University of Nottingham
UK | CHINA | MALAYSIA

Identifying a lawful (legal) basis for processing – a guide

Background

The General Data Protection Regulation (GDPR) will come into effect on 25 May 2018.

The GDPR will replace the Data Protection Act 1998 (DPA) and is considered to advance the protection of personal data and respect for privacy. Many of the GDPR's concepts and principles are similar to those in the DPA, however there are new elements and significant enhancements. For example, there is a greater emphasis on the documentation that data controllers must keep to demonstrate their accountability and the ability for the ICO to issue fines of up to 20m Euros or 4% of an organisation's global turnover (whichever is higher) in the event of a breach.

Introduction

In order to process personal data lawfully under the GDPR, it is necessary to identify a lawful basis for processing and to document it. It is essential that the processing of personal data is necessary in order to justify the lawful basis for processing. If you can reasonably achieve your purpose without using personal data, the lawful basis for processing will not apply.

Understanding what constitutes an individual's personal data

Please see 'Personal Data – a guide' allied to this fact sheet.

Lawful bases for processing an individual's personal data

Article 6(1) of the GDPR states that processing shall be lawful only if and to the extent that at least one of the following applies:

(a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Consent conditions are very specific under GDPR and positive, opt in consent is required for it to be legitimate. Please see 'Consent – a guide' allied to this fact sheet.

(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

This ground would apply to the bulk of processing necessary for carrying out our relationship with students, staff, applicants for degrees and job applicants. It is not necessary for a full, legal contract to be in place for this ground to be met.

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject.

This ground applies to the University's statutory reporting obligations such as student data supplied to HESA or the Office for Students at their request.

(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

This basis applies where the processing of someone's personal data is necessary to protect his or her life or the vital interests of another individual.

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The University is defined as a public authority under GDPR and as such the bulk of the processing of personal data carried out for teaching and research purposes, the University's 'public tasks' is likely to be on this basis (in addition to the contractual basis with respect to student data in many cases).

(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

This can be used as the basis for processing personal data where the University is **not** performing a task in the public interest, for example fundraising. Using this ground in dependent on a legitimate interest assessment – balancing the rights and freedoms of the individual against the legitimate interest that the University is processing the data in pursuit of.

Documenting your lawful basis for processing

GDPR requires that organisations are able to demonstrate compliance. It is therefore necessary to record your considerations with respect to the legal basis that applies to the process you need to carry out. There is no prescribed format for recording your decision making, the guidance from the Information Commissioner's Office (ICO) recommends that you keep 'a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies'.

Please check whether the processing that you need to carry out is already covered by the University's Privacy Notices for applicants and students, staff and alumni, which are available on the website. In this case, you may wish to document which processing purpose is covered by the Privacy Notice, but it should mean your process is less exhaustive.

Special Category Data

Special Category Data is personal data relating to:

- Ethnicity or race
- Political or philosophical beliefs, religious beliefs and trade union membership
- Health, sex life or sexuality
- Genetic or Biometric data

Processing of any of these types of data requires both a legal ground for processing the personal data, then a further special category condition in order for the processing of this data to be lawful.There are also specific conditions for processing criminal offence data.

University of Nottingham
UK | CHINA | MALAYSIA

Conditions for processing special category data

Special category data can be processed if the legal basis for processing a data subject's personal data has been established, **and** one or more of the conditions for processing special category data has been met. These are contained within Article 9(2) of the GDPR:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject.

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(d) processing is carried out in the course of [the organisation's] legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.

(e) processing relates to personal data which are manifestly made public by the data subject.

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) processing is necessary for reasons of substantial public interest.

(h) processing is necessary for the purposes of preventive or occupational medicine.

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats.

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

If you need to process data of this nature, please contact the information governance team for guidance at data-protection@nottingham.ac.uk.

Information that must be supplied to the data subject

Transparency and fair processing are central themes of GDPR. The lawful basis for processing an individual's personal data must be supplied within a Privacy Notice, which informs the data subject of exactly what is being done with their data and what their rights are.

It may well be that the processing you need to carry out is already covered by the University's Privacy Notices for applicants and students, staff and alumni, which are available on the website. If so, you just need to provide a link to these when you are communicating with data subjects about what will be done with their personal data.

For more information please contact the Information Governance Team at data-protection@nottingham.ac.uk.