IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Data Protection Reform: Gird your Loins for the GDPR

Eddie Powell

Eddie Powell
Partner
Fladgate LLP

Biography

Eddie Powell is a Partner in Fladgate LLP's (www.fladgate.com) IP, Technology and Commercial team, and is an intellectual property, technology and commercial law specialist and advises clients across a broad spectrum of legal issues. He has considerable experience in handling a wide variety of commercial issues and disputes involving all kinds of Intellectual Property (IP). He regularly advises on transactions ranging from exploitation through licensing or transfers to complex corporate or financing projects where IP is a key business asset. Eddie combines this with practical experience in enforcing IP rights and defending IP claims. He has considerable experience in advising content providers and publishers in this area.

He advises on commercial transactions such as licensing, distribution, franchising, agency and manufacturing arrangements, and technology projects such as IT procurement, supply and development. He regularly deals with e-business issues for clients across a range of industries.

Eddie also has considerable experience in data protection and privacy legal issues, and routinely advises clients on risk management methods, such as contract terms and policies, as well as day-to-day compliance steps.

Competition law issues are part and parcel of Eddie's work and he advises on the European and UK rules in this area, particularly those relating to free movement of goods and services within Europe.

Eddie qualified as a solicitor in England and Wales in 1991 and he has also been admitted in Hong Kong.

Keywords Data protection law, Brexit, General Data Protection Regulation (GDPR), Compliance, IT security
Paper type Opinion

Abstract

This article highlights changes to data protection law that will come into effect in 2018, including increases in the international scope of the law, changes to compliance steps, new rights for data subjects and new sanctions.

Introduction

25 May 2018: That is the day you need to have pinned to your noticeboard, as it is the day on which the EU's General Data Protection Regulation (GDPR) comes into force and will directly apply in the UK. Businesses have one year to improve their processes and systems ready for the changes.

These changes will apply regardless of Brexit the following year, and we can expect the provisions to remain intact for several years to ensure that data flows between the UK and Europe are not interrupted.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Set out below, is a summary of the key changes that will apply.

More businesses will be caught by EU DP Law

At the moment, the legislation only applies to data controllers who are based in the EU, so a cloud service provider based in the US allowing UK users to access the service will not be covered.

The GDPR will cover data controllers and processors, not just in the EU but those outside it where the processing relates to:

- the offering of goods or services to data subjects in the EU; or
- monitoring of the behaviour of subjects within the EU (for example, online behaviour tracking for advertising purposes).

The other key point is that data processors will now be directly subject to the regulations. Under the old system the controller was responsible for compliance and would simply contract the responsibilities down to his processor. Processors will now have their own set of responsibilities, even if they have no controlling function at all.

An overseas data controller or processor who is caught by EU rules will have to appoint a representative within the EU for data protection purposes if the processing is more than occasional, or if the data it processes includes "special categories" of personal data (such as health, ethnicity, sex life and political views).

Compliance will need to be built in

Two of the key principles in the new rules are:

1. **Purpose limitation**: data must be collected for specified explicit and legitimate purposes and not processed outside that purpose; and
2. **Data Minimization**: the data must be relevant and limited to what is necessary in relation to the purposes for which they are processed.

Controllers will have to consider whether they really need personal information to achieve a task or whether it is just "nice to have".

The GDPR goes even further; Article 25 is titled "Data Protection by design and default", and states that when determining the processing to be conducted, or the technology to be used, a data controller must implement effective technical and organizational measures to implement the principles of the GDPR, including data minimization. In addition, the controller must ensure that, by default, only data necessary for each specific purpose are processed; this applies to the amount collected, how it is used, how long it is kept and who can access it.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Essentially, data controllers must examine their systems and processes to ensure that they are set up from the word go to work to a minimum of personal data, and have appropriate processes for cleansing and compartmentalization, as well as tight security, discussed further below. If their systems are not set up to allow the controller to fully comply, that, of itself, will put the controller in breach of the GDPR.

Compliance will need to be documented and managed

The need to register or notify processing to regulators such as the ICO will be scrapped, but, in the UK, legislation will be put in place to allow the ICO to charge fees to data controllers (in what circumstances is not yet clear).

Instead, under the 'accountability principle' businesses will be obliged to have evidence available to demonstrate compliance with the key principles of the GDPR. In addition, Article 24 states that each controller must be able to demonstrate that its technical and organizational measures comply. These general obligations are supplemented by additional requirements depending on the controller and/or processor and the processing being conducted, as follows:

First, where a controller or processor will have to appoint a Data Protection Officer (DPO) if:

1. it is a public body; or

2. its core activities (which means primary, rather than ancillary activities) include processing operations which involve:

    i) regular and systematic monitoring of individuals on a large scale; or
    ii) large scale processing of special categories of data.

