BEST PRACTICE GUIDE

GDPR is coming – what shall we do?

ucisa
Universities and Colleges
Information Systems Association

Contents

Universities and Colleges
Information Systems Association

University of Oxford
13 Banbury Road
Oxford OX2 6NN

Tel: +44 (0)1865 283425
Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk
www.ucisa.ac.uk

1 Introduction

Overview

Universities and Colleges are increasingly aware of the impending need to comply with the General Data Protection Regulations (GDPR) from 25 May 2018. However, in many institutions this translates to high level corporate projects that do not include or appropriately communicate with the IT community.

Those charged with managing institutions' corporate information systems are well placed to understand both the current practices with regard to data management and the feasibility and impact of changes required to comply with GDPR. Evidence, however, suggests that such colleagues are not always sufficiently included in GDPR projects.

A note on suppliers

Corporate partners are increasingly referencing GDPR in their communications with the sector. This appears to revolve around:

(A) announcing their systems will be *GDPR compliant* by May 2018.

This is concerning as it is not entirely clear what a *GDPR compliant* system really is. GDPR compliance is much more about institutional practice in the use and management of data and the systems in which it resides. It is hard to envisage what could be changed in software to make it GDPR compliant over and above facilities for records removal – but even this needs to be appropriately implemented in each institutional context.

(B) using the *threat* of GDPR as a tactic to promote their products and companies.

This is concerning as in many cases it appears this is being used as a cynical sales tactic – unhelpfully adding to the noise, confusion and misinformation *fog* currently swirling around GDPR in institutions – and also in some cases the product/service is only tangentially related to GDPR.

GDPR – *"it's just DPA v2.0 isn't it?"*

One of the common remarks about GDPR is that it simply takes the principles of the 1998 Data Protection Act (DPA) and enhances them. This may be true in some cases, but the extent to which this is of comfort to institutions depends entirely on the degree to which they were completely DPA compliant. It is apparent that in some cases initiatives to comply with the DPA were either incomplete or acted at a point in time but not embedded for the long run (e.g. a concerted staff training and awareness campaign that covered all staff, but has not been continued to pick up subsequent new hires). Therefore, for some institutions, GDPR compliance first requires a *catch up* (which is understandably hard to publicly admit!)

Policy vs practice

There is a potential disconnect between policy writers and those who ultimately will have to enact it. A concern raised by some is that institutional projects are currently revolving around the authoring of new retention policies, privacy notices, consent agreements and the like which do not reflect current reality and are not implementable. It would be advisable for policy makers in institutions to invite those responsible for implementation of policy to use their practical experience to assist with the drafting of rational, workable policy.

This document

What is concerning IT colleagues is a lack of practical output from institutional GDPR projects. As IT professionals we are aware of many existing inadequacies in our data management which are likely to be more acute under GDPR. This document is intended to serve as a collection of assessments of implementation considerations and practical steps that have/should/can be taken written from the viewpoint of IT/CIS managers.

We have taken as a starting point the 12 steps to GDPR implementation published by the Information Commissioner's Office[1] and for each one sought case studies of real responses to them from around our sector. These are presented (anonymously) here in order to assist others with their own GDPR readiness. In a number of cases we have added some hints and tips in *Be Aware* sections where there might be some improvements to the practice being described. We have done it in this way to highlight where opportunities for improvement exist.

1 *Preparing for the General Data Protection Regulation (GDPR)* **https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf**

We also present a series of FAQs and tips which were drafted by UCISA CISG committee members following a meeting with Victoria Cetinkaya of the ICO.

At the time of writing (in early 2018) GDPR implementation is a live issue. This document, therefore, captures the state of play – both in terms of the thinking in universities and colleges, and the ICO – at this point in time. This will naturally develop over time as details become clearer, and we will seek to publish revisions to this document as and when any substantive changes become required.

You can check for updates to this document on the CISG section of the UCISA website **www.ucisa.ac.uk/groups/cisg**.

2 Disclaimer

This document is provided to help HEIs understand what the sector is doing, and provide some general information from the ICO. It does not constitute legal advice. All institutional contexts are different and what works in one institution will not necessarily translate identically to another. We recommend you seek your own specific advice from your Data Protection Officer and lawyers as appropriate.

3 Contributors

Case studies, FAQs and editorial input have been provided by the following (in addition to a number of anonymous contributors).

Aaron Haile	IT Programme Manager	King's College London	Aaron.Haile@kcl.ac.uk
Albert Chan	Assistant Director for Business Assurance and DPO	King's College London	Albert.Chan@kcl.ac.uk
Brenda Roshier	Project Manager	Cranfield University	brenda.roshier@cranfield.ac.uk
Duncan McCahill	IT Operations	University of Liverpool	duncanm@liverpool.ac.uk
Gareth McAleese	Head of Corporate Applications	Ulster University	g.mcaleese@ulster.ac.uk
James Blair	Head of Application Systems Group	Edinburgh Napier University	j.blair@napier.ac.uk
James Smith	Director of IT	Birkbeck, University of London	jg.smith@bbk.ac.uk
Matthew Marl	Head of Information Systems	University of Wales Trinity Saint David	m.marl@uwtsd.ac.uk
Nath Czechowski	Deputy CDIO (Service Management and Security)	Coventry University	n.czechowski@coventry.ac.uk
Neil Morris	Head of Applications	Heriot-Watt University	n.a.morris@hw.ac.uk
Sally Brown	Head of Corporate Systems	Loughborough University	s.a.brown@lboro.ac.uk
Stefan Kaempf	Head of Production Management	University of Edinburgh	stefan.kaempf@ed.ac.uk

The UCISA CISG Committee would like to record their thanks to Victoria Cetinkaya for her help and advice in the production of this document. Please note this document does not constitute official ICO advice.

4 The 12 steps to GDPR heaven

1. Awareness: The ICO says, "You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have."

Case Study: A – medium sized university

Current situation

Institution recognises it does not have a robust approach to educating new starters, and reminding existing colleagues about their responsibilities regarding *data security*.

Tried to address issues of data security for our staff rather than *GDPR compliance*, as we feel this will have greater traction.

We want to outline the risks as moral and reputational (personal) rather than financial (the institution's problem).

Feel we particularly need to address staff collecting data in *shadow systems* (both on premise, and cloud based), holding data on portable devices (both institution owned and personal) and staff holding data in emails.

Further need to ensure staff are only sharing data with external data processors or other data controllers where there is an appropriate agreement in place.

Communications have already been sent to all staff that explain *data security* guidance for staff (Appendix A).

Assessment of where the institution needs to be/nature of the gap

Ensure that all staff get and understand the message, including all new hires as and when they join.

We can't rely on our *new staff induction events* as they are not held frequently enough.

Update our data protection policy and code of practice and make sure the degree to which this is made clear to new staff made starkly clear is enhanced.

Make it clear what sorts of behaviors that staff may feel are *normal* are unacceptable, e.g:

- Use of third party *free* data processors such as Typeform, Jotform, Survey Monkey.
- Transfer of data to third parties *because it has always been done that way* – without verifying the contractual terms under which it has been done. Make it clear options for carrying on business as usual while complying with the law, e.g.:
- How to use Bristol Online Surveys or Office365 Forms as alternatives for the commonly used *free* options.
- How to arrange *Data Sharing Agreements* with third parties.

Practical steps

To update our video to incorporate specific reference to GDPR.

To embed a *notification* of responsibilities regarding data security within our staff self service application, including the video, and a declaration of compliance.

- Insist that all staff complete declaration within a fairly generous window, after which time access to systems containing corporate data will be rescinded until declaration is completed.
- Insist that all new staff complete declaration before access to systems containing corporate data is provided.

Provide a set of acceptable options for collecting data in university provided systems – e.g. Office 365 forms and Bristol Online Surveys.

Undertake an amnesty of data sharing arrangements, work to ensure existing arrangements formalised and register of them is available for staff to consult.

Unanswered questions

How much training is enough training?

Should we test our staff? What do we do if they *fail* the test?

Should there be a *higher level* training/awareness package?

Should we require counter signing for staff *declarations* of compliance (e.g. to confirm that new staff have discussed the *dos and don'ts* with a *senior* member of staff on arrival.

Resources identified

UCISA Information Security Awareness Training: **https://www.ucisa.ac.uk/groups/exec/infosec_training**

Other institutions misfortunes (makes it real):

https://teiss.co.uk/information-security/oxford-university-leaks-students/

http://www.bbc.co.uk/news/uk-england-norfolk-40306087

Case Study: B – large institution

Current situation

Institution has a set of mandatory training courses for new hires, including data protection and data security. Staff are unable to pass their probation without successfully completing this mandatory training.

BE AWARE

This is good, but there's a danger that this is seen as a one off training. What about existing staff/refresher training?

Case Study: C – large university

Current situation

Establish GDPR champions for different areas within the University. These champions would attend training and be first contacts for GDPR questions within their areas.

Case Study: D - large university

Current situation

As every member of staff processes personal data, all staff need to know about the University's compliance obligations and ensure they are equipped to deal with those arising in their role/area.

This event will cover the following topics:

- The new penalty regime
- Expanded definition of personal data (data you didn't consider to be *personal*, e.g. IP addresses, may now be included, which means you need to provide appropriate security and handling measures to it)
- Requirements to *demonstrate* compliance and accountability
- Privacy by design
- Expanded data subject rights
- New requirements for consent and expanded privacy notices
- What to do when sharing data
- Reviewing all contracts where data is shared and where data is processed outside the EEA
- How do we plan for implementation and what we can do now

Current/topical issues will be included in these interactive sessions and there will be opportunities for Q&As. Links to comprehensive advice and guidance and actions to follow up after a briefing session will also be provided.

Session outcomes for participants are to:

Be clear about their responsibilities under the new Regulation

Recognise the practical data protection issues

Know where to go for advice and guidance

Case Study: E – large university

Current situation

Early stages, need more engagement with all staff and also focused awareness sessions for Data Stewards/Custodians.

Assessment of where the institution needs to be/nature of the gap

Everyone across the organisation needs to understand what's happening, with those it impacts significantly thinking about what they need to do to adapt their processes.

