been made:
  - when individuals request copies of the personal data held by an organisation, that data must be provided within one month of the request (was 40 days under the Data Protection Act 1998)
  - individuals have the right of data portability – they can request that the data they provided to an organisation with their consent for processing, should be passed to another organisation in an easily accessible format
  - increased situations where the right to erasure ("the right to be forgotten") can be exercised

- **Lawful basis** – we used to just need to have a condition of processing to make our processing fair and lawful but the GDPR requires us to know and state – in *fair processing notices* – the lawful basis for all types of processing of personal and sensitive personal data, and for this to be made clear at all times (further information on this in **Factsheet 4** – privacy notices)

- **Compulsory data breach notification** – the previous legislation did not compel an organisation to notify the Information Commissioner's Office (ICO) of a data breach, but the GDPR requires data controllers to inform the ICO of data breaches (in certain circumstances) within 72 hours of identifying a data breach, providing certain information, and if necessary, contacting those individuals affected by the data breach

- **Increased fines** -under the GDPR the ICO will be able to impose fines up to 2% of annual turnover or €10 m (whichever is the greater) for offences relating to notification issues, or 4% of annual turnover or €20m (whichever is the greater) for breaches of data subject rights, breaches of the data protection principles and transfers of data to third countries

- **Transparency and accountability** - There is far more emphasis placed on providing information to data subjects about how their personal data will be used and stored

- **Increased responsibility for data processing** - data processors, that is, third parties processing personal data on the instructions of a data controller (doing what they have been asked to do but nothing more) now have more responsibility for training their own staff in data protection issues, maintaining secure processing processes and facilities and for notifying the data controller of a data breach. The data processor will also now be liable for a fine in the face of a data breach (if appropriate). Definitions of the terms data controller and data processor can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/ .

Further information on the changes being implemented by the new legislation is available from the University's Data Protection Officer, Samantha Hill, on ext 3642 or information-matters@port.ac.uk .