Second, each controller and each processor which has more than 250 staff, or who processes special categories of data which carries a risk or which is not occasional, must keep processing records. These records must contain:

- Purpose of processing;
- Description of data subjects and categories of personal data processed;
- Recipients of data;
- Transfers to non-EU countries;
- Proposed time limits for erasure; and
- Description of security measures.

Third, all controllers (regardless of their size) will be under an obligation to carry out data protection impact assessments (DPIAs) for categories of data processing that


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

can be seen as high risk and, where appropriate, this could involve consultation with data subjects (and, presumably, potential data subjects) themselves. This is required in particular when the processing:

- includes special categories of data;
- uses automatic profiling; or
- includes monitoring of public areas on a large scale using CCTV.

Guidance on when a DPIA is or is not required has been published by the collective EU data protection authorities[1]. They suggest circumstances where a DPIA is appropriate would include:

- processing of data related to employees;
- processing of data related to children; and
- plans to export data to a non-EU country.

If a DPIA is carried out and there is still a high risk to individuals, despite the measures proposed to be taken, then regulations require the controller to 'consult' with the supervisory authority. The supervisory authority can offer advice to the controller if it considers that the processing will breach the GDPR, or it can exercise its other powers (referred to below) in relation to the processing.

Fourth, a controller can only appoint a processor using legally binding contracts under which the processor provides sufficient guarantees of measures to comply with GDPR and protects the rights of data subjects. There is a long list of what the contracts must include, too long to list here, but the key points are:

- Limits on sub-contracting by the processor;
- Processor accepting responsibility for security measures;
- Processor being required to demonstrates compliance, and permitting the controller to conduct compliance audits;
- Deletion of all data at end of contract; and
- Restrictions on exports.

Security processes and breach notification

The GDPR sets out the new codification of security measures, although many elements are repeated from the previous legislation. It still refers to "appropriate technical and organizational measures" (now given the catchy acronym "TOMs") to be taken by the controller, but the new rules will require the controller to take into


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

account the costs, balanced against the risks, of implementing safeguards, in deciding what is an appropriate level of security. The GDPR lists what these measures could include:

- pseudonymisation/encryption of data;
- the ability to ensure system integrity and resilience;
- disaster recovery processes;
- processes for regularly testing and evaluating security.

One of the most striking and clear-cut of the changes introduced by the GDPR is the obligation to report security breaches:

1. A controller must notify a breach in security to the supervising authority, unless the breach is unlikely to result in a risk to individuals. Any notification has to be made within 72 hours of becoming aware of the breach. A processor has a corresponding duty under the GDPR to notify any breach (note there is no risk-based exception to this obligation) to the controller. Even if the controller decides the risk levels do not require it to notify, it must keep records of any breach.

2. There is a corresponding duty to notify the data subjects affected, where there is a 'high risk' to them. This can be relaxed if steps have been taken to resolve the risk. If notifying the individual subjects would involve a disproportionate effort, then an alternative is to find another means of 'public communication', such as advertising. Note that even if a controller does not consider notification to subjects to be appropriate, the supervising authority can require it to do so.

Export of data

There is no huge transformation in the restrictions on exporting data outside the EEA. As before, there will be a list of approved countries and there is provision for use of approved standard contract wording or binding corporate rules which will allow organizations to transfer data to unapproved countries. In addition, the GDPR makes provision for approved codes of conduct and third party certification mechanisms to be developed which, backed by binding contract commitments, could be used to permit transfers.

However, under the old regime, the data controller had the option, if neither of the more standard form mechanisms worked, of doing its own assessment, combined with its own contract for export. This will no longer be possible without getting authorization from the relevant national supervisory authority.

Processing gateways narrowed

We now focus on how the data controller interacts with the data subject and what is needed to allow personal data to be processed in the first place.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

This basic structure is unchanged. The new regulations set out gateways for processing, similar to the old rules which include:

- consent;
- processing necessary for performance or creation of a contract with the subject;
- processing necessary for compliance with a legal obligation on the controller;
- processing necessary for performance of a public interest task or exercise of official authority; and
- the processing being necessary for the legitimate interests of the data controller, balanced against the rights and interests of the data subject.

One of the key changes is where processing relies on the consent of the data subject. The new rules move much further towards requiring what lawyers would call express (rather than implied) consent. The definition of consent now requires a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

The reference to affirmative action means simply that pre-checked boxes or the very common notices that we all see saying "please check here if you do not agree" will no longer be valid.

