GDPR: Next Steps
Few could not know about GDPR, but what happens next and what do you need to know ...Page 2

Cyber Security
Universities collate, process, and store a wealth of data, read the top ten things universities should know ...Page 6

MILLS & REEVE
Achieve more. Together.

AHUA

Perspectives

Legal updates for the world of higher education

Dear Colleague

I doubt that many will remember in years to come where they were on "GDPR Day" (25 May 2018) when the General Data Protection Regulation came into force in every EU member state (including the UK), but you will no doubt remember receiving a blizzard of privacy notices which arrived in your email inbox in the days leading up to this historic privacy law milestone.

Only a few days before GDPR Day, however, the Information Commissioner issued a salutary warning on 21 May 2018 about the importance of privacy law in the form of a Monetary Penalty Notice to the University of Greenwich. This was for the sum of £120,000 and was the first Monetary Penalty Notice issued to a university in the UK. The Information Commissioner determined, following an investigation, that the university in question did not have in place appropriate technical and organisational measures for ensuring so far as possible that a security breach would not occur and that the contravention of the Data Protection Act 1998 on the facts of the case was sufficiently serious to warrant the imposition of a monetary penalty of this magnitude. The background facts are set out in the Monetary Penalty Notice which has been published on the Information Commissioner's website. It appears that one of the University's departments had developed a web microsite for a conference which was never decommissioned after the conference. The microsite was compromised and became the subject of a cyber-attack, leading to the extraction of personal data of approximately 19,500 individuals (including students, staff, alumni, external examiners and those attending events). The personal data comprised mostly names, addresses, telephone numbers and email addresses. However, it also comprised sensitive information of about 3,500 individuals, including various types of extenuating circumstances, assessment offences, learning difficulties, food allergies and staff sickness records. The Information Commissioner concluded that the University was not aware that its web infrastructure included a microsite that was vulnerable to external attack and which gave access to underlying databases and that the University did not undertake proactive monitoring activities to discover such vulnerabilities.

A new Data Protection Act 2018 has also now received Royal Assent and most of its provisions came into force on GDPR Day.

This edition of Perspectives looks at some of the important ongoing GDPR and cyber-security compliance issues facing data controllers and data processors and the rights that individuals now have under the new UK and EU privacy regime. Further information is available on our GDPR hub or by contacting me or one of our information law team, all the contact details are on page 12.

Gary Attle, Partner
+44 (0)1223 222394
gary.attle@
mills-reeve.com

In this issue:

“"We're not going to be looking at perfection, we're going to be looking for commitment."

GDPR:

Next steps...

Few will have failed to notice that the EU General Data Protection Regulation (GDPR) became effective throughout the European Union on 25 May 2018. It has been described by UK Information Commissioner, Elizabeth Denham as ***“the biggest change to data protection law for a generation”.***

Day one compliance with the GDPR is certainly a high bar. In fact, many organisations have reached “good” rather than “perfect”. Denham has acknowledged in media interviews that some organisations will need time to become fully compliant.

"We're not going to be looking at perfection, we're going to be looking for commitment."

She has emphasised that enforcement activity will be targeted towards larger data users who "deliberately, persistently or negligently misuse data". Although there is no grace period, the ICO is looking for an organisation to be “on the compliance journey”.

We set out below some of the key areas where your institution’s ongoing compliance effort should be focused.

Changes to your processing activity

If your institution is thinking of using existing data in a different way, or collecting data for a new project, you will need to think through the data privacy implications. Changes to the type of use will need to be notified to data subjects. Any new project should design in privacy from the outset, and a data protection impact assessment may be necessary.

As most institutions will fall within the GDPR definition of public authority, you will need to consider how this impacts any new activity, both in terms of identifying an appropriate lawful basis for processing activity and in terms of ensuring that your Data Protection Officer is appropriately involved in anticipated, new and ongoing processing activities.

