MAKE IT PERSONAL

With new EU data protection rules on the horizon, organisations should take steps to ensure compliance or face tough sanctions

IN RECENT YEARS, TECHNOLOGICAL advances in areas such as mobile and cloud computing and the ubiquity of the internet have made it ever easier for businesses to handle vast amounts of data on their customers, suppliers and staff, to move the information around and share it domestically and internationally.

With this come increasing threats to that data, some external (such as theft by hackers) and others internal (such as accidental loss by employees).

Understandably, particular concerns arise in respect of data relating to people and their personal lives, namely personal data. Those concerns have been exacerbated by recent publicity, such as the hack attacks on a Sony data centre (which led to the theft of data relating to millions of people), mass surveillance of citizens by the US National Security Agency (NSA) and the vulnerabilities of many websites and the personal data on them caused by the Heartbleed bug.

In short, businesses handling personal data are rightly concerned about what they can or cannot do with it, and people want to feel that their privacy will be respected.

A number of laws relate to the protection of data. In the EU, the main data protection laws derive from EU Directive 95/46/EC. However, the regime is being upgraded, with a draft General Data Protection Regulation currently proceeding through the European legislative process.

This article examines the directive in so far as it relates to international data transfers in the private sector and how this is likely to change following the introduction of the regulation.

Current landscape

The directive aims to protect people's privacy and their personal data. Following its ratification, each EU country introduced national legislation to give it effect, albeit with some discretion as to its implementation. As a result, there are 27 different implementations, some more light touch than others.

Under the directive, the "data controller" is responsible for any personal data it holds and for ensuring that the data is "processed" in accordance with its requirements. A controller is the "person" that decides what to do with the data, such as a retailer that holds personal data on its customers. Processing is defined widely and includes collecting, holding, disclosing and using the data. "Personal data" is data by which an individual can be identified, such as a name and address.

The directive also recognises the concept of the "data processor", which processes data on behalf of a controller. A cloud service provider that stores data on behalf of a controller is an example of a processor. No obligations are imposed on the processor and, in most countries, the processor has no statutory responsibilities.

Right to share and security

The directive imposes various obligations on the controller, the overarching one being that personal data must be processed "fairly and lawfully". At least one of several "fair processing" conditions must be fulfilled for the processing of personal data to be lawful.

Sharing (as in disclosing) data is a form of processing and the fair processing condition most relevant to sharing personal data in the business world is that it is necessary for the controller's "legitimate interests" unless the sharing is prejudicial to the individuals concerned. (The condition does not apply to sensitive personal data, which is afforded additional protection. An example of sensitive personal data is information about a person's racial origin and religious beliefs.)

Arguably, the most important requirement under the directive is that the controller must have appropriate organisational and technical measures in place (see below) to protect any personal data in its charge against unauthorised processing, loss or damage. To paraphrase, the controller must keep the data secure and be on guard against external threats (for example, from hackers) and insider threats (namely, from its own employees and consultants). Technical measures should, for example, include ensuring that vulnerabilities in IT systems are patched promptly. Organisational measures should include having appropriate policies and procedures in place.

In relation to data sharing, whether domestically or internationally, this means that a controller must satisfy itself that the recipient will also keep the data secure (from both technical and organisational perspectives). Where the personal data is to be transferred to a processor, the directive also specifies that the controller and processor must have a written agreement (or legally binding instrument) in place under which the processor undertakes to keep the data secure and to process it only in accordance with the controller's instructions.

The controller must have appropriate organisational and technical measures in place to protect any personal data in its charge against unauthorised processing, loss or damage

Even if sharing is allowed (for example, pursuant to the controller's legitimate interests), the directive prohibits personal data from being transferred outside the European Economic Area (EEA) unless the controller assures an adequate level of privacy protection (the adequacy requirement). The circumstances in which personal data can be exported outside the EEA are discussed below.

Exporting data

- *Safe list*: the European Commission can decide the adequacy of the protection in certain jurisdictions. Transfers of personal data to jurisdictions in the "safe list" are deemed to meet the adequacy requirements. Currently, jurisdictions on the safe list include Argentina, Canada, Israel, Switzerland, Uruguay, Jersey, Guernsey and the Isle of Man.
- *Safe harbor*: personal data can be exported to the US, which is not on the safe list, if it is transferred to a US company that is a member of the so-called "safe harbor" scheme (and has to adhere to certain principles and make a public declaration to this effect). The US Department of Commerce administers the scheme, but there is no approval mechanism.