Any request for consent must be presented in an intelligible and easily accessible form, using clear and plain language, and, importantly, must be distinguishable from other content and terms. In determining if consent is 'freely given', account is taken with regards to whether performance of a contract is conditional on the provision of data which is not necessary for the contract. A specific right for the data subject to withdraw consent at any time is also included.

The new rules deal specifically with consent given by children for the first time. A parent's or guardian's consent will be required for processing of data for anyone under 16, although individual member states can opt to reduce the age, to a minimum of 13.

The other main ground of processing that is used these days is the more general "legitimate interests of the data controller". As before, this gateway is subject to the fact that there must be a balancing act. Those "legitimate interests" can be overridden by the interests of the rights and freedoms of the data subject, and a higher standard applies for children.

There is now a specific prohibition on processing special categories of data unless there are grounds for doing so. But interestingly, the prohibition will not apply if the information concerned is "manifestly made public" by the data subject.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Subject's rights to information

Under the current rules, for processing to be lawful, the data subject has got to be made aware by the data controller of what processing is being carried out. The new rules will increase the amount of information that has to be provided, and the GDPR sets out a long list of what needs to be included in the notice. The ICO has recently updated its guidance on privacy notices, and helpfully confirms that if that guidance is followed in preparing privacy notices, they will comply with the GDPR when it comes into force[2].

Subject access requests (SARs) will be alive and kicking under the new regime. The basic provisions remain the same, but now when responding to an SAR, a data controller will also need to alert the data subject to the existence of their rights of rectification or erasure, and their rights to lodge a claim to a supervisory authority. It will no longer be possible to charge a fee, unless the request is 'manifestly unfounded' e.g. where the request is repetitive.

Other rights of data subjects

The basic rules in the existing legislation will remain: data must be accurate and can only be kept as long as necessary, and a data subject can require a correction of the data (the right of rectification).

The right to erasure or the "right to be forgotten" is a new basic right. The data subject can require a controller to erase personal data once the conditions that enabled processing no longer apply, for example, where consent is withdrawn, where the processing is no longer necessary, or where the rules have been broken. As well as erasing the controller's own data, there is an obligation to notify third parties to whom the data was transferred about the erasure, and to ask them to do likewise.

Another new right is the portability right – this allows a subject to insist that data provided by the subject being processed by one supplier is transferred in machine-readable form to another provider selected by the subject. Further guidance on this new right is available from the EU co-ordinating body[3].

Sanctions

Much of the regulation deals with how national supervisory authorities will be able to co-operate with each other, particularly for multinational companies. There will be a "lead" authority in one European country for multinationals, the idea being that companies with more than one office do not have to deal with multiple authorities.

The real sting in the tail of the new regulation is the new administrative fine regime, which is going to bring the data protection risk into the category that we have normally been used to seeing in competition law cases. The fines fall into two categories:

- **Level 1**: higher of: €20 Million or 4% group global turnover;
- **Level 2**: higher of: €10 Million or 2% group global turnover.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

The Level 1 fines cover issues such as not having complied with processing gateways, not complying with requests for rectification, erasure or porting of data, and not providing information to subjects when obliged to do so.

It is also worth noting that the authorities will have powers to order cessation of processing, powers of entry and systems access, and a ban on flows to specified overseas recipients.

Enforcement by civil litigation is also given more teeth: individuals will be entitled to take court proceedings in relation to breaches, even where the damage they have suffered is not material.

What should you do?

The ICO has produced a list of suggested steps for UK businesses[4]. You, as CEO or CFO, should take on the role as champion, even if you appoint a separate DPO. I would suggest a plan which includes the following:

1. The key starting point is to draw up a list of what personal data is held by your company, what for, and what is done with it.

2. Prepare draft processing records for the above and carry out DPIAs for your processing activities (even if GDPR does not require it) – this will help identify changes required.

3. Some of your IT systems will need to be changed – start the process for implementing these.

4. Ask your data processors (for example, payroll, marketing database and outsourced service providers) what they are doing to comply and vet these responses.

5. Some personal data you hold may need to be deleted! Apply a strict test of what is necessary.

6. Arrange upgrades to privacy notices and contracts as required, ready to be sent out Q1 2018.

Reference

1 Article 29 Working Party draft paper on data protection impact statement 4 April 2017
2 ICO's code of practice on privacy notices, transparency and control" 7 October 2016
3 Article 29 Working Party: *Guidelines on right to data portability*, 5 April 2107
4 ICO checklist: *Preparing for the GDPR: 12 steps to take now*, 13 March 2017