New laws and guidance

The EU’s coordinating data protection group, (previously the Article 29 Working Party, to be replaced with the European Data Protection Board), and the UK Information Commissioner’s Office have already issued detailed guidance on many aspects of the practical application of the GDPR. We can expect the roll-out of guidance to continue as the GDPR beds in. The Article 29 Working Party has already revised its guidance on key topics like consent and transparency, guidance which was adopted by the European Data Protection Board on 25 May. Keeping up to date with new guidance and new versions, and revising your compliance measures to take account of them, will be important to ensure ongoing compliance.

And changes can be made to the legislation itself. The Data Protection Act 2018 permits a certain amount of evolution. New reasons for processing particularly sensitive “special category” data can be added, for example.

GDPR:

Next steps...

Codes of conduct and certification schemes

Elizabeth Denham has said that the ICO's next areas of focus will be codes of conduct and certification schemes, envisaged by Articles 40 to 43 of the GDPR.

Codes of conduct will be tailored to individual sectors, and to the needs of SMEs, to help them comply. The new Data Protection Act requires the ICO to produce codes of practice on certain areas: data sharing, direct marketing, age-appropriate design and journalism. Some have asked why these have not already been drawn up. Instead organisations have largely been left to their own devices in working out how the new law applies to their particular circumstances. But the workload for regulators has been demanding, and Denham defended the priority given to preparing guidance and checklists ahead of codes of practice.

Certification schemes are likely to develop over a longer timeframe. These require the involvement of third party certification bodies who are accredited to set standards and carry out assessments.

Adopting these standards when they emerge will provide greater confidence that your organisation is compliant, and be a way of demonstrating good practice to your customers and partners. They can also for example, provide additional GDPR-compliant options for transferring data outside the EU.

Data security and data breach reporting

The GDPR imposes tougher obligations around keeping data secure using appropriate technology. What is current now may quickly look out of date. You'll need to keep your systems and policies up to date, respond quickly to new cybersecurity threats and, where appropriate, deploy innovative defensive methods.

Data security is linked to the GDPR requirement, subject to certain conditions, to report personal data breaches to regulators, without undue delay and within 72 hours of becoming aware of the breach. Potentially reportable breaches include not only the unauthorised disclosure or access to personal data, but also the accidental or unlawful destruction, loss or alteration of personal data.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, subject to certain conditions GDPR also imposes an obligation to communicate specified information to the individuals affected without undue delay.

Institutions will need to ensure that they maintain appropriate response plans and procedures to ensure that their senior management, Data Protection Officer and key advisers are involved in determining what information needs to be supplied to regulators and individuals.

In this edition of Perspectives, Claire Williams looks in more detail at some key cyber security compliance issues (page 6).

"GDPR has arrived. If you are not perfectly compliant now, don't despair – lots of organisations are likely to be still on the journey to get there."

GDPR:

Next steps...

Sharing data and outsourced processing

You may find that you need to share data with another organisation. You'll need to ensure that data subjects are fully informed about this, and that the data remains properly protected.

If you engage a third party processor, you will need to ensure that they are capable of protecting the information, and use written contracts with appropriate terms and conditions to meet the requirements of GDPR Article 28. You can find our checklist here on what these requirements are.

The GDPR envisages the introduction of standard contractual clauses for controller to processor contracts. When these are published they can be used to replace existing T's and C's where the contract permits, and used in new agreements.

International transfers

The GDPR provides for international transfers in a similar way to the outgoing Directive. Existing adequacy decisions continue to apply, but we can expect to see updated versions of adequacy decisions, binding corporate rules and standard clauses appearing when they are finalised. Organisations involved in international data transfer should monitor these developments and adapt or replace their documentation, policies and practices where necessary.

Dealing with requests from data subjects

You are likely to have more requests from data subjects to deal with under the GDPR. Data subjects may want to withdraw consent to certain types of processing, like targeted advertising for example, or ask for their information to be erased. They may wish to exercise new rights like data portability, and transfer their personal information to another provider in a machine-readable format. We have produced a checklist on data subjects' rights and what you need to do to respond.