It should, however, be borne in mind that safe harbor companies will also be subject to US laws. For example, the Patriot Act gives US government agencies extensive rights to access data, including personal data relating to EU citizens, on the computers of US companies, irrespective of whether they are safe harbored.

- *Binding corporate rules (BCRs)*: companies with operations in and outside the EEA can use BCRs to export data to other companies in its group but that are located outside of the EEA. An application is made to the "home" data protection authority and, if approved, it will be circulated to the other relevant data protection authorities for approval. The rules now include a mutual recognition process in 15 member states. If the authority receiving the submission accepts the BCRs, other participating authorities should do so without further scrutiny. Setting up BCRs is not to be taken lightly as the documentation must explain how the group will provide adequate safeguards and be legally binding; one company in the group has to be responsible for the entire group's compliance; and the entire group has to undertake comprehensive data protection audits. In practice, only the larger and more sophisticated multinationals choose this option.
- *Self-assessment*: in the UK, a controller can undertake a "self-assessment" and, if satisfied that the data will be adequately protected, the data can be transferred outside the EEA. The Information Commissioner (the UK's data regulator) expects any controller to be able to demonstrate that an appropriate analysis has been undertaken.
- *Model contractual clauses*: the company to which the data is to be exported can sign up to model contractual clauses approved by the European Commission. Two sets exist: one applies when the importer is a controller and the other set to when it is a processor. In practice, most companies rely on these clauses to fulfil the adequacy test. Some countries have imposed additional conditions in implementing the adequacy test, such as a requirement to have the arrangements approved by the local regulator before the transfer takes place.
- *Other derogations*: personal data can be transferred to countries outside the EEA in other circumstances, although these are less likely to be relevant in a corporate context. For example, the transfer can take place if the individuals to whom the data relates have given consent. In practice, however, it is difficult to secure consent from large numbers of people.

Sanctions and private actions

Failure to comply with the directive can result in the censure of the regulators, hefty fines and criminal sanctions in the case of flagrant abuses. In the UK, the Information Commissioner can impose fines of up to £500,000 (€607,000). To date, the largest fees have been given for serious failures to keep the data secure.

Under the existing rules, an individual can sue a controller for damages suffered as a result of the unlawful processing of their personal data. However, private actions are rare, partly because of the difficulties in claiming compensation for distress and partly because individual claims, whether for financial or distress damages, are unlikely to be significant.

However, new case law arguably makes it easier to claim for distress and the possibility also remains of US style class actions being undertaken against controllers. Substantial damages have already been awarded in US courts and a class action lawsuit has recently been filed against a major US retailer following a security breach that affected millions of its customers.

On the horizon

As mentioned above, a regulation is currently making its way through the EU legislative process. The Parliament recently approved a provisional text after months of fierce lobbying in relation to the Commission's original proposal. Once it becomes law, it

Top tips

1 **Data security:** make this a priority.

2 **Threats:** use a combination of technical and organisational measures to guard against internal threats (accidental loss by employees) and external threats (hack attacks).

3 **Technical measures:** these should include patch management, firewalls to guard against viruses/malware, device encryption and the like.

4 **Organisational measures:** use appropriate policies and procedures so that employees can play their part in keeping things secure.

5 **Data sharing:** only share data if you are satisfied that this is permitted (for example, it is in your legitimate interests to do so) and that recipient also has effective technical and organisational measures to keep the data secure. If the recipient is a processor, make sure you also have this assurance in writing (namely in a contract) and other assurances which make sense, such as the right to get the data back or have it destroyed as you deem fit.

6 **International transfers:** there will extra hoops to jump through if personal data is to be sent outside of the EEA to a country which is not regarded by the European Commission as having adequate privacy laws in place (for example, there are model clauses which you will need to impose on the recipient).

7 **Subcontracting:** keep an eye on the extent to which your suppliers use sub-contractors as the same considerations apply. You will be held responsible if something goes wrong.

Although these tips are based on privacy laws relating to personal data, they should also be borne in mind (if not applied mutatis mutandis) in respect of other data for which you are responsible.

will take direct effect two years later in the member states without the need for local implementation. Several proposals should be noted in respect of international data transfers.