Practical steps

Awareness training for all staff, online training to be completed in early 2018. With targeted webinars for those who require move detail and the opportunity t to join drop in sessions for specific subject matter areas.

Unanswered questions

What the priority projects are, conflicting ideas regarding what should be done now and what can be planed over next few years, what's achievable.

Case Study: F – Large Russell Group university

Current situation

In the process of raising awareness through a series of one day training courses leading to a test and certification.

Assessment of where the institution needs to be/nature of the gap

This is mostly being done in the IT area but needs to go out to the wider University.

Practical steps

A working group has been formed which is chaired by the Head of Legal.

Unanswered questions

Need to undertake more work to identify gaps in our knowledge of the information held especially outside of IT.

Resources identified

The training raised awareness and created the demand for more courses.

Case Study: G – Medium sized university

Current situation

The Institution has set up a focus group to raise awareness of GDPR. This has convened once and has been followed up with a meeting between each Resource area representative and the Data Protection Officer to discuss and produce a summary of *The Issues and Challenges of GDPR compliance* in their area. These will be considered in the next meeting and Academic Faculties will be invited to complete the same exercise.

Assessment of where the institution needs to be/nature of the gap

This will be considered as a part of the analysis of responses. We have also been in discussion with Jisc about their offer of a *gap analysis* and this whether we should pursue this will be considered in the next GDPR focus group meeting.

Practical steps

This is yet to be quantified.

Unanswered questions

The level of response appropriate for GDPR is subjective. We would like to undertake the GDPR compliance actions in line with the actions of other Universities, and our Data Protection Officer is engaged in regular meetings with other institutions.

Resources identified

Events organised by UCISA to improve awareness of GDPR and what needs consideration.

Case Study: H – Large university

Current situation

Institution is amending its current mandatory training courses on data protection and data security; so that it integrates all of the new points of GDPR. The training will have a pass mark and everyone has to pass. It is intended that staff member would need to take the training at least once year.

Case Study: I – Large university

Current situation

The institution has undertaken a review of GDPR and what impact it would have across all activities. Some of the initial focus has been around fundraising and external activities that are deemed critical to University strategy. A Task and Finish group has been formed to identity activities that need carried out, a gap analysis undertaken against current DPA practices, prioritisation of these activities and ensuring resources are made available to progress the work.

Assessment of where the institution needs to be/nature of the gap

> *2. Information you hold: The ICO says, "You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit."*

Some initial work done in reviewing where we think we are strong with regards DPA, reviewing initial guidance and identify high level priorities. One identified priority is a data inventory/audit.

Practical steps

Make sure you have a training and awareness process as part of your GDPR project. Make sure key technical and functional staff are aware of their duties, ensure they are briefed, they can be useful advocates of good practice. Make sure you have a clear and complete inventory of your data and how it's being used.

Resources identified

Events organised by UCISA and Jisc. Seminars provided by your key suppliers can also be useful in looking at what others are doing towards compliance. ICO website. Also follow the UCISA CISG (@UCISA_CISG) and ICO (@iconews) twitter accounts for useful updates on GDPR.

Other resources/notes

Who is ultimately responsible? – Everyone! All employees should be trained.

It is important for staff to understand that de-anonymisation of data is likely to become a criminal offence in the Data Protection Bill currently making its way through Parliament at the time of writing.

Case Study: A – Medium sized university

The University has established a SharePoint site to provide a repository for the collation of an Information Audit on all personal data processed. The recording of the data is based on the EU General Data Protection Regulation (GDPR) Documentation Toolkit (a commercial offering published by itgovernance.co.uk).

https://www.itgovernance.co.uk/shop/product/eu-general-data-protection-regulation-gdpr-documentation-toolkit

Each system manager is uploading their information about the data they are responsible for into this data recording tool that is delivered to a reporting tool for easy access to review each of the systems. This gives easy visibility of the data we hold and highlights any holes within the data that can be captured and actioned for collection.

The toolkit includes:

- A complete set of easy to use and customisable documentation templates, saving time hopefully ensuring compliance with the GDPR.
- Easy to use dashboards and project tools to ensure complete coverage of the GDPR.

Example: dashboard

The dashboard is an easy way to understand what you have in place with your policies and procedures across your responsible stakeholders across your institutions and allows you to focus on gaps you may have across your policies and procedure records the tool should be used as a live document that changes as the deadline approaches.

Document	Tier	Responsible	Approver	Progress
GDPR DOC 1.0 Data Protection Policy	Tier 1: Policy	Data Protection Officer	Board of Directors	Approved
GDPR DOC 1.1 Training Policy	Tier 1: Policy	Head of HR	Board of Directors Chief Executive Officer (CEO)	Not started
GDPR DOC 2.1 Fair Processing Procedure	Tier 2: Procedure	Data Protection Officer GDPR Owner	Chief Executive Officer (CEO)	Approved
GDPR DOC 2.2 Subject Access Request Procedure	Tier 2: Procedure	Data Protection Officer GDPR Owner	Head of IT (CIO)	Approved
GDPR DOC 2.3 Retention of Records Procedure	Tier 2: Procedure	Data Protection Officer GDPR Owner	Head of IT (CIO)	Approved
GDPR DOC 2.4 Privacy Impact Assessment Procedure	Tier 2: Procedure	Data Protection Officer GDPR Owner	Board of Directors Chief Executive Officer (CEO)	Approved
GDPR DOC 2.5 Breach Notification Procedure	Tier 2: Procedure	Data Protection Officer GDPR Owner	Chief Executive Officer (CEO)	Approved
GDPR DOC 2.7 Consent Procedure	Tier 2: Procedure	Manager/Executive (generic/line)	Data Protection Officer GDPR Owner	Approved
GDPR DOC 2.7A Removal of Consent Procedure	Tier 2: Procedure	Manager/Executive (generic/line)	Data Protection Officer GDPR Owner	Not started
GDPR DOC 2.8 Managing Sub Contract Processing	Tier 2: Procedure	Quality Manager	Data Protection Officer GDPR Owner	Not started
GDPR REC 4.1 Fair Processing Notice	Tier 4: Record	Data Protection Officer GDPR Owner	Chief Executive Officer (CEO)	Approved
GDPR REC 4.1A Fair Processing Notice Register	Tier 4: Record	Data Protection Officer GDPR Owner	Information Security Manager	In Progress
GDPR REC 4.2 Subject Access Request Form	Tier 4: Record	Data Protection Officer GDPR Owner	Board of Directors Chief Executive Officer (CEO)	Approved
GDPR REC 4.3 Data Protection Officer (DPO) Job Description	Tier 4: Record	Head of HR	Board of Directors	Not started
GDPR REC 4.3A Data Protection Responsibilities - GDPR Owner and data protection representatives	Tier 4: Record	Head of HR		Approved
GDPR REC 4.4 Data Inventory	Tier 4: Record	Data Protection Officer GDPR Owner	Chief Information Security Officer (CISO)	In Progress
GDPR REC 4.5 Internal Breach Register	Tier 4: Record	Data Protection Officer GDPR Owner	Chief Information Security Officer (CISO)	In Progress
GDPR REC 4.5A Breach Notification Form	Tier 4: Record	Data Protection Officer GDPR Owner		Approved

The toolkit also gives a number of examples and pre-developed templates of the documents you may wish to develop that you may not have in place, for example *Parental Consent* forms for under 16 year olds.

Included within the toolkit are a complete set of mandatory and supporting documentation templates that are easy to use, customisable and try to ensure compliance with the GDPR, including:

- Data protection policy
- Training policy
- Information security policy
- Data protection impact assessment procedure
- Retention of records procedure
- Subject access request form and procedure
- Privacy procedure
- International data transfer procedure
- Data portability procedure
- Data protection officer (DPO) job description
- Complaints procedure
- Audit checklist for compliance
- Privacy notice

Case Study: B – Small university teaching and research in diverse subject areas

Current situation

The University holds student data in a wide range of computer systems, paper records and unstructured data. Although we have a retention schedule it is not a complete list of all systems, data is duplicated and stored in many forms.

Assessment of where we need to be

We need to understand fully the data we hold and change our culture and attitude to data. To produce a document that records details of all the data that the University holds on its various stakeholders, the reasons for processing that date, retention periods, to be the one place to refer to for understanding of data. To educate staff in the importance of data.

Practical steps

Update the retentions schedule to list all systems which have been discovered through conversations with staff. Meet with designated system owners to document the systems. However, before meeting we need to understand the following:

- The rights of individuals under GDPR
- The processing reasons for data by type
- Interfaces and transfers of data between internal systems
- Transfers of data into and out of the University (data processors contracts)
- Staff, student and other journeys

Discuss with system owners the changes we need to make to the systems, data we need to remove, processes we need to change.

Implement the items agreed above.

Unanswered questions

How we are going to handle the unstructured data held, e.g. data in spreadsheets and reports, which are stored on local drives, shared drives, etc? – Suggestions at present include an awareness approach through communications and a data amnesty to encourage staff to clear files.

Can universities use the legitimate interest process reason or not? – mixed advice at present.

How are we going to remove records or parts of a record from our computer systems?

Guidance not available on all aspects of GDPR as yet.

Resources identified

Using ICO and JISC resources plus a range of supplier material. Nothing that most other people wouldn't have already discovered.

BE AWARE

There is now guidance here: ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing. Note the University example halfway down the page.

Case Study: C – Large university

Current situation

Aware of areas of potential GDPR risk, and *known unknowns*, e.g. processing activity going on across the organisation that we weren't aware of.

Assessment of where the institution needs to be/nature of the gap

Needed a better understanding of what processing was taking place across the organisation, specifically in terms of our four working groups but also in other areas.

Practical steps

Formed GDPR Readiness Board with 4 area working groups covering Research, Workforce, Students and Alumni/ Donors. Each working group asked to completed the record of processing activities, which captures information relating to article 30 requirements, such as categories of information that we hold, categories of personal data, categories of processing, data subjects and those we share personal information with, retention period, general description of security measures.

Added sections to cover data processors (details of who they are), whether a Privacy Impact Assessment (PIA) has been conducted for the particular area, data collection (lawful basis, privacy notices, consent). Working groups have until the end of January 2018 to complete initial review and to submit it to the GDPR Programme manager for review.