We have already seen an uptick in both subject access requests and requests for erasure, with some clients receiving hundreds of requests since updating their privacy notices.

Organisations should keep under review their ability to respond in a timely way to these requests. You may find with experience that your current systems fall short, and better methods are needed to ensure compliance.

For more detail on data subject rights in this edition of Perspectives, see Helen Tringham's article (page 8).

Active review

It makes sense to timetable active review of compliance obligations to ensure that your organisation does not slip into non-compliance. Your priorities and teaching, research and commercial partnerships may change over time, and it can be easy to overlook the impact that these changes might have on data privacy.

GDPR:

Next steps...

E-privacy reform

A new e-privacy regulation was originally planned to take effect at the same time as the GDPR. Failure to reach agreement amongst EU member states has meant that that hasn't happened. But the proposal remains a priority, with the EU Commission repeatedly calling for EU ministers to make progress. When the new e-privacy regulation is settled, we expect to see new rules on electronic marketing, likely to extend beyond phone calls, emails and texts to "over-the-top" communication channels like internet based phone calls and messaging apps. Current rules on use of cookies are likely to be exchanged for transparent use of browser privacy settings.

Although not a part of GDPR compliance, being ready for this additional element of data privacy reform is equally important for affected organisations. The sanctions regime is likely to be the same as for GDPR. That means fines of up to €20 million, or 4 per cent of global annual turnover if that is higher. Breach of direct marketing rules has been one of the few types of breach that has attracted the monetary penalty under the outgoing regime.

Brexit

The UK has expressed its intention to stay aligned with the GDPR after Brexit. How that plays out in practice, however, remains uncertain. While regulatory relaxation is not on the cards, divergence in the details may well evolve over time.

For the future?

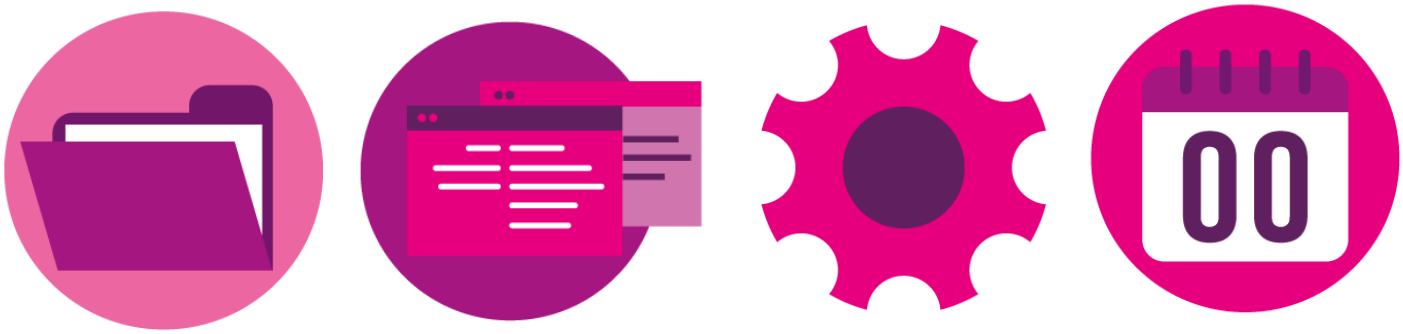
GDPR has arrived. If you are not perfectly compliant now, don't despair – lots of organisations are likely to be still on the journey to get there. And for the future, the message is – keep an eye on ongoing developments, and view compliance with privacy law as a continuing process that needs to be actively managed, rather than something to be done once and forgotten.

Any questions?

Robert Renfree

+(44)(0)1223 222212

Robert.renfree@mills-reeve.com



"Implementing cyber defences and promoting an appropriate security-focused culture is vital for continued innovation, as well as crucial to protect your brand."

Cyber Security:

Top 10 cyber issues for universities

Universities collate, process, and store a wealth of data. New research discoveries, commercially-valuable intellectual property, and the personal financial, health and other data of students, staff and others, are all contained within university servers. Implementing cyber defences and promoting an appropriate security-focused culture is vital for continued innovation, as well as crucial to protect your brand.