Right to share and security

The legitimate interests condition is preserved but can be overridden when the processing does not meet the individual's reasonable expectations. Greater transparency obligations will also be imposed on the controller, such as informing the individuals concerned of the legitimate interests being pursued, documenting these and reminding the individuals of their right to object. If data has been 'pseudonymised' (personal identifiers are replaced with a code, but the person may be identified by anyone with access to the code), processing is presumed to meet the individual's reasonable expectations.

The regulation keeps the spotlight on security by obliging both the controller and the processor to implement appropriate measures to keep the data secure and to test those measures regularly.

Where processing is to be carried out by a processor, the controller must also reserve the contractual right to inspect the processor's facilities, which many service providers resist at the moment.

Exporting data

- *Safe list*: the Commission will be able to determine a country, territory or processing sector in a country or an international organisation as being on the safe list. Only the Commission (not a controller) will be allowed to decide that an adequate level of protection for personal data is in place. This rules out the use of self-assessment in the UK.
- *Safe harbor*: changes to the safe harbor scheme were not planned, but reform is now expected following revelations of safe harbor companies sharing personal data with the NSA. For example, a controller or processor must defer to its data protection authority if a government agency requests the disclosure of personal data.
- *BCRs*: these will be approved by a single data protection authority. That said, only larger international organisations are likely to continue to use BCRs.
- *Model contractual clauses*: a data protection authority can adopt model data protection clauses that have been declared valid by the Commission or can specifically authorise contractual clauses between the controller or processor and the recipient of the data.
- *European data protection seal*: if both the controller and the recipient of the data have obtained a European data protection seal (discussed below), the adequacy requirement will be met.

As to transitional periods, existing adequacy decisions by the Commission (for example, as to which countries are on the safe list) will benefit from a five-year sunset period after the regulation comes into force and authorisations by data protection authorities (such as transfers based on standard data protection clauses and BCRs) will benefit from a two-year sunset period.

Sanctions and private actions

Sanctions will be tougher. For example, fines will be up to €100m or 5% of global turnover (whichever is higher). However, if the controller or processor has a valid seal, the fine will be imposed only in cases of intentional or negligent non-compliance.

Organisation should not underestimate how easy it is to lose control of data that is in its charge because of advances in technology and developments in working practices

The regulation gives anyone who has suffered damage (including non-pecuniary damage) as a result of unlawful processing the right to compensation by the controller or processor for the damage suffered.

Further, the regulation includes provisions allowing consumer and privacy groups to bring actions on behalf of one or more claimants and there are proposals for collective redress (akin to US-style class actions) in the EU's legislative pipeline.

Other features

The controller or processor may request its data protection authority, for a reasonable fee, to confirm whether the processing of personal data is complying with the regulation. The authority may accredit specialists to carry out the auditing of the controller or processor on its behalf. If the authority is satisfied that the controller or processor is competent, it will be certified with the seal, which will be valid up to five years.

The regulation imposes a general requirement on controllers and processors to carry out and document risk analyses of the potential impact of processing on the rights of individuals. Where the processing operations are likely to present specific risks (for example, if there will be the processing of personal data relating to more than 5,000 data subjects during any 12-month period), the controller or processor is required to carry out a formal "data protection impact assessment". Impact assessments must be reviewed regularly (or straight away, if the circumstances change). Although impact assessments are not mandatory under existing laws, the UK's Information Commissioner has been encouraging their use for some time.

The regulation will catch all processing by a controller or processor relating to the offering of goods or services to individuals in the EU (irrespective of payment) or monitoring their behaviour even though the controller or the processor is established outside the EU. This means that a US cloud service provider that hosts personal data of EU individuals will be caught even if the provider's clients are not themselves based in the EU.

The regulation introduces a requirement on the controller to notify the data protection authority without undue delay of any breach of personal data and to inform the individuals concerned. A concern here is that data protection authorities will be inundated with notifications (as there is no materiality qualification) and will not cope. Further, companies remain concerned about having to notify all affected people as a matter of course, not least because of adverse publicity and loss of goodwill.

Personal data is defined widely to include identifiers such as IP addresses as long as they relate to an identified or identifiable individual. The term "sensitive personal data" is replaced by special categories of data that has been expanded to cover gender identity. Where consent is required, it must be freely given, specific and "explicit" (whether sensitive or not), silence or mere use of a service will not suffice. Consent requires clear affirmative action such as ticking a box in a privacy policy. (Presenting users with pre-ticked boxes that they have to untick will not be acceptable.).