Ongoing piece of work, not just a one off and will need to be updated as part of a rolling review process. Additional areas identified, such as marketing and finance, are now also going to complete. Two of four working groups have submitted the ROPA for review to date.

The intention is that the ROPA will give high level map of the processing we complete, and identify areas of risk and gaps to address. Also being used to help to develop GDPR/DPA training, via a training needs assessment for the organisation.

Potential for the ROPA to form the basis of an Information Asset Register in the future to maintain information going forward.

Unanswered questions

Still not clear how much detail is expected for the article 30 requirement. We asked people to fill in at quite a high level for practical purposes and we think this is fine, but ICO haven't provided any guidance relating to the level of detail required.

Resources identified

The majority of working groups have managed to complete this work within normal resource. However, the research area is more problematic partly because of the scale and the fact that they don't have much of the necessary information to hand. The research ROPA work will require conversations with 1000's of researchers to understand the research position and we are trying to identify additional resource to support this work.

BE AWARE

The ICO have now published guidance and templates here: ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Other resources/notes

Need to review ALL data holdings, not just data captured after 25 May 2018.

Some commentators have recommended that institutions have a *data amnesty*.

3. Communicating privacy information: You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Case Study: A – Large university

Current situation

We have a fair processing notice in place, but are reviewing it for students and staff so it is much clearer what data is being collected and ensure we address the following heading:

- What personal data we hold
- The main purposes for processing the data (e.g. manage student wellbeing and health care, accommodation … etc.)
- Disclosure to third party and rational (e.g. HESA, SLC, external examiners, external auditors)
- Student's responsibilities
- Retention

Practical steps

Assessing all of the identify all the systems that are externally managed which contains students or staff data and have one privacy notice that covers all of the system and put this in the contract.

Creation of a register to capture all privacy notices.

Unanswered questions

Do we need a privacy notice for each system or can we cover it all by one privacy notice?

BE AWARE

The privacy notice must cover all the GDPR requirements, listed here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

It is not clear what is meant by the stated intention above to create one privacy notice and, *put this in the contract*. A privacy notice is a requirement that needs to be provided whatever the lawful basis for processing is.

Case Study: B – Large university

Current situation

Reviewing our privacy notice that is in place and addressing any areas of concerns.

A privacy notice form has been put together which is available in Appendix E.

4. Individuals' rights: You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Case Study: A – Large university

Current situation

Currently not compliant, we will ensure that we provide information to all individuals so that they understand their rights.

Practical steps

Reviewing our processes and the governance of the individual rights.

Designing and implementing the processes for data portability.

Planning system changes to enable (if appropriate) right to be forgotten.

Review back up procedures to ensure can re-enact rights to be forgotten and any consent changes.

Review developers access right, type of data in each environment taking into account the need to conserve system integration.

BE AWARE

The right to be forgotten is called the *right to erasure* in GDPR.

Case Study: B – Medium sized university

Current situation

Personal data is held in a variety of different centrally managed corporate systems, but also realistically, all over the institution in a set of locally devised and managed setups.

Currently requests related to data protection (e.g. subject access requests, requests for deletion etc.) generally find their way to our Secretariat, Registry or HR department. A semi-formal set of email exchanges between the *likely candidates* for system management is the current process for executing these requests.

Lots of discussion usually ensues regarding the ability or otherwise to comply (especially regarding record deletion) as policies are not clear and have not kept pace with the rapid expansion of *mechanised* record keeping.

Assessment of where the institution needs to be/nature of gap

A clear set of retention policies is clearly required, and this is being addressed through our actions under step 2 (Information You Hold) and also step 3 (communicating privacy information).

A clear set of processes that are (a) widely understood, (b) clearly signposted – so everyone knows where to go to start them and (c) reliably and consistently executed are required.

Practical steps

Our work in step 2 will identify a set of *data custodians* for different areas of our data processing activity. We will undertake a set of *Process Improvement/Process Creation* workshops with all the process champions, facilitated in a Lean/6 Sigma type approach.

Having designed a set of processes, it is likely we will build an electronic workflow for each to ensure that all cases are recorded, and that we can have assurance that they are not forgotten and acted upon as required.

5. Subject access requests: The ICO says, "You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information".

Case Study: A – Large university

Current situation

There is a legacy Subject Access Request (SAR) process in place which needs to be updated.

Assessment of where the institution needs to be/nature of the gap

The tighter timescales outlined by GDPR do present a challenge for us, in that often delays are caused by the complex nature of requests – i.e. locating where material might be held and liaising with staff to release it to us. Likewise, the volume of material can be problematic, as it all needs reviewing before it can be deemed safe for release. This is currently done by staff who, depending on the time of the year, may have other workload that needs balancing alongside this.

Practical steps

We are currently in the process of reviewing and updating our Subject Access Request (SAR) procedures. This will result in a documented process, which will be published online and will incorporate the tighter timescales, as outlined by GDPR. Some of the enhancements that we are looking to deliver focus on; clearer guidance to data subjects as to how to submit a request, as well as a defined retention schedule, which will result in all compiled data for a completed SAR being securely deleted after a set period of time.

Whilst we will of course aim to release all material according to the new timescales; in the event that the clock does beats us, then, as with the current timescales, we would administer a partial release (i.e. only that material that is deemed appropriate for release), along with a covering letter which would detail the planned release schedule for the remaining material. If the material has not been reviewed, then we can't release it as we would run in the risk of breaching a third parties' privacy.

BE AWARE

It is worth noting that delaying the release of material would be a technical breach of the GDPR requirement, unless the requests are many and complex, as per the GDPR Article 12(3), where in certain (presumably extreme) circumstances an extension of up to two further months may be available.

6. Lawful basis for processing personal data: The ICO says, "You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it."

Case Study: Large university

Current situation

Mapping each data processing and its purposes against the legal basis. This will be made available to students and staff, e.g.:

No	Specific purposes	Legal basis
1.	Management of enquiries with prospective students and communication of information about our services, events and activities	Consent to receive such communications

Assessment of where the institution needs to be/nature of the gap

Looking to claim Legitimate Interest in processing the data (e.g. reporting to HESA, data analytics).

Resources identified

D.P. Network https://www.dpnetwork.org.uk/gdpr-legal-grounds-processing-consent-legitimate-interests/

BE AWARE

It might be possible to claim *legitimate interest* as a lawful basis for processing necessary for purposes that fall outside the institution's *public task*, to be subject to the balancing exercise: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

7. Consent: The ICO says, "You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard."

Case Study: A – Large university

Current situation

Currently reviewing all of the consents that we already have.

Putting a consent register together to record it all in a central place.

The consent form will have the process and the unit to contact if want to withdraw the consent and form is GDPR compliant.

Practical steps

Think about the process of restoring from back up that consent is correctly replicated.

BE AWARE

A key part of a review of all existing consents will be to check whether consent is the appropriate lawful basis, or whether an alternative lawful basis can be identified.

Case Study: B – Large university

Current situation

Currently reviewing consent that is in place and reviewing any areas of concerns.

A consent guidance document has been put together which is available in Appendix D.

8. Children: The ICO says, "You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity."

Case Study: A – Small university teaching and research in diverse subject areas

Current situation

Understand all circumstances where children (under 16) come into contact with the University so that we can handle their data appropriately.

The University has a preschool which is open to children of staff and students of the University. Other circumstances where children come into contact with the University are mostly un-documented.

Assessment of where we need to be/nature of gap

None

Practical steps

Review and document processes of the preschool. Review and document student events like graduation, alumni events where children are likely to attend with parents or guardians. Review and document staff events like bring child to work days and social occasions for staff where children are likely to attend with parents or guardians. Review and document events where children (under 16) are likely to attend in their own right, e.g. apprenticeship days, events with local schools etc. Update privacy policies on the website to be in easy to understand language so that if children visit the website they can understand what is being done with their data.

Unanswered questions

How we are going to find the non-official events that children might attend? Where and when we need to record children's data?

Resources identified

None

9. Data breaches: The ICO says, "You should make sure you have the right procedures in place to detect, report and investigate a personal data breach."

Case Study: A – Large university

Current situation

In order to quickly move the GDPR requirements forward, the institution has re-used some of the existing processes in already in place for data breaches.

The institution has a simple Incident Response Team (IRT) which is responsible for security related breaches. This team is historic and has been setup pre GDPR and pre increased security attacks over the last few years.

The following organisational changes have been put in place:

- A Chief Information Security Officer (CISO) has been hired in 2015, and a small security team reporting to the CISO has been established over 2016/17.
- A Data Protection Officer (DPO) has been appointed in October 2017 to manage and implement GDPR.
- The concept of data stewards has been established and data stewards have been assigned to key data sets.
- A review of the data breach process has been done and GDPR requirements have been added to the existing IRT process.

When a breach occurs, the first point of call is the IRT. Whoever notices the breach will contact the IRT who will do a triage: if the breach does not involve personal data, they will deal with it. If the breach does involve personal data, the IRT will contact the DPO and if the DPO is on leave or off sick, Records management. The DPO will investigate and decide whether the ICO needs to be notified.

The Information Commissioner's Office (ICO) will be notified[2] if the breach involves one of the Special Categories of personal data outlined in Article 9 of the GDPR (e.g. health data, data relating to race or ethnicity...) or if the incident is likely to create a risk to the rights or freedoms of the data subjects.

The timescale is important: if an incident must be reported to the ICO, then that must happen within 72 after noticing the breach. Therefore, the system must run smoothly with everybody knowing their duties. An awareness campaign is going to have to happen to ensure that all staff members know that as soon as they notice a breach, they MUST get in touch with the IRT.

The IRT will receive additional training as to what constitutes personal data.

Assessment of where the institution needs to be/nature of gap

- Review IRT membership. The IRT team is a historic group, which needs to be reviewed, both regarding membership and responsibilities.
- There are certain data sets that have no data stewards.
- Most data sets and services had no GDPR impact review.

Practical steps

- Setup of a data steward group with lead by Enterprise Architecture.
- Review the IRT responsibilities and membership.

10. Data Protection by Design and Data Protection Impact Assessments: The ICO says, "GDPR makes privacy by design an express legal requirement and also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances."

