UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 15

GDPR Myth Busting (GUIDANCE FOR ALL STAFF)

New data protection legislation has been a prominent source of discussion as the regulation is implemented. However amongst this discussion there are a number of myths that need to be addressed. The list below contains just some of the more prominent misconceptions around GDPR.

Myth	Reality
Everything about GDPR hinges on meeting the 25th May deadline	The GDPR is not focused on a fixed point in time. It is an evolution of existing law and organisational practices will need to change over time. Very few organisations will be completely compliant by the 25th May and for those that aren't it is important to plan the necessary changes which should include identifying risks and putting in place measures to mitigate against those risks.
GDPR is all about massive fines	Whilst it is true that the fines associated with GDPR attract many headlines, the regulation is actually about encouraging organisations to take responsibility for the management of individual's data and taking that responsibility seriously. The ICO prefers the carrot to the stick but they won't be afraid to use the sanctions if we do not take our responsibilities seriously.
GDPR is a massive and disruptive change	GDPR should not be a new burden if you are currently compliant with existing Data Protection Act 1998 which has been UK law for 20 years. GDPR is described by the ICO as an evolution of data protection law not a revolution.
GDPR is just yet another compliance regime	GDPR is a regulation that we will need to demonstrate compliance with. However GDPR is also about adhering to some common sense best practice and about ensuring that we can demonstrate to individuals how seriously we take their personal data. If we want to collect and use individual's data (either as potential students or research subjects) we need to obtain their trust and GDPR compliance is a significant way of demonstrating the standards to which we adhere to.
GDPR means individuals now need to consent for us to hold their data	Consent is one lawful basis for processing personal data but it is not the only one. In most cases data will be processed as part of a contract (such as the student or staff contract) or as an activity outlined in our public task as an educational and research institution. Consent is not a silver bullet and should not be the default for processing personal data.
GDPR means every breach needs reporting to the ICO	Only breaches that lead to a risk to an individual's rights and freedoms need reporting to the ICO. When considering whether a breach needs reporting the University will need to think about the nature of the personal data involved; how easy is it to identify individuals; and what the consequences are of the data breach. Information Assurance Services will be responsible for formally notifying the ICO.

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 15

Myth	Reality
GDPR means I need to get rid of all of my old files	GDPR does not require us to dispose of all of our 'old' information. However, it does say that we should only hold personal information for as long as it was required for the purpose of collection. Therefore if there is a valid and reasonable reason to retain the information you are likely to be able to do so. However, if you no longer need the information then you should look to dispose of it. It is sometimes possible to retain personal data for longer than normally required for historical and statistical purposes, in these cases you should liaise with the University Archivist to discuss transferring the information to the University Archives and Special Collections.
GDPR means I need to get rid of all of my old emails	As with other documents GDPR does not require us to dispose of all of our old emails. However it does say that we should only hold on to personal information in our inboxes for as long as it was required for the purpose of collection. Therefore if there is a valid and reasonable reason to retain the information you are likely to be able to do so. In general terms if you still have regular dealings with the individual then it is acceptable to retain the email. However, if you no longer need the information then you should look to delete the emails. Reviewing inboxes can be a large task for individuals therefore it can often be best to plan a thorough review over a number of weeks or months to make the task more manageable.
GDPR means I cannot display student's work	GDPR does not mean that you cannot display example of student's work. However in order to comply with both GDPR and Copyright legislation you should seek the explicit consent of the student to display their work (or to anonymise it).
GDPR means I cannot keep exemplars of a student's assessed work	GDPR does not mean that you cannot keep good examples of student's work to share with other students. However in order to comply with both GDPR and Copyright legislation you should seek the explicit consent of the student to display their work (or to anonymise it)
GDPR means I can't display photos of individuals	Photos are personal data under GDPR however this does not mean that you cannot display them. The legislation is not specific on photographs however you should consider the individuals in the photographs and what the likely impact on them will be. If your photographs are of a cohort of teaching/public facing staff it is not unreasonable to display the photos.
GDPR means I can no longer send information to the contacts on my database	If you currently maintain a mailing list of contacts which you routinely send information out to it is likely that you can still continue use this. However, you will need to ensure that those individuals have given you their explicit consent to hold their information. You should contact them to ask if they are happy for you to hold their information and use it for agreed and defined purposes. If you do not receive a reply then you should remove their information.

For further information on GDPR please see the University's GDPR web pages (www.le.ac.uk/gdpr) or email gdpr@le.acuk