**Privacy Notices – 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 to Privacy Notices**

GDPR requires all organisations to be transparent about the personal data they process, and to inform individuals of certain things with respect to that data. This information should be contained in a ‘privacy notice’ which should be issued to all individuals whose personal data is processed by the University.

**The information that needs to be in a Privacy Notice**

GDPR is prescriptive about the information that needs to be contained in a Privacy Notice and this is provided in Appendix 1 for information. The University’s privacy notices can be found on the GDPR workspace until 11 May 2018 in draft, and then in final form on the University’s website from 14 May 2018.

These notices should cover the bulk of personal data processing undertaken by university staff where the personal data processed is that of existing university staff, students, applicants for courses or members of the public who visit the university or correspond with it.

**The action you need to take now**

Please read through the draft Privacy Notices on the GDPR workspace or at <https://www.nottingham.ac.uk/utilities/privacy.aspx> after 14 May 2018. Any comments/additions to the privacy notices can be made until Friday 11 May 2018, after which they will be finalised and posted to the University’s website at <https://www.nottingham.ac.uk/utilities/privacy.aspx>.

We can work with you to add to or amend any of the draft privacy notices so that the processing you need to carry out is covered. Once these privacy notices go live on Monday 14 May however they will be difficult to change and if you have not notified us of any additions necessary to them you may find yourself having to prepare a full privacy notice and issue that to the subjects whose data you process. Please send any and all comments and queries on the privacy notices to data-protection@nottingham.ac.uk and we will respond to you.

**What you need to do if the privacy notice doesn’t cover the personal data processing you need to carry out**

In the first instance, please seek guidance from the data protection team at data-protection@nottingham.ac.uk.

If you need to provide additional privacy information, the governance team can help you identify your purpose and legal basis for processing any additional personal data and guide you in which other more general privacy information you should be providing a link to.

Where additional wording is needed, an outline structure is provided in the Privacy Notice procedure.

**Providing this information to research subjects**

Research subjects whose personal data is processed within a research project need to receive the information that a Privacy Notice provides. This should consist of a combination of the Privacy Information available at <https://www.nottingham.ac.uk/utilities/privacy.aspx> and specific information about the purposes of and legal basis or bases for processing an individual’s data. Please contact the data protection team on data-protection@nottingham.ac.uk for help with this, especially if health or other ‘special category’ data will be being collected.

**Other information sheets that may be of use**

* Privacy Notice Procedure
* Identifying a legal basis for processing – a guide
* GDPR update - personal data

**Appendix 1 Information that must be contained in a Privacy Notice**

|  |  |  |
| --- | --- | --- |
| **What information must be supplied?** | **Data from subject** | **Data from elsewhere** |
| **Identity and contact details of the controller and where applicable, the controller’s representative) and the Data Protection Officer** | Yes | Yes |
| **Purpose of the processing and the legal basis for the processing** | Yes | Yes |
| **The legitimate interests of the controller or third party, where applicable** | Yes | Yes |
| **Categories of personal data** | No | Yes |
| **Any recipient or categories of recipients of the personal data** | Yes | Yes |
| **Details of transfers to third country and safeguards** | Yes | Yes |
| **Retention period or criteria used to determine the retention period** | Yes | Yes |
| **The existence of each of data subject’s rights** | Yes | Yes |
| **The right to withdraw consent at any time, where relevant** | Yes | Yes |
| **The right to lodge a complaint with a supervisory authority** | Yes | Yes |
| **The source the personal data originates from and whether it came from publicly accessible sources** | No | Yes |
| **Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data** | Yes | No |
| **The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.** | Yes | Yes |