Five key operational considerations

Governance: Governing bodies, Vice Chancellors and other senior management functions are expected to drive the implementation of a cyber- and data protection culture, and be accountable in the event of a breach. Universities need to ensure they have implemented practical and enforceable security policies.

Marketing: In a competitive market, attracting the right students, investors and donors is essential. Changes in legislation mean that previous practices such as wholesale purchasing of contact lists without significant due diligence are no longer viable. Universities need to review and identify new, sustainable methods.

Data transfers: Cloud computing has numerous benefits, but in order to remain compliant with current data protection law it is vital that universities find out precisely where the servers they are uploading data to are located and what protections are in place. If they are overseas, you should have taken steps to ensure that the data remains secure and complies with GDPR requirements. Also, if data is processed on your behalf, does the contract specify the security measures required, and are you able to check they are in fact used?

Data processor contracts: Universities should continue to undertake appropriate due diligence checks on data processors before engaging them to process data on the University's behalf. They should also ensure that their contracts with data processors meet GDPR requirements, including obligations on the processor to take appropriate measures to ensure the security of its operations and systems.

Data management: Universities hold vast quantities of data, in both electronic and hard copy format, which they rarely access or use. Under the current law, personal data should not be held longer than is necessary to fulfil the purpose for which it was collected, and data minimisation is a central premise of the GDPR. At the same time, requests by data subjects for copies of the personal information that is held about them are on the rise. If you have not already done so, now is an ideal time to ask whether your organisation should continue to store these materials.

Five key cyber threats

Insider threats: It remains the case that most cyber security and privacy breaches are caused by malicious or accidental employee actions. Robust policies setting out protective measures, a sound understanding of data flows into and out of your organisation, and a well-designed and tested data incident response plan, will go a long way to preventing breaches or at least minimising their impact. Appropriate, interactive and targeted employee training is a necessary investment.

Bring your own device (BYOD)/mobile working: Students and staff use a vast array of laptops, tablets and mobile devices. The connection of so many personal items to your system brings with it the risk of malicious applications, targeted attacks which exploit known software vulnerabilities, and the theft of devices

Cyber Security:

Top 10 cyber issues for universities

with open connections to a university's networks. You should have a clear, published approach setting out the measures that you expect to be taken to alleviate the dangers, such as software patching, password use and encryption.

The Internet of Things: Modern printers, photocopiers, televisions, thermostats, locks and even desk toys may be 'smart', transferring data to each other and their manufacturers. Software vulnerabilities and failure to change factory-set passwords can allow third parties to access and control devices, whether as part of a targeted attempt to access your servers, or in order to co-opt your devices for use in cyber attacks. Organisations should be alive to the dangers and take appropriate counter measures.

Outsider infiltration: Complex and data-heavy organisations like universities are a target for cyber criminals, who seek access via phishing scams, theft of user credentials or even physically accessing your premises to obtain papers or install malicious software. A robust understanding of potential entry routes will let you formulate appropriate policies and deploy defensive technological measures. The use of layered security measures and increased defences for particularly sensitive or valuable data will be expected by students, investors and regulators alike.

Impersonation and spoof emails: Hoax websites and spoofed emails, created to mislead readers pose dangers for universities. Cyber criminals use these tools to divert funds (such as by providing students with false account details into which fees should be paid), or to damage an organisation's reputation. Basic defences include purchasing domain names similar to your own and applying email validation systems such as DMARC.

Any questions?

Claire Williams

+(44)(0)1223 222555

Claire.williams@mills-reeve.com

Data Subject Rights:

The new regime

GDPR has made a number of changes to the scope and type of rights available to data subjects.

Where a data subject exercised their rights before 25 May 2018 (i.e. under the previous law), the UK Data Protection Act 2018 includes transitional arrangements where the data controller had not yet completed the request by 25 May (broadly speaking, the Data Protection Act 1998 will still apply to such requests).