Shutterstock

The Commission had originally proposed a "one-stop shop" for compliance, but this has been replaced by a "lead authority", where a controller or processor is established in more than one member state or where personal data of residents of several member states are processed. The data protection authority of the main establishment of the controller or processor will be the lead authority and must consult other data protection authorities to reach a consensus. If a consensus cannot be found, the European Data Protection Board (EDPB) must be involved and has the power to impose decisions on the individual authorities.

The regulation when the controller and processor must appoint a data protection officer. This includes processing being carried out in relation to more than 5,000 people in any 12-month period.

Originally, the Commission had envisaged a big role for itself in issuing guidelines, recommendations and best practice etc. This role has been cut back and the role of the EDPB beefed up.

Under its investigative powers, the authority has access from the controller or processor to all personal data, documents, information and premises, including any data processing equipment. A data controller that appoints a processor will therefore need to ensure that it secures the right for the regulator to have access to the processor's equipment.

What next?

After the vote by the European Parliament, the draft regulation will now be passed to the Council, which will approve it or send it back to Parliament with further amendments. If the Council approves the text, it will become law. If the text is amended again, Parliament could approve the new amendments (in which case it becomes law), reject them (then the process ends) or amend the text again and send it back to the Council. If it comes to this, the Council must accept the text or send it to the Conciliation Committee. This committee is comprised of representatives of the Council and Parliament and it will try to agree a compromise text. This is the last chance for amendments to be made. If the committee cannot agree a text, the process ends. If a compromise text is agreed, it goes to Parliament and the Council for a final vote. If either party rejects the text, the process ends. If the process ends, everything goes back to square one and the Commission will have to decide whether to start over or to abandon the proposed legislation.

If adopted in its current form, the law will be more prescriptive than currently, will place a heavier compliance burden on controllers and will impose statutory obligations on processors (such as cloud service providers) as well as on controllers. In other words, businesses falling short under the current rules will fall short under the new regime and face tougher sanctions.

Therefore, any steps an organisation takes to comply with the current rules and to establish good (if not best) practice will put it in good stead for the future. Although the rules can be technical, no organisation should underestimate the importance of applying common sense and taking precautions appropriate to its business and the data for which it is responsible.

Organisations should also not underestimate how easy it is to lose control of data that is in their charge because of advances in technology and developments in working practices. (For example, data that is downloaded onto a personal mobile device, such as a tablet, which is being used for work purposes (known as 'bring your own device') will be at risk if the device is lost or stolen, particularly if the device is not protected. The risks necessarily increase if that data is subsequently backed up onto a public cloud service and is then synched onto a number of other devices.)

In short, organisations need to be on top of the risks to their data and be ready to respond to changes in technology and working practices. Whether an organisation is undertaking a top-down review of its approach to data protection or looking at specific aspects, such as data sharing, a few issues should be considered.

First and foremost, the controller will need to have its own house in order in terms of security. Technical measures should include installing security software updates as soon as they are available, using robust firewalls to guard against viruses and other malware and encrypting all mobile devices and storage media to prevent loss or theft of the data. Organisational measures should include having effective (and user-friendly) policies and procedures in place so that employees and consultants can play their part. Importantly, the policies should be supported by appropriate training, particularly when they are updated.

It will be worth assessing the extent to which personal data is shared with other group companies or third parties (such as cloud service providers), inside and outside the EEA. Where the data is (or about to be) shared, the controller will need to be satisfied that the recipient is also in good shape as far as security is concerned. If the recipient is a processor, the controller will also need to extract a contractual promise from the processor to this effect. Furthermore, the contractual right to get the data back or have it destroyed should be seen as a minimum requirement. Where the data is to be exported outside the EEA, the controller will need to satisfy the "adequacy requirements" (such as having model clauses in place).

The controller will also need to be on top of things as far as subcontracting is concerned. For example, the use of a cloud service by a processor may, of itself, make the controller non-compliant, particularly if the service provider is located outside the EU and has inadequate security in place.

Last, but not least, organisations should get used to the idea of carrying out risk assessments, particularly in respect of activities likely to present specific risks to personal data (such as data sharing) and to keeping these assessments under review. If a company suffers a major security breach, it will not go down well with the regulators if it transpires that a risk assessment has not been undertaken.

Anthony Lee is a partner at DMH Stallard