Case Study: A – Large university

Current situation

University has a data privacy impact assessment (DPIA) process and document based on the old DPA rules, which should be filled out on the purchase of new software, service or significant changes to data processing. This process is owned by the governance directorate, not IT and is normally completed in collaboration with the data protection officer. The DPIA is not embedded into any institutional procurement process, or project management methodology so can often be an afterthought or forgotten completely. On more than one occasion the DPIA has been done after a new system has gone live and identified possible risks.

However, the GDPR makes privacy by design an express legal requirement and also makes *Privacy Impact Assessments* (PIAs) – also referred to as *Data Protection Impact Assessments* (DPIAs) mandatory in certain circumstances.

The current process also incorporates the data processing and confidentiality agreement between the University and the supplier.

2 *ICO Report a breach (**https://ico.org.uk/for-organisations/report-a-breach/**)*

Assessment of where the institution needs to be/nature of gap

DPIA should now be considered a legal requirement unless specifically discounted. The GDPR project is led by Governance who are updating the process and forms used to ensure they cover all areas required by GDPR. However, no work to embed in procurement or project management has been done yet and little consultation with IT has taken place.

Specific gaps:

- Acceptance into normal working practice. The biggest gap is probably with the acceptance of this processes into normal working practice, some of this might be addressed in step 1 (awareness).
- Embedding into procurement and project management. This is now very important given the procurements should have this built in as a mandatory step as the GDPR makes it a legal obligation to do a DPIA and have data protection by design.
- Management of DPIA outputs is essential as the documentary evidence could be crucial if there is a data protection issue. This could be part of a project management documentation or centrally managed by the institutions data protection officer.

Many existing systems should have retrospective DPIA done on them to identify risks and identify mitigation steps.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Resources identified

You should familiarise yourself with the guidance the ICO has produced on DPIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how DPIA can link to other organisational processes such as risk management and project management.

- Consider a DPIA to be a legal requirement for any new system or major system change.
- Have a DPIA process which is centrally owned and managed.
- Ensure the DPIA is embedded into procurement and project management.
- Ensure adequate documentation of assessment, risks identified and actions. In the event of a problem this may be of help when talking to the ICO.
- Contact ICO if risks appear significantly high with little possible mitigation.
- **https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf**
- **http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083**

11. Data Protection Officers : The ICO says, "You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer."

Case Study: A – Scotland

Practical steps

The IS Catalyst in Scotland, part of University and Colleges Shared Services, is currently looking to hire a number of named DPOS to be shared among member institutions that choose to join. This service will look to provide qualified DPOs to participating institutions – each institution have a share of a named DPO performing all the tasks of a DPO. Additional benefits of this service are; independence, resiliency, emergency cover and support, as well as sectoral expertise and providing the DPOs with a team of peers and line management with a view to fostering best practice and career development for the team. At present the IS Catalyst has received commitment from a number of institutions to begin recruitment for these roles, with a view to them being in place prior to May 2018.

Deliverables of the DPO role could include the following:

- Experience, expertise and legal guidance in Data Protection and GDPR.
- To review and update periodically each institution's data protection policy.
- Knowledge of case law/ICO decisions and dissemination of learnings, recommended actions and issue of guidance informed by this.
- To provide annual Data Protection Assessments and Compliance Reports to governing bodies/senior management teams.
- To achieve a fundamental understanding of the sector to ensure pragmatic, proportionate and workable guidance and support is delivered.
- Participation in operational meetings and offering advice on how regulations impact upon institutions.
- Training provided/offered to institutional staff both ongoing.
- Use of balance judgement. Deal with competing priorities/demands.
- Compliance/audit.
- Appropriately tailored solution for different institutions/circumstances.
- Central/single point of investigation (should a breach impact more than one member institution).
- Provide consistency of advice across institutions.
- Contextualised guidance in different functional areas within institutions (HR, Finance etc.).
- Available over phone for immediate questions/advice even if at a work day at another institution.
- Develop and support use of data protection assessments tools and templates (privacy assessment tools etc.).

Case Study: B – Large university

Current situation

The University already has an Information Governance Office and a Data Protection Officer based within the Academic Registry. The University has an Information Governance Working Group, chaired by the Academic Registrar.

Each school/department has a *Data Co-ordinator*, who acts on behalf of the Dean or Head of Service, to work towards GDPR compliance.

Assessment of where the institution needs to be/nature of gap

There needs to be more expertise on the GDPR throughout the institution in order to work consistently and successfully towards compliance.

Practical steps

A new member of staff has been appointed by the Chief Operating Officer for a period of six months to work throughout the institution to ensure that the University reaches a reasonable position regarding GDPR compliance. Not only is the appointee very knowledgeable on GDPR but they have many years' experience as a senior academic administrator in a number of universities – they therefore not only understand the policy landscape but importantly, the context in which we all work.

The Chief Operating Officer has recently written to senior members of staff to remind them of responsibilities under the new General Data Protection Regulation, and to share a link to the Information Commissioner's Office.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Initial deliverables of the new role include the following:

- First task is to work on a risk map of GDPR compliance based on the datasets we are holding across all academic departments and general administration.
- Identify where the most severe risks are and then seek to work with units to mitigate those risks.
- Whilst the postholder is there to work in partnership with existing staff to help find solutions to problems rather than simply flag the policy, inevitably the responsibility for most of the mitigation will rest with the Data Coordinator and all colleagues.

Resources identified

This new post is 0.7 FTE for a period of six months.

Case Study: C – Medium sized university

Current situation

No DPO is currently in place.

Practical steps

Currently recruiting for DPO – see Appendix B for a job description.

Case Study: D – Large university

Current situation

The University already has hired a Data Protection Officer based within Planning and Governance. The University has an Information Security Working Group, chaired by the Information Security Officer.

Assessment of where the institution needs to be/nature of gap

The University hired a DPO in Autumn 2017 and is now working on ensuring GDPR compliance.

Practical steps

The DPO is to work throughout the institution to ensure that the University reaches a reasonable position regarding GDPR compliance.

Resources identified

This new post and is a full FTE post.

A full Job Description can be found at Appendix C.

12. International: The ICO states that,"If your organisation operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this".

Case Study: A – Large university

Current situation

We have a small number of high level conversations about this, but as of yet have not begun to think about it in the context of the supervisory authority.

Practical Steps

One of the key objectives of another group that I am working with (the Data Coordinators Group), will be to begin the process of undertaking a data review. This will provide an opportunity for Schools/Services to identify what data they process (and in doing so could identify any scenarios in which they operate internationally).

Case Study: B – Large university

Current situation

- Mapping the data with the institution and overseas sites.
- Putting corporate standards the way IT and security are set up overseas, e.g. ensure all devices are purchased in the UK and encrypted, then shipped across.
- Putting in place with partner (academic partnership) a data transfer agreement.
- May use performance of the contract or legitimate interest as a lawful basis for processing.

Unanswered questions

- For staff, can we rely on legitimate interest or performance of the contract for processing some of their data in offices overseas which provide administrative support or do we actually need to seek consent by each member of staff?

Resources Identified

- Legal briefing note on cross-border data transfers in light of GDPR
  https://www.lexology.com/library/detail.aspx?g=6f888c07-df51-42a5-abaa-5ef223a09bf9

BE AWARE

The *unanswered question* posed above conflates the issue of lawful basis for processing, and the restrictions on the transfer of data outside the European Union.

***Legitimate interest* and *contract* are two of the possible lawful bases for processing (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing). Lawful bases for processing do not give data controllers the right to undertake international data transfers.**

The ICO provide guidance on the rules around international transfers https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers.

There are a number of permissible ways to legally transfer data outside the EU. One of those are the derogations that permit international transfer in certain specific situation – but it must be noted that these derogations cannot be used where the personal data processing is being carried out using the public task as a lawful basis for processing.

5 The ICO view – answers to frequently asked questions

On 10 January 2018, the UCISA CISG Committee met with Victoria Cetinkaya, Senior Policy Officer – Policy and Engagement (Public Sector) at the ICO to discuss GDPR preparation and compliance at UK universities and colleges.

In addition to an excellent training tip (Victoria told us that the ICO have data security awareness notices on the back of the toilet doors!), the following questions and answers were discussed during the meeting and are provided to assist institutions in their own GDPR preparations.

1. Is 25 May 2018 a drop dead date?

The 25 May 2018 is not a cliff edge.

As the Information Commissioner has said, *"GDPR preparation doesn't end on 25 May 2018 – it requires ongoing effort. It's an evolutionary process for organisations – 25 May is the date the legislation takes effect but no business stands still. You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018."*[3]

If there is a breach after 25 May, the ICO will have to act and apply the law as it stands at that time. However, the ICO are clear to point out that efforts clearly being taken in an attempt to comply will help mitigate actions/penalties. The Information Commissioner has stated in her blog, *"It's true we'll have the power to impose fines much bigger than the £500,000 limit the DPA allows us. It's also true that companies are fearful of the maximum £17 million or 4% of turnover allowed under the new law.*

But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm.

The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick."[4] There is no need to panic, ICO will look to see if an institution has been logical and systematic in their decision and approach.

2. Is it a reasonable idea to undertake a *data amnesty* in institutions in order to discover what personal data is being processed locally (perhaps *under the radar* of central control)?

A data amnesty is a really good idea. There is a high likelihood that individuals have signed up to *funky online systems* (often free) for the processing of personal data without the knowledge of anyone else in the institution. This is a potentially useful tactic to discover this activity and encourage people to declare it.

ICO is fully aware on the challenge that HEI's have especially when it comes to research. Indeed, having performed mini audits (with volunteers); it is clear that central admin is well understood, but often the academic side is messy and complex.

3. How will the ICO interpret who is the data controller in the situation where an academic is undertaking a data collection activity but where the academic in question has a *portfolio career* and is working with multiple organisations?

It is important that the data controller for any given processing purpose is made clear. It is, therefore, important for institutions to be able to demonstrate that they have appropriate training and processes in place to show that they have made reasonable efforts to ensure academic staff do not undertake new personal data processing activities without undertaking due diligence.

Ultimately, however, if any member of staff undertakes personal data processing activities under the banner of their employer, then they are making that employer a legally liable data controller. It is, therefore, imperative for staff to be under no illusion that this is an action that will not be tolerated.