For requests received on or after 25 May, GDPR requires that information supplied to data subjects that exercise their rights, and communications relating to rights should be:

- Concise, transparent, intelligible, easily accessible and use clear and plain language (particularly where the recipient is a child); and
- Provided in writing "or by other means, including, where appropriate, by electronic means".

The tables in the following pages summarises the rights available to data subjects under GDPR and the main rules that apply. As with the exercise of data subject rights under the previous law, institutions will need to continue to apply careful judgment when responding to data subject requests. Such judgments will need to take account of the institution's legal obligations to data subjects including, where appropriate, to "third party" data subjects.

Any questions?

Helen Tringham

+(44)(0)121 456 8229

Helen.tringham@mills-reeve.com

For more information and resources visit our dedicated GDPR hub

www.mills-reeve.com/gdpr

Right provided by GDPR	**Notes**
Right to be informed See our privacy notice checklist for the details required to be communicated to the data subject.	If data is obtained directly from the data subject, the information should be provided at the time of collection of the data. If data is not obtained directly the information should be provided: ✓ within a reasonable period of obtaining the data (within one month); ✓ if the data are used to communicate with the data subject, at the latest, when the first communication takes place; and ✓ if disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
Right of access Data subjects have the right to obtain: ✓ confirmation that their data is being processed; ✓ access to their personal data; and ✓ other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).	Information must be provided without delay and at the latest within one month of receipt. You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If so, you must inform the individual within one month and explain why. Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to. You must provide a copy of the information free of charge. You can charge a 'reasonable fee': ✓ when a request is manifestly unfounded or excessive, particularly if it is repetitive. You could also refuse to respond but, without undue delay and within one month, you would have to explain why and inform them of their right to complain and to a judicial remedy; or ✓ to comply with requests for further copies of the same information.
Right to rectification Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.	You must respond within one month or, if the request is complex, this can be extended by two months. If you are not taking any action, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy. If you have disclosed the personal data to third parties, you must inform them of the rectification where possible and inform the data subject where appropriate.

