General Data Protection Regulation (GDPR)

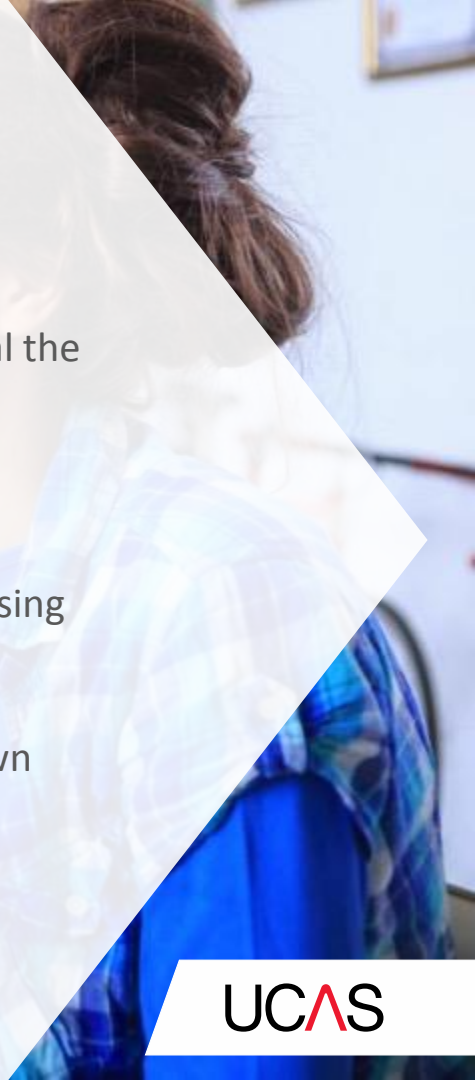
Nigel Parr, Information Governance Manager

GDPR – What does it mean?

- Data Protection Act 1998 – provides an existing DP framework, including Data Protection principles and individuals' rights
- Replaced by the GDPR on 25th May 2018
- Provides the following:
    - Enhanced rights for individuals
    - Enhanced powers for the Information Commissioner
    - Additional obligations for data controllers
- Conflicting opinions
    - 'Data Protection Armageddon'
    - Adds good practice expectations to existing DPA
- Full impact of the GDPR won't be known for many years and will depend on case law and how the Information Commissioner's Office interprets/enforces the legislation

Consent

- Stricter requirements around ‘consent’ for data processing
- ICO guidance produced
- *‘freely given, specific, informed and unambiguous indication’* – likely to signal the end of the pre-ticked opt-in
- For specific and limited purposes
- Consent can be withdrawn by the individual at any time
- Must be as easy to withdraw as it is to provide
- Don’t rely on consent to process personal data if it’s not the basis for processing
- Actions:
    - Review current consents obtained to check GDPR compliance
    - Assess whether processing would continue if consent was withdrawn
    - Look at creation of permissions/preferences dashboards