In the event that some data processing activity is undertaken without the knowledge of an institution, by a rogue employee, acting against the clear instructions of their employer, it is likely to improve the outcome for the institution if they can prove that all reasonable steps had been taken.

3 *Quote from Elizabeth Denham's blog 22 December 2017:* **https://iconewsblog.org.uk/2017/12/22/gdpr-is-not-y2k/**

4 *Quote from Elizabeth Denham's blog 9 August 2017:* **https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/**

4. How do we protect ourselves if our supplier has a data breach?

Currently (under 1998 DPA), if a supplier (data processor) makes a terrible mistake resulting in a data breach, the institution (data controller) remains responsible. Under GDPR, data processors (the supplier) can also be considered legally responsible. This does not, however, absolve the controller of responsibility. Therefore, HEIs ought to cover themselves by ensuring contracts covers data breach. Before entering into a contract with a supplier, we need to ensure that we have performed due diligence checks and we have taken all of the precaution when exchanging data, e.g. encryptions etc.

When sharing data internationally (outside the European Economic Area – EEA) one way is to use specific EU contract clauses that can be added to the contracts (although these are yet to be drafted). See question 6.

5. Would it be sensible or even required to test staff following GDPR awareness training, and should there be the concept of a pass mark?

Training with test and passmark would assist in evidencing compliance. GDPR training is important. Staff should be trained. Good practise would be that mandatory training should be undertaken at least once a year.

6. Is it possible to use data processors outside the European Economic Area (EEA). For example, a *follow the sun* support service based in the southern hemisphere?

It is possible to remain GDPR compliant while exporting data outside EEA, but care needs to be taken to do so correctly. There will be approved contract clauses to add to agreements to protect data outside EEA. Such clauses have not yet been drafted for GDPR but it is likely either the European Commission or the ICO will do so at some point.

It is recommended that data processing activities outside the EEA are made clear by a data controller within the privacy notice.

Brexit is likely to have an impact on data transfer abroad, but this is not yet quantifiable.

7. There has been much debate about the definition of universities as public authorities (especially amongst institutional fundraisers who are concerned about the use of *legitimate interests* as a lawful basis for processing). Is this definition black and white?

The ICO have stated *"Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances [...]. For example, a university might rely on public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes."*[5]

It is expected that a Government amendment to the Data Protection Bill will clarify that institutions are only a public authority when carrying out public tasks. However, if this amendment is not passed, the ICO are still clear that they will use their interpretation above.

This will, therefore, allow the use of *legitimate interests* as a lawful basis for processing (on non *public task* activities). It is important to note, however, that demonstrating *legitimate interests* is not easy, and consists of four steps:

- make the argument that the processing is legitimate interests.
- make the argument that the processing is necessary.
- make the argument that the processing does not adversely impact the data subject's privacy rights – it is reasonable/fair.
- tell them you're doing it.

8. Is it necessary to explicitly name data processors in privacy notices?

Technically speaking, you only need to name categories of recipients of data. It would be good practise to list them somewhere and link to it.

5 **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/**

9. How should we structure privacy notices for presentation to groups of individuals whose interactions with our institution is likely to develop over time?

For example, people who enquire, then apply, then enrol, then actively study will be asked for increasing amounts of personal data as the relationship develops. Should we provide one catch all privacy notice (which would be long and potentially confusing for those who simply enquire, and never apply or enrol) or several separate notices at each stage where further information is required (which addresses the confusion for enquirers, but potentially adds confusion for those who do go on to study, as it may not be clear to them or the institution which privacy notice(s) are *current* and which have been superseded.

The overwhelming requirement for privacy notices is for the information they impart to be clear and accurate and understandable by the data subject. The data subject should be in no doubt as to what personal data they are providing, for what purpose and for how long it will be retained by the data controller.

Specific guidance is provided by the ICO on what needs to be included (**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed**).

It is reasonable to *layer* privacy notices – but make it clear which part relates to the data that the data subject is providing *now* in any given transaction.

10. Can we incorporate consent into privacy notices?

Yes – but it must be clear, so that consent requests are separate from other terms and conditions to the extent that individuals can see what they have a choice in and what they do not.

11. How should we handle situations where we have received data from someone or some organisation other than the data subject themselves (e.g. applicants via UCAS, emergency contacts from staff and students)?

Article 14 states that data controllers don't have to contact the data subject with a privacy notice if it would require disproportionate effort, although this is in particular noted to apply where processing personal data for archiving in the public interests, research or statistical purposes.

However, it is difficult to prove unreasonable effort.

For example, when someone applies for a job they usually supply the contact details of one or more data subjects as *referees*. It is hard to argue that it would require unreasonable effort to contact these referees to provide a privacy notice as it could easily be done by email. In this instance, it would be more appropriate to amend the recruitment process and only gather referee information when we actually required it to make the query and not at the time of the application. The referee information should then be deleted once the recruitment process is complete.

12. Should we gather consent for historic records?

All records processed after 25 May need to be processed in GDPR compliant way. If processing records on basis of consent, and consent was obtained previously, this will need to be reviewed to ensure that the consent obtained meets the GDPR standard of consent. If it does not, that consent will have to be refreshed.

For some processing, it may be that consent is not the appropriate lawful basis, in which case an appropriate lawful basis should be identified and recorded, and privacy notices updated accordingly.

For example:

- The lawful basis for *holding* Alumni data for the purposes of keeping them informed of their former universities news and events may be legitimate interests.
- The Lawful basis for *contacting* Alumni by telephone and email to request donations for fundraising initiatives may be consent. In addition the Privacy and Electronic Communication Regulations (PECR – see **https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/**) require consent for this type of activity.

13. Is it only where consent is relied on as the lawful basis for processing, that we need to clarify how we seek and record it?

It is only necessary to gain and record consent where this is the lawful basis for processing.

14. Should we attempt to keeping records for an individual up to date where they are separate (e.g. separate same person is recorded as a referee for multiple applicants)?

The requirement is to keep personal data up to date *where necessary* (Article 5(1)(d). The fact that a referee's details were accurate at the time the reference was obtained is the important one here. Consideration should also be given to how long this data should be retained anyway.

15. Data Portability – what does it mean to our sector?

One of the new GDPR rights is the right to data portability. This requires the data controller to provide the data subject with a copy of their data in a *structured, commonly used and machine readable form*. This could be for instance a simple CSV file or other standard format such as XML. You may also be asked to pass this data directly to another organisation, but you don't need to create interfaces to do this if this is technically complex to put in place.

This right only applies where the lawful basis relied upon is consent, or contract, and then only to data provided by the data subject, processed by automated means. See here: **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability**.

16. Is it ok to keep logs and backups that may contain *deleted* data?

There are no specific requirements. However, the ICO has previously described an approach under the DPA98 focused upon whether data is beyond use (see here: **https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf**)

Specifically four important safeguards for *putting data out of use* are described in the above guidance:

1. The controller is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
2. It does not give any other organisation access to the personal data;
3. It surrounds the personal data with appropriate technical and organisational security;
4. It commits to permanent deletion of the information if, or when, this becomes possible.

17. Is it necessary to encrypt databases at rest?

DPA states same as GDPR: encryption could be appropriate, but it is not a requirement. Factors are: risk of data loss, data sensitivity, cost to implement. Use risk based approach. This might help demonstrate compliance, but is not explicitly required, and an institution might be able to argue is not proportionate.

18. Is it acceptable for *real* data to be held in non-production systems (e.g. Dev and Test environments)?

You should try to anonymise data in these systems where possible. If you need to hold personal data on non-production environments, lawful basis can be used. It is not about where to hold the data, but the reason why you need to hold it for and what functionally needs copies of *real* data. Ensure it is well managed.

Environment used for training needs to be anonymised.

19. When should we carry out Data Privacy Impact Assessments (DPIA)?

A DPIA is required whenever you are implementing new technology for processing personal data, or undertaking processing of high risk or special category data. However, the ICO would recommend we do a risk assessment and consider whether a DPIA is required whenever we implement new or changed systems and processes.

DPIA documents ought to be stored and easily accessed when audited.

20. Do you have any advice for mobile devices?

Use common sense: mobile devices should be encrypted, secure and not contain any information they don't need to (to minimise risk of loss). The institution should have a clear policy in place, especially around BYOD.

21. Any other top tips?

a. As a basic rule: don't panic. GDPR is DPA (Data Protection Act) 2.0 in many ways. If we have had good DPA cover GDPR is not a massive step.

b. Focus on the data, the data drives who is responsible. Whoever is the data controller (data steward) needs to ensure their data follows the GDPR rules. Map out what personal data we have.

c. Remember that the law is focussed around *purposes for processing* personal data. You do not establish a right to *hold data for individual X to do whatever you please with* – you establish a basis to hold a person's data for a given purpose. If you need to use that person's data for another purpose, you need to establish that lawful basis (and communicate it appropriately) in addition.

d. Privacy notices are about transparency – what we do, why we do it, what you can do about it if you don't like it – not necessarily consent. You could combine consent notifications within them – but that is not the intended purpose and this might serve to confuse the data subject (which is counter productive).

e. Record for GDPR that has been agreed and why you made what decision. Share this decision with the DPO for approval and so that you can demonstrate appropriate consideration was given.

f. Under DPA the data controller is fully responsible for everything. Under GDPR data processors have responsible as well. This means that SaaS solutions will have data processing liability. If the data controller has the SLA and contract in place ensuring proof that data processing is covered the data processor will be responsible and the university could sue the data processor (SaaS provider). Data processor contracts have some specific requirements under GDPR – see here: **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts**.

g. Think about email retention. Lots of personal data resides in inboxes. To address this some corporate email system deletes all messages automatically after six months. If within six months of receipt you haven't saved the correspondence in an appropriate corporate filing system (with appropriate retention policy) – it is deleted.

6 Other considerations for GDPR preparation from an IT perspective

The following points fall outside the ICO 12 steps, but are areas of consideration for those charged with the management and support of institutional IT.