Right provided by GDPR	Notes
Right to erasure A data subject may request the erasure of personal data where: a. the personal data: ✓ is no longer necessary in relation to the purpose for which it was originally collected/processed ✓ was unlawfully processed ✓ has to be erased in order to comply with a legal obligation ✓ is processed in relation to the offer of information society services to a child b. the individual: • withdraws consent • objects to the processing and there is no overriding legitimate interest for continuing the processing	You can refuse to comply with a request for erasure where the personal data is processed: ✓ to exercise the right of freedom of expression and information; ✓ to comply with a legal obligation or for the performance of a public interest task or exercise of official authority; ✓ for public health purposes in the public interest; ✓ for archiving purposes in the public interest, scientific research historical research or statistical purposes; or ✓ for the exercise or defence of legal claims. If you have disclosed the personal data to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
Right to restrict processing Processing must be suppressed where: ✓ the individual contests the accuracy of the personal data; ✓ an individual has objected to the processing (where it was necessary for performance of a public interest task or legitimate interests); ✓ processing is unlawful and the individual requests restriction instead of erasure; ✓ you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.	You can continue to store the personal data, but may only further process it: ✓ with the data subject's consent; ✓ to establish, exercise, or defend legal claims; ✓ to protect the rights of another individual or legal entity; or ✓ for important public interest reasons. You must inform individuals when you decide to lift a restriction on processing. If you have disclosed the personal data to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
Right to data portability This includes the right to: ✓ receive a copy of the personal data, free of charge, from the data controller in a commonly used and machine-readable format and store it for further personal use on a private device; ✓ transmit the personal data to another data controller; and ✓ have personal data transmitted directly from one data controller to another where technically possible.	The right to data portability only applies: ✓ to personal data that an individual has provided to a controller; ✓ where the processing is based on the individual's consent or for the performance of a contract; and ✓ when processing is carried out by automated means. You must respond without undue delay and within one month or, if the request is complex or there are numerous requests, this can be extended by two months. You must inform the individual of any extension within one month of the receipt of the request and explain why it is necessary. If you are not taking any action, you must explain why to the individual, without undue delay and within one month, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right provided by GDPR	Notes
Right to object Individuals have the right to object to: ✓ processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling); ✓ direct marketing (including profiling); and ✓ processing for purposes of scientific/historical research and statistics.	If processing for the performance of a legal task or legitimate interests, individuals must have an objection on "grounds relating to his or her particular situation". You must stop processing the personal data unless: ✓ you can demonstrate compelling legitimate grounds for processing, which override the interests, rights and freedoms of the individual; or ✓ the processing is for the establishment, exercise or defence of legal claims. If processing for the performance of a legal task or legitimate interests or for direct marketing purposes: You must inform individuals of their right to object "at the point of first communication" and in your privacy notice. This must be "explicitly brought to the attention of the data subject and presented clearly and separately from any other information". If processing for direct marketing purposes, there are no exemptions or grounds to refuse. If you receive an objection to processing for direct marketing purposes: ✓ you must stop processing personal data for direct marketing on receipt; and ✓ you must deal the objection at any time and free of charge. If processing for research purposes, individuals must have "grounds relating to his or her particular situation" in order to object. You are not required to comply with an objection if you are conducting research where the processing of personal data is necessary for the performance of a public interest task. If your processing activities fall into any of the specified categories and are carried out online, you must offer a way for individuals to object online.
Rights in relation to automated decision making and profiling Individuals have the right not to be subject to a decision when: ✓ it is based on automated processing; and ✓ it produces a legal effect or a similarly significant effect on the individual.	The right does not apply if the decision: ✓ is necessary for entering into or performance of a contract between you and the individual; ✓ is authorised by law (egg for the purposes of fraud or tax evasion prevention); ✓ is based on explicit consent (Article 9(2)); or ✓ does not have a legal or similarly significant effect on the individual. You must ensure that individuals are able to: ✓ obtain human intervention; ✓ express their point of view; and ✓ obtain an explanation of the decision and challenge it.
Breach Notification Right When a personal data breach is likely to result in a high risk to a data subject's rights, a data controller must notify the data subject of the security breach without undue delay.	The breach must be notified without undue delay.

Contact us...

Claire Williams
+(44)(0)1223 222555
Claire.williams@mills-reeve.com

Helen Tringham
+(44)(0)121 456 8229
Helen.tringham@mills-reeve.com

Robert Renfree
+(44)(0)1223 222212
Robert.renfree@mills-reeve.com

Kate Allan
+(44)(0)20 7648 9252
Kate.allan@mills-reeve.com

Richard Sykes
+(44)(0)121 456 8436
Richard.sykes@mills-reeve.com

Paul Knight
+(44)(0)161 234 8702
Paul.knight@mills-reeve.com

Peter Wainman
+(44)(0)1223 222408
Peter.wainman@mills-reeve.com

Gary Attle, Partner
T: +44 (0)1223 222394
E: gary.attle@
mills-reeve.com

About Mills & Reeve

Leading national law firm Mills & Reeve are a leading provider of legal services and commercial advice to the education sector. We have 119 partners and over 400 other lawyers across six offices: Birmingham, Cambridge, Leeds, London, Manchester and Norwich.

We have supported our education clients in their international activities in over 75 jurisdictions. In 2017/18 we invested in additional partner appointments to continue to support our clients with their international, technology and life sciences activities.

We have also continued to invest in our work on public law, regulatory, corporate and commercial matters to support our clients with their opportunities and challenges arising from the decision of the UK to withdraw from the European Union and the new regulatory frameworks under the Higher Education & Research Act 2017 and the EU General Data Protection Regulation.

We are the only law firm to be named for fifteen consecutive years in the Sunday Times 100 Best Companies to Work For.

MILLS & REEVE

Achieve more. Together.