GDPR Podbriefing Audio Transcript

Title

Hello my name is Geraldine Swanton, and I'm a legal director with Shakespeare Martineau in their education team, and I'm here today to talk to you about data protection.

Information is the oxygen of the modern age, at least according to Ronald Reagan, and that is particularly apt today, given the rapid technological change we have available to us, which makes personal data a very valuable asset in the hands of many organisations, including universities.

Introduction 00:30

There has been an enormous increase in the use of personal data, and this has created a need to prevent the erosion of personal privacy. When you think about it, universities use enormous volumes of personal data when carrying out their core and their everyday activities. For example, in the provision of teaching, in the conduct of research, in fundraising, and in the provision of support and other professional services.

The current data protection law was enacted in 1998 and it has failed to keep abreast of these rapid technological changes. My purpose today is to talk about the new data protection regime, which will come into force on 25 May 2018. It's called the General Data Protection Regulation, which I will refer to as the GDPR.

GDPR 01:30

The GDPR will apply to EU based organisations and EU organisations based outside of the EU. Further, it will apply to non-EU based organisations, which offer goods and services to individuals in the EU.

Now, just to provide you with a little bit of assurance, the new data protection regime, the GDPR, is very similar to the current data protection regime, but there are however some significant changes, and the purpose of this Podbriefing is to highlight those changes.

Personal data is entrusted to us by current students, current members of staff, prospective students, actual students, and sometimes they entrust to us their highly sensitive data so that it's very important that each of us understands the need to balance personal privacy with business and educational efficacy. Even though the legislation will not be fully enforced until 25 May next year [2018], it is really important to prepare now, so that we're compliant for May.

02:48

The General Data Protection Regulation regulates the processing of personal data relating to living individuals. Now, processing means anything that can be done to personal data from its creation, to its destruction, including its creation and destruction. It includes personal data in its electronic form, for example in emails or various electronic databases. It also includes information held in manual form, provided the

manual record is sufficiently structured so that specific information about individuals is readily accessible.

Personal data 03:35

Personal data does not need to include a person's name in order to amount to personal data. The key emphasis is on identifiability. Can somebody be identified either directly or indirectly? For example; can they be identified from the content, or can they be identified by additional information which is already known to other members of the University? In order to decide what is personal data, account needs to be taken of all the means used to identify the individual.

Principles of Processing 04:18

Now the GDPR has six basic principles for processing personal data and they are very similar in many respects to the current data protection regime. The first and very important principle is fairness and transparency. These are achieved by providing each individual with clear, intelligible, accessible privacy notices that inform individuals of why we have their data, the legal justification for having their data, how long they're going to keep it, are we going to give it to third parties? We have to identify the recipients or the categories of recipients, or are we going to transfer it overseas?

So the University is required to demonstrate much more detailed understanding of its uses of personal data than is currently required under the data protection act. A further emphasis on transparency are two new duties to report breaches. The first is a duty to report breaches of the GDPR to the Information Commissioner where there is a risk to the individual. The second duty is a duty to report to the individual where the breach represents a high risk to that individual. An example of that risk would be where a person was made vulnerable to identity fraud, or where we have inadvertently disclosed a large volume of their highly sensitive personal data.

06:00

The second principle is purpose limitation. That means that we can only use peoples' data for specified, lawful, and explicit purposes, and we can't use their data for any purposes incompatible with those specified and lawful purposes and I think the moral of the story here is that personal data is no longer our sovereign property to use as we will, simply because we hold it. We are accountable to the individual, to the uses to which we put their personal data.

A third principle is data minimisation. That means the information that we hold on people must be adequate to enable us to achieve the purposes for which we've obtained it in the first place. Secondly, that data must be relevant and not excessive, given the purposes for which we've obtained it. In short, it means we must be proportionate in our use of peoples' personal data. It's a prohibition on amassing excessive amounts of data that have no relevance whatsoever.

The principle of accuracy is also significant; our data relating to individuals must be accurate and we all know of the prejudice we can cause to individuals where we have inaccurate records. For example; where we put a record of disciplinary penalties on the wrong file and then we write a reference for an individual on the basis of that inaccurate information. The GDPR will require us to take all reasonable steps to either erase, or to rectify inaccurate personal data. That's a significant right for all individuals.

07:58

The next principle is one of storage limitation. That simply means that we must not keep personal data in a form which identifies individuals for any longer than is necessary given the purposes. There are of course exceptions to this principle and that's when we need to keep information in that form for public interest reasons or we need the information in identifiable form for research, historical or statistical purposes.

08:31

There is a principle of integrity and confidentiality that simply means that appropriate technical organisational measures should adopted to prevent unauthorised processing, or accidental loss, destruction or damage of personal data. Now this is really important because security is each persons' individual responsibility to discharge.