- Retention of data in systems – policy and how systems can implement this (we need to keep a record of the IDs of records that have been deleted because we need to be able to re-delete them if we restore a backup).
- SaaS, Cloud services etc. – need to ensure that all frameworks templates include GDPR related questions. Need to do this now, rather than waiting until May 2018!
- Existing IT contracts need to be reviewed to ensure GDPR compliance.
- GDPR compliance questions need to be built into all tender documents/frameworks.
- Audit user access rights. Regular review and remove access of data to those who don't need it.
- Fine grained access control – reduce access to student data by department/school.
- Conflict of interest between business objectives (e.g. fundraising) and GDPR legislation. IT can enforce system rules, but these need to be decided by the business.

7 Appendices

Appendix A – example staff awareness email

To: All staff

1. Report data loss and fraudulent activity

If you suspect data has been revealed to third parties – you must report it immediately to its@xxx.ac.uk

If you suspect your account details have been compromised (whether you believe the account has been accessed or not) – you must report it immediately to its@xxx.ac.uk.

2. Protect your user account

Your user account provides you with access to a range of personal data that allows you to perform your role. Both you as an individual, and XXX University as a whole are legally bound to protect this data. Never, ever, on any account, should you share your user credentials with anyone.

Do not reveal your password to anyone.

Only use your password to log into services that you are sure are provided by XXX University. If you are in any doubt, check it first by contacting its@xxx.ac.uk.

Ensure your password(s) are strong (are at least 8 characters in length, and contain a mixture of letters and numbers as a minimum).

3. Phishing emails

Sadly, the simplest way for fraudsters to obtain personal information is to simply pose as a trusted organisation, and ask for it. If you ask enough people a few will respond – and it is very easy when emailing to ask a lot of people very quickly, at zero cost.

On a daily basis, emails are received by college staff and students asking them to visit third party (fraudulent) sites and enter their usernames and passwords.

Examples of emails received by XXX University staff and students include those purporting to come from IT Services regarding mail quotas being exceeded, or from the Registry offering cash bursaries – in both cases the objective of the fraudster is to take the recipient to a fraudulent website, often made to look like a XXX University site, and ask them to provide username, password and other information.

There are a number of *tell tale signs* in fraudulent messages including the following:

A. The message is offering something that is too good to be true.

B. The message is unexpected or out of context.

C. The message has not been sent from who it purports to come from. Often compromised accounts (from previous phishing victims) are used to send such emails.

D. The site you are directed to does not belong to the organisation from whom the message is meant to originate – hovering over the link will show where the site will take you. (You don't need to click on it.)

E. The message is anonymous, without person or contact details.

Other signs that you should treat the message with extreme caution, or disregard it, are:

F. The link is asking for personal information and bank details.

G. If the timing of the message is suspicious. Phishing emails are often sent with immediate deadlines, often at times when you would find it difficult to confirm their veracity.

And finally, but more obscure:

H. If you are able to view the message *headers*, you can see details of the mail system from where the message originated.

4. Bulk emailing

A. Ideally emails sent to groups of recipients will originate from our corporate systems or be sent to distribution lists.

B. Should you have to send emails from outside of a corporate system, and an appropriate distribution list does not exist, email should be sent using Blind Carbon Copy (bcc) functionality.
This is to protect the privacy of the recipient's email address. It also avoids a user intentionally or unintentionally using the *Reply to All* option which would result in a second bulk email resulting in additional replies causing annoyance to users. Provide an instition contact for the recipient to check if the message is genuine.

C. Bulk email should be sent from a verifiable institutional email account.
Bulk email should not be sent from third party email accounts that provide no measure of authenticity. All institutional bulk emails must be sent from xxx.ac.uk email accounts.

D. Provide a named institutional contact for the recipient to check if the email message is genuine.
It is important to note that any email address can be impersonated by someone with malicious intent. If an email appears suspicious, the sender should be contacted to validate authenticity. You should send the email from a named person in a team and offer a telephone number for follow up queries.

E. Bulk email should have a Subject that clearly defines the purpose of the email.
Ambiguous subject lines make it difficult to differentiate between legitimate emails and spam or phishing emails. As a result, an email may be inadvertently ignored or deleted.

F. Take care in composing and checking the accuracy of the message content and recipient list.
Make sure the message you are sending is going to apply to the majority of those on the recipients list. Irrelevant message can be disproportionately irritating to their recipients. Double check the contents of the message as any errors will be repeated many times and cause annoyance to users. Also, keep the message short, perhaps a page at the most.

G. Provide an opt out option for Bulk Email relating to marketing information.
If appropriate provide a mechanism for people to opt out of receiving any further communication. Note that in our student record system we do flag students who have opted out of marketing communication. They can do so by logging on at www.xxx.ac.uk/myxxx and clicking on the *My communication preferences* under *Manage my profile* to change their preferences.

H. Respect the express wishes of the recipients with regard to marketing mailing.
We are legally bound not to send unsolicited marketing messaging to those who have expressly requested not to receive it. Therefore, you should ensure that unless there is a clear need to send a message (it contains information required to allow a student to study, or colleague to work) that you should not send it to anyone who has opted out of receiving marketing information. That means in practice:

- Do not use old *stale* lists of email addresses to send marketing messages to – always acquire a fresh list excluding those who have opted out of marketing communications.
- Do not use a list sourced from locally held records – you will not be able to ensure that those who have opted out in our corporate data are excluded, and you must.

I. Avoid sending attachments in bulk email.
Email attachments are a common tool for propagating computer viruses. As a result, some users are hesitant to open unexpected attachments. Senders of bulk email should consider posting files to a xxx hosted website and then providing instructions in the email on how to download the file. This provides some measure of authenticity.

J. Avoid hyperlinks to third party websites.
Spam and phishing emails often include hyperlinks to malicious websites. As a result, recipients may be hesitant to click on a hyperlink even in an email that appears legitimate. Similar to attachments, posting third-party hyperlinks to a university hosted website provides some measure of authenticity.

5. Obtaining, storing and handling personal data

When personal data is requested from individuals organisations have a legal duty to:

- Explain why the data is required.
- Explain how it will be held, used and disposed of.
- Hold it securely, only granting access as necessary.

Data that is provided by prospective students, applicants and students, via our corporate systems, is done so after terms and conditions, which state the above have been acknowledged.

A. Ideally you should not be holding local records of personally identifiable information on any individuals.

B. Please consider whether it is necessary to hold personal data outside our corporate systems. If it is necessary then you should ensure you make use of the encryption and password protection facilities available to you (e.g. Word and Excel documents can be password protected).

C. You should not setup systems for collecting or storing personal information on behalf of the institution, either in locally developed infrastructure, or cloud hosted online services (e.g. Survey Monkey, Google Forms, Type Form).

D. You should not transfer data to any third party without first checking that there is an appropriate agreement in place between xxx and the third party.

E. Regularly check for and delete files that contain personal information that are no longer required.

Above all else, if you are unsure about anything regarding the above, or in any other respect of data protection, please contact its@xxx.ac.uk in the first instance for advice and guidance.

BE AWARE

Point 4.H. of this email regarding email communications appears to be overly lax. The Privacy and Electronic Communications Regulations (PECR) already requires that email marketing only be carried out with consent. It's not enough that a recipient has not opted out, they must have actively opted in.

Appendix B – example DPO job description

Job description

JOB TITLE:	Head of Data Protection and Information Compliance
SCHOOL/ DEPARTMENT:	College Secretariat
REPORTS TO:	Deputy College Secretary (Governance)
SUPERVISES:	None
INDICATIVE GRADE:	

Purpose of the job

To be accountable for the College's strategic approach to data protection across all of its academic and business operations, and to ensure compliance with relevant data protection legislation and regulations. The post holder will be responsible for ensuring that the College is compliant with the EU General Data Protection Regulations and the UK Data Protection Act, as well as Freedom of Information and Records Management requirements, by developing and implementing an awareness and compliance programme, working with colleagues across the College.

Main duties of the job holder

Develop and implement procedures to facilitate and ensure compliance with data protection law and regulation, initially via a scheduled compliance programme to enable the College to meet the requirements of the General Data Protection Regulations from May 2018.

Perform the responsibilities and functions of Data Protection Officer and of Freedom of Information Officer for the College.

Prepare and deliver information on data protection legislation, its impact on College operations and the measures to be implemented in response, to colleagues at all levels including the College's senior management and to teams in the Schools and central Professional Services.

Draft and communicate Data Protection, Freedom of Information and Records Management policies and procedures for the College.

Work proactively with Schools and services to provide effective advice and guidance to colleagues on the steps to be taken to identify and address areas of data protection risk and comply with data protection legislation.

Manage procedures for handling and responding to Freedom of Information requests, subject data access requests, complaints, queries and information requests from data subjects and Environmental Information requests.

Maintain accurate, comprehensive and authoritative records of all data processing activities undertaken by, or on behalf of the College.

Develop a monitoring framework to support the College's obligations and compliance with data protection and Freedom of Information law and regulations, including appropriate management information to report on compliance.

Plan and execute a schedule of Data Protection audits and work effectively with colleagues to implement their recommendations.

Advise on when Privacy Impact Assessments are necessary and conduct these assessments as appropriate.

Assess and take action in response to actual and potential data protection related incidents, including data breaches, by ensuring external bodies are notified as appropriate and engaging with colleagues to resolve issues and prevent further incidents.

Work with relevant staff groups, including the Directors and Managers in the Schools and central Professional Services, to ensure data protection compliance and the concept of privacy by design is embedded into all systems, policies and processes.

Establish effective networks which promote and support a data protection culture within the College, good practice for data processing and protection, and strong working relationships with the staff involved.

Develop and lead a training and awareness programme to promote good practice for data processing and protection among staff.

Work with the Information Security Manager to support improvements to data security policy and practice.

Establish and participate in networks with those responsible for data protection and information compliance in other HE institutions and outside the HE sector.

Working relationships and contacts

Provides authoritative advice to:

- the College Senior Management Team including the College Data Controller;
- the Directors and Managers of operations in Schools and central professional services.

Works with staff at all levels to ensure understanding of the requirements of data protection and freedom of information law.

Dimensions

This post has responsibility for planning, delivering and developing activities to ensure compliance with external legal obligations. It requires knowledge of current external requirements combined with the ability to apply high level problem solving, risk assessment and communication skills to work with Directors, managers and teams to ensure the College's operational activities are both effective and compliant with the law.