Privacy Information

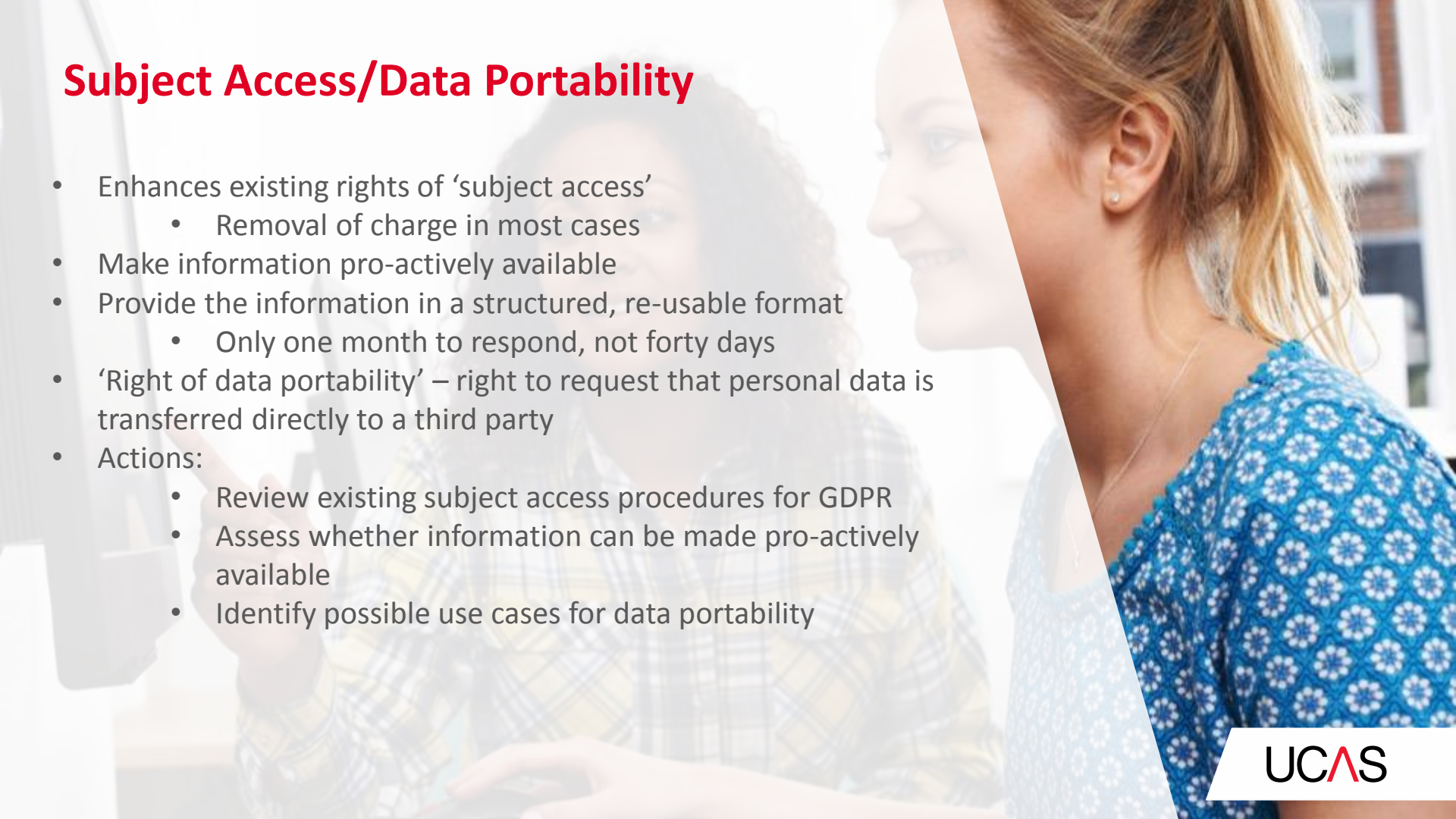
- Enhanced transparency requirements – individuals need to know about uses of the personal data so they can exercise their rights
- Includes specific requirements to notify individuals of retention of personal data, who it is shared with, rights of subject access and data portability, automated decision taking, a named DP contact
- Explain where consent is sought and where we have other grounds for processing (Legitimate interests/public interest)
- Provide the information in concise and easy to understand language
- Actions:
    - Review existing privacy information for compliance and amend as required
    - Consider ‘layered privacy information’ and pro-actively publish why you collected personal data

Right to be forgotten

- DPA - right to deletion is limited to personal data causing unwarranted damage and distress
- GDPR includes statutory right to request permanent deletion of personal data
- Not an absolute right - applies where an individual withdraws consent and there is no overriding legitimate interest to continue processing
- Does not apply where retention is necessary for:
    - Archiving purposes, research or statistical purposes
    - Compliance with a legal obligation
    - Defence of legal claims
- Actions – Identify whether you have overriding requirements to retain personal data and what you can delete, consider data minimisation and also whether you can restrict access to personal data subject to long term retention requirements.

Subject Access/Data Portability

- Enhances existing rights of ‘subject access’
    - Removal of charge in most cases
- Make information pro-actively available
- Provide the information in a structured, re-usable format
    - Only one month to respond, not forty days
- ‘Right of data portability’ – right to request that personal data is transferred directly to a third party
- Actions:
    - Review existing subject access procedures for GDPR
    - Assess whether information can be made pro-actively available
    - Identify possible use cases for data portability



Additional Requirements

- Stricter requirements in respect of ‘automated decision making’
- Privacy Impact Assessments for new projects involving personal data
- Mandatory breach reporting
- Data Protection Officer role
- Tougher penalties for non-compliance

How GDPR impacts on the UCAS/Provider relationship

- UCAS has started to receive enquiries about how we are preparing and whether we will have to make changes to our relationship/working arrangements to accommodate GDPR
- Focus on the consent UCAS obtains from learners and the extent to which this supports the admissions process and possible further uses of data providers might make, such as contacting learners for promotional activities at the point of application
- Also received requests to insert additional specific consents into our admissions process
- Have spoken to HESA regarding their own preparations – intention to provide guidance to providers with a view to facilitating an exchange of ideas

How GDPR impacts on the UCAS/Provider relationship

- UCAS view - GDPR doesn't alter our relationship from a Data Protection perspective
- Under existing Data Protection legislation – UCAS is a data controller responsible for ensuring use of personal data is compliant with the DPA
- Once the personal data is transferred to a provider and used, for example, to populate a Student Record System, the responsibility transfers to the provider, who become the data controller responsible for decisions about use of personal data (e.g. using for communications or retention)
- When learners submit an application through our admissions schemes, they pro-actively consent to the sharing of their personal information with providers, for the purpose of considering and processing their application

How GDPR impacts on the UCAS/Provider relationship

- This wording is unlikely to change significantly
- It provides sufficient consent for providers to use personal data collected by UCAS to support the admissions process, without seeking additional consent from learners
- Plan to issue guidance to providers some time in late June
- Actively want feedback from providers in case there are things we can do to assist preparations for compliance
- May approach the Information Commissioner's Office on behalf of the sector if there are consistent themes to the feedback received

Thank you