TITLE: General Data Protection Regulation (GDPR)

DATE 14 November 2017

AUTHOR: Nigel Parr, Information Governance Manager

Background

An analysis of the main requirements of the General Data Protection Regulation (GDPR) was provided to the Data Group on 19 June 2017. It was agreed that an update would be shared later in the year, focussing on the impact of the GDPR on UCAS' services.

In September, the Government published the Data Protection Bill 2017, which provides greater clarity on the basis for processing 'special categories' of personal data and criminal convictions. UCAS has also asked providers to share concerns or questions about the GDPR.

GDPR - Overall Approach

UCAS' position on how GDPR impacts on our relationship with providers has not fundamentally changed from that outlined in the provider bulletin on 3 July 2017. We remain of the view that both UCAS and providers will act as 'data controllers' under GDPR, responsible for ensuring compliance with Data Protection legislation, through the deployment of appropriate technical and organisational controls.

A good example illustrating this is retention of personal data. Providers periodically ask UCAS how long they can retain personal data accessed via our admissions services. Our position is that we notify learners of UCAS' retention of personal data at the point they access our admissions services. We also notify learners that we will share their personal data with providers so that their application can be considered, however, we do not specifically reference providers' retention of their personal data.

This is because once this personal data is shared with a provider, that provider becomes the data controller, responsible for making decisions about data protection compliance. In the case of retention, we would advise that any decision would be influenced whether the learner subsequently enrols for a course of study, or whether long-term retention requirements exist, such as supporting academic research in respect of admissions. However, providers will reach different conclusion on this matter, based on their own specific requirements and UCAS should not seek to define providers' retention schedules.

GDPR – Specific compliance issues

However, we have identified issues that may affect the services UCAS provides and these are outlined below, accompanied by the actions we are taking to help providers comply.

Consent/Basis for Processing – For processing of personal data to be lawful, data controllers must satisfy one of the conditions listed at Article 6 of the GDPR, or Article 9 where 'special categories' of personal data are processed (e.g. ethnicity, sexual orientation). Additional

clarity on processing 'special categories' of personal data is provided within the Data Protection Bill 2017. Data controllers will be required to publish their basis for processing.

UCAS has therefore reviewed the processing of personal data undertaken to support our admissions services and other services we provide. Our intended basis for processing is attached at Appendix A. Wherever possible, we have sought to rely on the following grounds:

- Fulfilment of a contract;
- Processing in the public interest/substantial public interest;
- Legitimate interests.

The privacy information and the terms learners accept when applying through UCAS' admissions schemes will be amended to reflect this. We have done this to avoid relying on consent as the Article 6 basis for processing wherever possible, because consent under the GDPR can be withdrawn at any time.

In practice, this will mean that learner consent will not be the lawful basis that supports most of the admissions services and should provide greater certainty around UCAS' and providers' processing of this data.

Criminal Convictions - UCAS currently asks two questions regarding criminal convictions; one asked of all learners in respect of unspent criminal convictions and an additional, course level, question where the course applied for has been identified by a provider as requiring an enhanced disclosure check, such as social work.

The Data Protection Bill 2017 was intended to provide clarity on the circumstances under which data controllers process personal data about criminal convictions. However, UCAS' initial review of the Bill did not identify an unequivocal lawful basis to support the continued collection of the criminal conviction question asked of all learners. Similar concerns were raised by a small number of providers.

We have therefore written to the ICO to seek clarity on this issue. Our letter has:

- stressed that providers require this information to conduct risk assessments and fulfil their duty of care to learners and staff;
- referenced the advice they issued in 2009 when UCAS originally considered extending the scope of the criminal conviction questions, a proposal which at the time they considered to be legitimate and proportionate:
- stated what we consider our lawful basis for asking this question is.

We are currently awaiting the ICO's response.

Privacy Information – The GDPR enhances existing requirements to notify individuals about uses of their personal data, including notifying individuals of the following:

- Purpose of the processing of personal data and the legal basis;
- Any recipients of the personal data;

- Retention of personal data;
- Individuals' rights under the GDPR;
- Nominated Data Protection contact.

This list is not exhaustive. Many providers have asked UCAS what it tells learners about use of personal data accessed via our admissions services. UCAS' current declaration within our UG admissions service notifies learners that:

'We share personal information in your application with the universities and colleges that you have applied to, so that they can consider and process your application. This will also include sharing your results from the examination and awarding bodies with the universities and colleges where you hold offers'.

UCAS is reviewing the privacy information we provide to learners. In our opinion, adding additional wording to cover all conceivable further uses by providers would make our privacy notices unwieldly, however, we would consider minor enhancements to reference further uses common to all or most providers.

The GDPR enhances requirements to provide information about uses of personal data, where a data controller obtains personal data via a third party. Providers will be expected to notify applicants about their uses of personal data within one month, or when the first communication takes place. Whilst it is the responsibility of providers to ensure that they satisfy these requirements, UCAS is currently exploring whether we can help providers make their privacy information more prominent to learners.

Direct Marketing – UCAS notifies learners that providers use their personal data to consider their application.

Some providers have asked UCAS for guidance on the types of communications they can send to learners once they have received an application and at a recent meeting of the Higher Education Marketing Data Group, a provider shared advice provided by the ICO about communications issued to applicants. This advice suggested that contacting applicants about things not directly necessary for the purposes of the application would be classed as direct marketing, where additional consent would be required. An example of communications classed as direct marketing by the ICO in their advice was invitations to post-offer open days.

A request was made for UCAS to approach the ICO on behalf of the sector, to obtain guidance on the communications providers can issue without obtaining additional consent. We have therefore written to the ICO on this issue. The letter has highlighted the types of communications providers send to applicants, stressed their importance to the admissions process and our opinion that the issuing of such communications is covered by the 'legitimate interests' condition and that additional consent is not required. We are currently awaiting the ICO's response.

Further Actions – We expect to publish guidance to providers on the GDPR before the end of the calendar year, which will include any feedback received from the ICO.

We will also monitor the progress of the Data Protection Bill 2017 and advice from the ICO and provide feedback to providers if anything of relevance to our services is identified.

We have also worked closely with HESA to be confident that we are interpreting the provisions of the GDPR in a consistent manner and ensure that this is reflected in any advice we issue on the subject.