General responsibilities

These are standard to all College job descriptions.

- To adhere to the College's Equal Opportunities policy in all activities, and to actively promote equality of opportunity wherever possible.
- To be responsible for your own health and safety and that of your colleagues, in accordance with the Health and Safety at Work Act (1974) and relevant EC directives.
- To work in accordance with the Data Protection Act and to ensure that all new systems are reported to your Data Protection Controller.
- To undertake such other duties as may be reasonably expected.
- To provide a healthy and comfortable working environment.

Person specification

JOB TITLE:	Head of Data Protection and Information Compliance		
DEPARTMENT:	**College Secretariat**		
ATTRIBUTES	**ESSENTIAL CRITERIA**	**DESIRABLE CRITERIA**	**METHOD OF ASSESSMENT**
Knowledge technical/ Work based skills	In depth understanding of current UK data protection requirements, strong understanding of the EU General Data Protection Regulations and the UK Data Protection Bill and subsequent Act, including the impact of this on the UK Higher Education sector. Understanding of systems and processes involved in gathering, storing, transferring and collecting data. Solid technical knowledge of data processing, IT security arrangements and Big Data requirements. Knowledge of the Freedom of Information Act 2000 and the processes required to comply.	Understanding and knowledge of Information Security and its supporting processes. Understanding and knowledge of Records Management and its supporting processes. Understanding and knowledge of Information Assurance and its supporting processes. Understanding and knowledge of Information Risk Management and its supporting processes. Understanding and knowledge of Information Governance and its supporting processes.	Application Interview Presentation Test
General skills/ attributes	Ability to communicate effectively with colleagues at all levels. Ability to plan own workload in accordance with the requirements of the schedule to ensure personal deadlines are met. An executive presence and expert communication skills to enable engagement with School leadership at all levels.		Application Interview Presentation Test
Experience	Extensive experience of Data Protection compliance operating at a senior level. Practical experience in the area of data protection and freedom of information compliance in the UK. Practical experience of Incident Management in relation to data protection and freedom of information. Project management and organisational skills including the ability to run multiple initiatives in parallel.	Experience in the legal profession advising on data protection issues. Experience of working in higher education. Experience of advising on data sharing arrangements, particularly collaborations and third party engagements.	Application Interview Presentation Test
Qualifications	Data Protection Practitioner Certificate	Information Security qualification	Application Interview Presentation Test

Appendix C – example DPO job description

Job description

Data Protection Officer

Job Title: Data Protection Officer

Department Name: Governance and Strategic Planning

This is an exciting opportunity to become the Data Protection Officer of one of the best Universities in the world as we move to implement our new Strategic Plan. Our plan recognises the need to influence globally, contribute locally, to advance our partnerships with Industry and to progress work on Digital Transformation and Data. A specialist in the field of data protection, the post-holder will support the delivery of the University's business and strategic plans by advising on business focused solutions as we respond to the changes in regulation in this area and drive forward our strategic aspirations.

The post-holder is expected to provide leadership to colleagues across the University working collaboratively with colleagues in Information Security, Legal Services and Records Management. The successful candidate, in addition to specialist expertise in data protection, will be an effective communicator with strong influencing skills.

1. Job details

Job title: Data Protection Officer

School/Support Department: Governance & Strategic Planning

Line manager: Deputy Secretary, Strategic Planning

2. Job purpose

The Data Protection Officer is the University's specialist adviser on Information Governance legislation supporting organisational compliance with data protection, freedom of information and other related legislation. The role holder is accountable for governance of personal data across the institution and will be key contact for external regulators in this area.

3. Main responsibilities

1. The role holder holds the statutory position of Data Protection Officer for the University and is the primary liaison point with OISC and ICO. The Data Protection Officer is responsible for ensuring that policies and procedures for protection and use of personal data of University staff, students, partners, collaborators and others are in place across the University and for the reporting of breaches to the ICO. (65%).

Initial priorities will include:

- Establishment and leadership of the University's implementation of its obligations under the General Data Protection Regulations (GDPR) and ongoing compliance; and
- Addressing actions to be taken as a result of the Etherington review of charitable fundraising.

2. Working closely with the Chief Information Security Officer (who has responsibility of the overall security of University information), Director of Legal Services and Convenor of Risk Management Committee to ensure the University's information risk levels in relation to personal data are appropriately controlled. (20%)
3. Writing and revising University policies and guidelines in relation to information governance of personal data, reviewing regularly and making any changes necessary as a result of new or changing legislation, or changes to the University's information risk profile. (10%)
4. Planning and developing responses to legislative change, such as additional training and guidance, typically over a timeframe of several months and with impact across the whole institution. (5%)

4. Planning and organising

- Horizon scanning to ensure that the University is aware of, and prepared for, any upcoming legislative changes or legal precedents that could have an impact.
- Planning and undertaking work in the light of the immediate and medium/long term implications of changes in information legislation and the University environment so far as they affect personal data.
- Planning personal workload and resources around responses that are required within legal deadlines under data protection, freedom of information and other related legislation.

5. Problem solving

- The post holder finds practical, business focussed, solutions in relation to complex scenarios to ensure the University is compliant with a variety of pieces of information legislation (that often overlap) where there is often a lack of precedent and competing requirements.
- Risk/benefit decisions are sometimes required to fit specific circumstances and ensure the University is able to function effectively, taking into account any impact on the University's reputation.
- Pragmatic and strategic thinking is needed to avoid creating additional burdens for staff from across the institution.
- Using qualifications, professional experience and reference to a wide variety of sources, including ICO guidance and ever evolving case law (that often provides conflicting evidence), to arrive at a conclusion and advise on possible courses of action.
- Proactively identify information risks/issues and propose solutions.

6. Decision making

- Making decisions about the best approach in current *grey areas* of information governance and compliance, to ensure the University and its stakeholders are appropriately protected. Such decisions often involve consideration of the legal and reputational risks for the University.
- Providing advice and solutions to staff in relation to Data Protection and Freedom of Information issues, particularly with regard to planned procedural and technical developments e.g. new information storage systems or major and novel new projects.

7. Key contacts/relationships

- Influence and engagement with senior managers, stakeholders and University committees (e.g. IT Committee, Central Management Group, College Registrars) is key to ensure that information governance is afforded the necessary importance at executive level and is embedded as a core function of a large organisation with significant multi-sector and international collaborations and joint ventures.
- The post holder does not have line management responsibilities but will work within a virtual team drawing on the input of Information Security, Legal and Records Management staff. The operational management of Freedom of Information requests, Environmental Information Regulation requests, Subject Access Requests and general enquiries is located in Records Management while Information Security incidents are primarily the responsibility of Information Services Group. It is anticipated that the post holder will provide expert support and advice to other parts of the virtual team; for instance in reviewing FoI responses which have resulted in a complaint from the requester.

8. Knowledge, skills and experience needed

- The post holder should hold nationally recognised professional qualifications in Data Protection, Freedom of Information and information security principles and have a number of years' experience in information rights management.
- Strong influencing and communication skills are essential for this role.

Qualifications/training

Essential:

Information governance/data protection qualification

Relevant undergraduate degree or equivalent experience

Experience:

Essential:
Substantial experience leading data protection work in a large/complex organisation.

Desirable:
Experience of data protection in a Higher Education environment.

Knowledge, skills and competencies

Essential:
Expert understanding of data protection legislation including the GDPR.
Strong influencing and communication skills including with senior colleagues.
Project leadership and implementation skills.
Ability to produce business focused solutions not simply compliance implementation.

Desirable:

Understanding of the status of Universities as public authorities.

Personal attributes

Essential:

Strong attention to detail, confident self direction of work planning. Confident engagement with colleagues and senior staff.

9. Dimensions

The post holder, as the University's Data Protection Officer, is responsible for ensuring that the Senior Management of the University are aware of the institution's responsibilities and the significant risks associated with data protection legislation. The post holder will be expected to work in a virtual team with our Records Management, Legal Services and Information Security team to ensure that expert advice results in business focused solutions which can then be implemented by local areas/functions.

Appendix D – example of a Consent Guidance document

Guidance – how and when to use consent

Audience and Purpose

This guidance is for any member of University staff intending to use consent as the legal basis for processing personal data. This guidance should be read in conjunction with the main guidance *How to determine the legal basis for processing personal data*.

- How to determine the legal basis for processing personal data.

You will need to use this guidance when intending to use personal data and none of the other legal bases (such as contractual obligation or performing a task in the public interest) are applicable.

Definitions

- **Personal data**
- **Sensitive personal data**
- **Data subject**
- **Processing**
- **Data processor**
- **Data controller**

The basic rules of consent

The requirements for consent are stringent to protect the rights of data subjects. Thus, consent must be verifiable, specific, freely given, informed, and withdrawable at any time.

Consent is inappropriate if data subjects do not have a genuine choice over how data about them are being used. This would be the case if you would still process the data under a different legal basis if consent were refused or withdrawn. In these circumstances consent would be misleading and inherently unfair.

Active opt in

Under data protection legislation, consent must be an unambiguous indication, which means that consent must be either a statement or an affirmative action. Consent must be more than just a confirmation that the person has read terms and conditions – there must be a clear signal that they agree. Clear affirmative action means someone must take deliberate action to opt in, however this does not necessarily have to be through ticking an opt in box. Other methods might include signing a consent statement, oral communication, a binary choice presented with equal prominence or switching technical settings away from the default.

The key point is that all consent must be opt in – there is no such thing as *opt out consent*. Failure to opt out is not consent and you may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions.

Implied consent, however, is still possible in circumstances where the individual has shown consent through an action. Again, mere silence or inactivity are insufficient.

For special categories of sensitive personal data, consent must always be in writing.

> **Example:**
> *"Would all those who want to be in the conference photo please make their way onto the stage. We'll publish the photo on the conference website."*

This would suffice for consent as conference participants have shown their consent through an action, i.e. going onto the stage.

At recruitment fairs or the University Open Day, potential applicants consent to receiving information material by providing their email address.

Freely given

Freely given consent means that people have a genuine choice and control over how the data controller uses their data. This means that the data subject must be able to refuse to give consent without any detriment, and must be able to withdraw consent easily at any time. There must be no imbalance in the relationship between data controller and data subject and consent must not be a prerequisite for provision of a service.