Lawfulness of processing 09:02

As well as adhering to six basic principles, the GDPR also requires that there are lawful justifications for our processing of personal data. So, we cannot process unless it is legally justified. We need to comply with one of the conditions prescribed by the GDPR in order to render processing of personal data, particularly non-sensitive data, justified.

Now, those grounds of lawfulness are very very similar to the grounds under the data protection act with one or two exceptions. The first exception is where we are relying on a persons' consent to process their personal data, there is a much higher standard of consent required. Under the GDPR, consent must be a freely given specific informed unambiguous indication of an individuals' agreement to the University processing their personal data. So, that means no pre-ticked boxes, no lists of consents tucked away in contractual documents. If there is no choice, if there is no individual control, then there will be no consent. The other slight change is that the condition of legitimate interests is slightly narrower in its application than we are currently used to under the data protection act.

Sensitive personal data, which includes data about a persons' health, disability perhaps, criminal convictions; that's usually justified only when we have a persons' explicit consent. However, there are other grounds on which we can rely, such as if we need to process it for medical purposes, for legal proceedings, or for the substantial public interest.

Data Protection by design and default 11:16

A new concept introduced by the GDPR is data protection by design and default. This means that the University has to adopt technical and organisational measures to ensure that data protection permeates every aspect of the University's business, and it's there to ensure that data protection is effectively implemented by everybody.

The concept of data protection by design and default introduces the notion of pseudonymisation, which is rather a strange term, but this simply means that we must consider storing personal data in a way that minimises the opportunity for identifying individuals without reference to other information. So, that would promote the use of ID codes, rather than the use of people's names. It also requires that personal data is not accessible to an indefinite number of individuals, and here this theme of proportionality is also obvious.

Third party processers 12:28

There are new provisions in relation to third party processors; they are third parties the University commissions to process personal data on its behalf. For example, when you use outsourced payroll companies, or when you use third parties to conduct student surveys on behalf of the University. As before, there must be a written contract between the University and the third party contractor, but this time the GDPR is much more prescriptive about the clauses that need to be inserted into the contract and essentially it is more prescriptive because it wants to ensure that the University is effecting proper control over the personal data processed by the third party on the University's behalf.

Transfers of personal data outside of EU 13:24

As with the current data protection regime, the University may not transfer personal data outside of the EU unless there is adequate protection for that data in the recipient territory. Now this is very relevant to the University with its overseas campuses. Adequacy can be demonstrated in a number of ways, and that is why the University has a data transfer protocol between it and its overseas campuses.

Adequacy of protection can however be demonstrated by other means. For example; where the individual has consented to the transfer of their data, or it's necessary to transfer their data to perform a contract with that individual.

Other obligations 14:09

Amongst the other new obligations the GDPR imposes is the requirement, not only to be compliant, but the University must also demonstrate its compliance. The University does this by having a very effective data protection policy, which is updated from time to time and everyone, each member of staff, needs to be familiar with it. The University must also, for the first time, keep a rather detailed record of all its data processing activities. So there is a need, under the new regime, for quite a lot of records to be maintained.

14:53

The individual has many rights under current law and these will be very similar under the General Data Protection Regulation. So, as for now, an individual will have the right of access to their data, they will have the right to have data erased (particularly where it's inaccurate), they will have the right to rectify data (again, where it's inaccurate), they have the right to object to processing or to restrict the processing of their personal data. Some of these rights are not absolute, so their application will be limited in nature.

Sanctions/remedies for non-compliance 15:36

Now, if the value of personal privacy and the requirement to balance personal privacy with the need to process personal data for business and legitimate educational purposes is not sufficient motivation to comply with the GDPR, then the new increased fines will no doubt do so. Under the GDPR the University can be fined up to the greater of 2% annual worldwide turnover or €10 million for particular breaches of the GDPR. For example; a failure to keep appropriate records, a failure to have proper data processer contracts, or a failure to maintain data protection by design and default.

Greater fines will be levied, up to 4% of annual turnover worldwide or €20 million (whichever is greater), for breach of the data protection principles, a failure to discharge individuals rights, or to transfers to third countries without adequate protection. As well as the fines, an individual can claim compensation for damage and/or distress as a result of a breach.

Final thoughts, key messages 17:00

Data protection is a benefit to each and every individual, but it is also the responsibility of every individual to discharge. So, when you handle personal data, some of the key messages are the following. Be sensitive to the potential for the invasion of personal privacy, don't amass large volumes of personal data that are not relevant, think about who really needs to have access to the personal data you handle, use ID codes where appropriate to minimise the potential for identifying individuals, familiarise yourself with the University's policies, and finally, treat all emails you send as professional correspondence that could be scrutinised by third parties in the future.

17:56

Thank you for your time. If you need any help or guidance with the General Data Protection Regulation, or compliance with current data protection law; information about how you gain access to those sources will be provided at the end of this Podbriefing. Thank you.