

# UCAS' provider **General Data Protection Regulation (GDPR)** briefing



## General Data Protection Regulation – Briefing note

This briefing note provides details of the actions UCAS is taking to ensure our services comply with the provisions of the General Data Protection Regulation (GDPR). It also outlines the actions providers should consider when reviewing their own compliance.

It is not intended as legal advice; however, we would recommend that you share its contents with colleagues responsible for Data Protection compliance.

### Background and scope

The GDPR and Data Protection Bill 2017 will come into force on 25 May 2018. They represent the most significant change in Data Protection laws for almost twenty years.

Providers have asked us whether we are making changes to our services to accommodate GDPR, and raised specific questions about 'opt-ins' for uses of personal data and what we tell learners who submit applications about providers' subsequent uses of personal data.

In addition, to better understand providers' concerns, we have attended UCAS stakeholder groups (Data Group, Higher Education Marketing Group, Technology Group) to seek additional feedback from the sector. This briefing note seeks to address the questions we have received. We have also liaised with the Higher Education Statistics (HESA) to ensure the guidance we issue about GDPR is consistent with their own.

This briefing note is not intended to provide a general guide to the GDPR, as providers are ultimately responsible for ensuring they comply with the GDPR. It does, however, set out what UCAS is doing in respect of the services we provide, and the actions you may wish to consider as a means of enhancing compliance in your own institutions.

### GDPR – Overall approach

UCAS outlined how the GDPR will impact on our relationship with providers in [the 3 July 2017 provider bulletin](#). UCAS and its providers are 'data controllers' under GDPR, and are responsible for ensuring compliance with Data Protection legislation.

This is illustrated by the retention of personal data. Providers periodically ask UCAS for how long they can retain personal data accessed through our admissions services. We believe providers should determine this for themselves, based on their own retention policies and continued requirement to use personal data.

UCAS notifies applicants of our retention of personal data via our [privacy policy](#) and applicant [terms](#). We also notify applicants that we share personal data with providers, so they can consider their application. However, we do not specifically reference providers' retention of personal data, as, once a provider accesses personal data (e.g. for the purposes of making an admissions decision) the provider is the data controller, responsible for making decisions about data protection compliance.

Retention decisions will likely be influenced by whether the applicant enrolls for a course of study, and retention is necessary to support statutory reporting or research. However,

providers are likely to adopt different approaches, based on their own requirements; UCAS would not seek to define a preferred retention period.

## **GDPR – compliance issue specific to UCAS' services**

Below, UCAS has identified issues that affect the services we provide, accompanied by the actions we are taking to help providers comply.

### **Issue 1: Basis for processing and consent**

For processing of personal data to be lawful under the GDPR, one of the bases for processing personal data listed at Article 6 of the GDPR must be met. Where 'special categories'<sup>1</sup> of personal data are processed, a condition listed at Article 9 (2) must also be met. Unless you can satisfy one of these conditions, you cannot process personal data.

### **What has UCAS done?**

There has been an assumption that most of our uses of personal data have taken place with the consent of applicants, which is provided when they voluntarily submit an application. In light of GDPR requirements, we have reviewed this to be specific about the basis for processing personal data and advice provided by the Information Commissioner's Office on consent.

UCAS' intended basis for processing personal data (and special category personal data) 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

Wherever possible, we have sought to avoid relying on consent as our basis for processing personal data. This is due to the restrictive conditions surrounding the processing of personal data with consent. Guidance from the Information Commissioner's Office clarifies that consent:

- Must be a pro-active indication of the individual's wishes.
- Must be for specific purposes.
- Can be withdrawn at any time – the use of personal data would have to stop if consent was the basis for processing.

To meet the requirements for consent, UCAS is amending the 'opt-ins' to marketing within our admissions schemes, to ensure they are pro-active and GDPR compliant.

---

<sup>1</sup> Special Category personal data includes the following: racial or ethnic origin, political opinions, religious opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, health, sexual orientation. Personal data relating to criminal convictions is also subject to stricter conditions.

The information we provide to applicants about uses of personal data will be amended to ensure the Article 6 basis for processing their personal data is made clear to them.

However, we are still seeking to clarify our basis for collecting personal data relating to criminal convictions. When applicants apply, they are asked to declare whether they have any relevant, unspent criminal convictions. If a applicant is applying to a course that leads to certain professions or occupations exempt from the Rehabilitation of Offenders Act (1974), they are also asked to declare whether they have any criminal convictions generally.

The Data Protection Bill was intended to provide clarity on the circumstances under which organisations could process personal data about criminal convictions, and the legal basis for doing so. However, it was more ambiguous than expected, and concerns around our continued collection of this personal data have been raised by a small number of providers.

We wrote to the Information Commissioner's Office (ICO) in October 2017 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 the ICO issued in 2009, when UCAS originally considered extending the scope of the criminal conviction questions, a proposal which at the time was considered to be legitimate and proportionate
- stated what we consider our lawful basis for asking these questions is

The ICO have confirmed they are reviewing our letter; we have provided requested clarification and are awaiting a final response.

**Further actions:** UCAS will share the response from the ICO as soon as it is available. It's recommended providers identify the basis for processing, relevant to their own processing of personal data.

## Issue 2: Privacy information

The existing Data Protection Act 1998 requires data controllers to provide information about their uses of personal data. The GDPR enhances these requirements to include details of the following:

- purpose of the processing of personal data
- the legal basis for processing
- recipients of the personal data
- retention of personal data
- individuals' rights under the GDPR
- nominated Data Protection representative

The above list is not exhaustive and the GDPR requires the information provided to be 'concise, easily accessible and easy to understand'.