Imbalance of power

Consent will be inappropriate if there is a clear imbalance of power between data controller and data subject. This is because consent cannot be considered to be freely given if data subjects feel they have no choice but to agree to the data processing. For example, data subjects may depend on a service or fear adverse consequences if they do not consent.

Condition of service

If a data controller arranges for a service to be dependent on the data subject consenting to data processing, then consent will not be valid as it won't be freely given. However, providing incentives such as loyalty schemes, is possible to some extent. For example, staff and students may be persuaded to sign up to a cashless catering system and as a reward for allowing the company to send them special offers, they will receive vouchers and a free cup of coffee on their birthday.

> **Examples for inappropriate consent:**
>
> *A lecturer asks students for consent to have their photos and contact details displayed on a public website linked to a project as otherwise they will not be able to participate in the project.*
>
> *The HR department asks potential employees for their consent to have their dates of birth, salary and private addresses transferred to the cashless catering system as otherwise they won't be able to participate.*

Specific and informed

For consent to be specific and informed, people must first be aware of the identity of who is processing their personal data. Both the University and any third party data controllers relying on the consent you are aiming to obtain will need to be expressly named. It is not enough to simply define a category of third parties.

> **Example:**
>
> This consent request would not be sufficient:
>
> *"You agree to the University, and any recruitment agencies with whom we might consult, processing your personal data in order to help you with your career choice."*
>
> This consent would be sufficient:
>
> *"You agree to the University to transfer your data to the University's Careers Service to help you with your career choice."*

People must also know what it is they consent to. This means that you must provide information in the relevant privacy notice about all the purposes for which personal data is being processed. Refer to the guidance about privacy notices and the privacy notice template for further information.

- Privacy Notice Template
- Privacy Notice Guidance

Verifiable

You must have an effective audit trail of how and when consent was given, so you can provide evidence if challenged, which means that you will need to keep a record in order to demonstrate what the person has consented to, including what information they were given, and when and in what way they consented.

You also need to record when people have withdrawn their consent. The consent record needs to be kept for as long as you continue to hold information about the data subject for that purpose.

Withdrawable

If you are relying on consent as the legal basis for processing data subjects' personal data, they have the right to withdraw their consent at any time. Therefore, when you ask for consent, you should also include details of how it can be withdrawn. Withdrawing consent must be as easy as giving it. There should be an easily accessible one step process which people can use on their own initiative at any time. If possible, people should be able to withdraw their consent using the same method as they gave it. For example, provide an *unsubscribe* link in every email or an email address, freephone telephone number or freepost address in your communications.

Once consent has been withdrawn, you should stop processing as soon as possible. However, if a person withdraws their consent it does not retrospectively affect the processing already undertaken. For example, if somebody has consented to participate in research, they will not be able to ask you to extricate their data from published studies, but they can change their mind about raw data about them being used in future studies.

Unbundled

Consent requests must be clearly distinguishable from the rest of the text of the document or form you use; it will need to be separate from other terms and conditions and as such easily identifiable as a request for consent. This can be done by using a separate consent form or by ensuring that the consent request is kept separate at the bottom of a form.

> **Example for *bundled*, invalid consent**
>
> *"We will collect your name, date of birth and any medical conditions from you. We will process the information you have provided us in order to enable you to use the University Sports Centre and take part in classes. You agree to us passing your personal data on to our sponsor who will send you marketing material for sportswear with the University's logo. We will also use the information you have provided us with to ensure you are kept informed of any new classes we offer. We will keep the information you have provided for as long as you are matriculated. We do not use automated decision-making or profiling.*
>
> *Please sign here....."*

Granular

Wherever appropriate, you will need to provide data subjects with granular options to consent separately to different types of processing. If you obtain consent for, say, processing personal data for displaying student photos on your website, you must have separate consent for using the photos for newsletters or for marketing purposes. Only if the activities are clearly interdependent or if providing a granular list of consent would be disruptive or confusing can you provide a single option for consenting.

The most important factor is that you clearly explain to people what they consent to in an understandable way. Should your purposes for processing the personal data change, you will have to consider reconsenting people as there is no such thing as *evolving* consent.

Note: For marketing activities (which does not only include the offer for sale of goods or services, but also the promotion of an organisation's aims and ideals. This includes any promotion such as, for example, a *healthy lifestyle* promotion, or a promotion of the University's cafeterias with a free coffee for the first 20 students presenting a coupon), see **Guidance on Direct Marketing**.

How long does consent last?

There is no specific time limit for consent. However, consent is likely to *degrade* over time, but the exact duration will depend on the context. Both the scope of the original consent and the data subjects' expectations need to be taken into account.

Consent will need to be reviewed regularly to check the relationship, processing and purposes have not changed. Processes must be in place to refresh consent at appropriate intervals.

A record of when and how consent was received and of the information provided to data subjects at the time of consenting must be kept.

Should data subjects withdraw their consent, a suppression lists must be kept to manage the withdrawal of consent and ensure that these data subjects are not contacted and/or asked for consent again.

If personal data has been received from third party data controllers, you will need to ensure that they have obtained consent from the data subjects before.

Examples:

The University Sports Centre runs a promotion that gives members the opportunity to opt in to receiving emails with tips about healthy living to get in shape for the summer holidays this year. As the consent request specifies a particular timescale and end point – the summer holiday – the expectation will be that no more emails will be sent out once the summer is over. The consent will then expire.

Development and Alumni can under the legal basis of legitimate interest contact individuals that are not alumni of the University and ask them to become donors. If an individual refuses consent to any further communication, then that individual's name and contact details must be entered into a suppression list to avoid any future contact.

Consent for scientific research

In the new data protection legislation it is acknowledged that collecting personal data for scientific research won't always allow the researcher to fully specify all precise purposes in advance. Therefore, consent will not need to be as specific as for other purposes. The general areas of research will need to be identified and, where possible, granular options to consent only to certain areas of research or research projects should be given.

BE AWARE

RE: *"You agree to the University to transfer your data to the University's Careers Service to help you with your career choice."* – What will happen as a result if this data transfer? Will the careers service contact the individual?

RE: *"For example, if somebody has consented to participate in research, they will not be able to ask you to extricate their data from published studies, but they can change their mind about raw data about them being used in future studies."* – This is a tricky area. If consent is withdrawn, under what lawful basis would the university be holding any personal data they wish to continue to hold? This is why the ICO suggests using alternative lawful bases for processing research data. That doesn't mean that consent wouldn't still be obtained for participation in the research, just that the lawful basis for the processing of the data as part of the research would not be GDPR consent. GDPR consent for data processing is not the same as ethical consent for participation, or consent for the common law of confidentiality, for example.

RE: *"Development and Alumni can under the legal basis of legitimate interest contact individuals that are not alumni of the University and ask them to become donors."* – Not if they do this electronically. The Privacy and Electronic Communications Regulations (PECR) would apply and they'd need consent for this.

Appendix E – example of a Privacy Notice Form

PRIVACY STATEMENT

(This part will be customised by you and placed on the form, website etc. you are using to collect the personal data)

Information about you: how we use it and with whom we share it

The information you provide will be used by the University to...

[Insert a plain English description of every purpose for which you will use the personal data. Refer to Section 1 of the how to customise your privacy notice *guidance.]*

[If applicable:]

The University uses an external company to.....

[Insert a plain English description of the processing undertaken by the data processor. Refer to Section 1 of the how to customise your privacy notice *guidance.]*

....on the University's behalf.

We are using information about you because...

[Insert legal basis, for example, because you have given us your consent, or: because it is necessary for the performance of your contract with us, or: because we have a legal obligation to do so, or: because processing is performed in the exercise of official authority vested in the University, in this case... Refer to Section 2 of the how to customise your privacy notice *guidance.]*

[If you rely on legitimate interest, explain in plain English why it is in the University's legitimate interest *to process personal data for this purpose.]*

[If applicable:]

Information about you will be shared with...

[Insert a list of all external bodies, agencies etc. with whom you will share the data. List all those internal departments that use the data for a different purpose. Refer to Section 3 of the how to customise your privacy notice *guidance.*

If you don't share data with a third party, delete this section.]

We will hold the personal data you provided us for ....

[To determine the time, please consult your local retention schedules.]

[If applicable:]

We do not use profiling or automated decision making processes. Some processes are semi-automated (such as anti-fraud data matching) but a human decision maker will always be involved before any decision is reached in relation to you.

[Note: Whether this section applies will need to be determined on a case by case basis and amended accordingly if not applicable. Refer to Section 5 of the how to customise your privacy notice *guidance.]*

If you have any questions, please contact...

[Insert role title and email address for local contact within school/department]

(This part is on the website)

Data controller and contact details

For data collected under this privacy notice, the University (the *University*) is the Data Controller (as that term is defined in the EU General Data Protection Regulation (*Regulation (EU)* 2016/679), registered with the Information Commissioner's Office.

You can contact our Data Protection Officer at dpo@your_university. Our data protection policy is on our website at http://www.your_university/

Data sharing

In addition to the primary purposes, we are also legally obliged to share certain data with other public bodies such as HMRC and will do so where the law requires this; we will also generally comply with requests for specific information from other regulatory and law enforcement bodies where this is necessary and proportionate.

Transfers outside the EEA

The University will only transfer data to countries outside the EEA when satisfied that both the party which handles the data and the country it is processing it in provide adequate safeguards for personal privacy. Details of such transfers and safeguards are on our website.

Your rights

You have the right to request access to, copies of and rectification or (in some cases) erasure of personal data held by the University and can request that we restrict processing or object to processing as well as (in some cases) the right to data portability (i.e. the right to ask us to put your data into a format that it can be transferred easily to a different organisation). If you wish to make use of one of these rights, please email your local contact.

If we have asked for your consent in order to process your personal data you can withdraw this consent in whole or part at any time. To withdraw consent, please email your local contact, who will explain the consequences of doing so in any particular case and initiate proceedings for withdrawing consent.

Complaints

If you are unhappy with the way we have processed your personal data you have the right to complain to the Information Commissioner's Office at **casework@ico.org.uk** but we ask that you raise the issue with our Data Protection Officer first.