## What has UCAS done?

UCAS improved the privacy information about our uses of personal data in 2015, and it already meets many of the GDPR requirements. However, we are currently reviewing our privacy policy to ensure it meets the enhanced requirements, and how it can be provided in a more user-friendly way.

Many providers have requested to know what UCAS tells applicants about providers' use of personal data, accessed through our admissions services. UCAS' existing terms within our UCAS Undergraduate admissions service notifies applicants that:

'We share personal information in your application with the universities and colleges that you have applied to, so 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'.

We also notify learners about the collection of sensitive personal data, such as ethnicity data, and inform the applicant that this personal data is provided after an admissions decision has been made. Similar wording is provided within our other admissions schemes.

We provide the following information to learners who attend UCAS events in respect of sharing their personal data with exhibitors:

'We will provide exhibitors with your date of birth, current school, and year, when you want to start university, the areas of the country where you want to study, and the subjects you want to study. We will also let them know whether you are considering studying overseas or at a conservatoire, interested in a gap year, apprenticeship, or going straight into employment. If you have chosen to provide the subjects you are currently studying, this will also be provided.

The exhibitors may use this information to help ensure any communications you receive from them are relevant and of interest to you. The exhibitor should also provide details of how they use your personal information on their website – you may want to refer to this before you share any personal information with them'.

## What do providers need to consider?

The GDPR also places requirements on organisations to provide privacy information, where they obtain personal data from a third party, which would include the personal data providers have access to through UCAS.

In practice, providers will be expected to notify applicants about their uses of personal data within one month, or when the first communication with them takes place. It is a matter for providers as to exactly how this information is provided to applicants. However, a suggestion is to provide accessible links to a provider's privacy information within initial communications, and reference your lawful basis for processing and obtaining any additional consents you consider necessary.

Providers should share any possible suggestions for enhancing our privacy information by 31 January 2018. UCAS will explore whether we are able to include improved functionality for providers to make their privacy information more prominent to applicants.

### **Issue 3: Providers direct communications with applicants**

UCAS notifies applicants that personal data contained within their application to higher education is used by providers to consider their application.

Providers occasionally ask UCAS what types of communications they can send to applicants that have applied to their institution, and whether they need additional consent. An example is an invitation to post-offer open days, which an ICO official suggests may be direct marketing, and therefore requires consent.

### **What has UCAS done?**

A request was made for UCAS to approach the ICO on behalf of the sector, to gain guidance on the communications providers can issue without obtaining additional consent. We have therefore written to the ICO, highlighting the types of communications providers send to applicants and their importance to student decision-making. We have also stressed the potential negative impact on students if they are required to provide up to five additional consents, to receive communications they would reasonably expect to receive. We will update the sector as soon as we hear from the ICO.

This will not affect the communications issued by providers following attendance at UCAS events, as in these cases students will have specifically 'opted-in' to receive such communications.

**Further actions** – UCAS will update the sector once we have received the ICO's response. We may be able to add information about the types of communications issued by providers, and would welcome input from providers in this regard.

### **Other issues**

This briefing note focusses on issues that providers have raised with UCAS, which we consider to impact upon our relationship. However, the GDPR contains wider provisions that will need to be considered, including:

- requirements to undertake 'Privacy Impact Assessments', considering privacy risks and steps to reduce them before new uses of personal data are approved
- mandatory reporting of serious data protection breaches to the ICO
- enhanced rights for individuals, including the right to request deletion of personal data ('Right to be Forgotten'), rights to object to 'automated decision making' in certain circumstances, and rights to request transfer of personal data to third parties upon request (data portability)

The above requirements are not exhaustive, and will need to be considered by providers themselves as part of a general GDPR plan. However, we are happy to share our thinking in these areas as it is finalised.

We would welcome feedback on both this guidance, and possible amendments to the privacy information we currently provide. We would also welcome further questions about GDPR in terms of how UCAS can further assist providers.

We will provide an update in respect of our discussions with the ICO as soon as possible.

We have also scheduled a GDPR session into the Admissions Conference in March 2018.

Please forward any questions to [datagovernance@ucas.ac.uk](mailto:datagovernance@ucas.ac.uk).

### Appendix A - Article 6 – Basis for Processing personal data – UG Admissions Scheme

Fulfil Contract with Learner	'Public Interest' Processing	Value added processing using additional consent of applicants	'Legitimate Interests'
Provision of personal data from a learner to support an application/sharing of this information with providers to enable an admissions decision to be made.	Processing of personal data to support research functions to inform the sector and sharing with external bodies with statutory or regulatory responsibilities for the sector.	Sharing personal data with HEPs as part of the Direct Contact Service offering.	Linking of applications to Apply Centres – enables Apply Centres to upload references and track progress of applications (learners can choose not to link their application).
Processing of personal data necessary to support the operation of the admission schemes, e.g. provision of examination results from awarding bodies and the sharing of this data with the HEPs.	Sharing of personal data with providers for reporting requirements/enhancing their understanding of their admissions processes.	Sharing personal data with organisations who provide services directly relevant to learners applying to higher education, such as Student Finance.	

Sharing personal data with providers and sector bodies for fraud and verification purposes.	Sharing personal data with non-commercial bodies to facilitate research about higher education.
Issuing communications that directly support an application, such as those notifying a learner to take action.	Sharing personal data with statutory agencies for crime prevention purposes in individual cases.