European data protection – prepare now and avoid the risks

Contents

Publication number 13778679

European data protection – prepare now and avoid the risks

Time to review your approach?

There is not an organisation that does not hold and process personally identifiable data – not least about its staff, clients or suppliers, or all three. In Europe, how this data is handled has been regulated by data protection laws since the early 1980s. Those already complex rules are set to be shaken up by the European Commission (**EC** or **Commission**), which is on a mission to force both the public and private sector to apply more rigorous standards to data processing activities.

In January 2012 the Commission announced a radical proposal to overhaul the Data Protection Directive. The changes will have a huge impact on all organisations with operations in or focused at Europe, as will the penalties for those who get it wrong. Large fines (up to 2% of global turnover have been proposed) are being lined up for local regulators to impose on non-compliant organisations.

In short, the new laws will:

- increase the regulatory burden on organisations;
- increase the amount of time, money and personnel required to achieve compliance; and
- raise the stakes, in terms of potential fines and brand damage, which could arise from non-compliance.

Savvy organisations are preparing now. Many are calling on experts to audit their data procedures, as well as those of their partners and suppliers. Others are already implementing the measures which the law will shortly require and which regulators are already taking as their measure for good industry practice.

The case for taking action now to improve data protection compliance is compelling. It will take time to ingrain the level of data governance that the new laws are seeking to set. Also, recent regulator enforcement actions, in the UK and across Europe, show that poor data governance practices are already being punished by the data protection authorities. Often this is done via the imposition of an obligation to bring in costly new processes and training schemes at short notice across not only an errant company, but also its supply chain.

Perhaps most significantly, there are also the ever-present PR consequences of data protection non-compliance to consider and the question of what steps can be taken in advance to manage the damage which a data breach could cause? The knock on effect of Sony's experience at the hands of hackers in 2011 was a timely reminder to all businesses of the difficulty that the media, public and shareholders have in forgiving a failure to have in place good data protection procedures and plans.

Here is our guide to the new data protection laws that have been proposed and the compliance steps that we recommend that companies should be taking.

What's around the corner?

Most people would agree that Europe's data protection regulatory regime desperately needs an overhaul. The current laws originate from a Directive written in 1995 in a pre-cloud computing era, before offshoring, globalisation and digital business practices became key business concerns.

Since 1995, new data protection laws have been layered one upon another as law makers have desperately sought to keep up with technology developments. The result is widely seen as over-bureaucratic, with too much focus on registrations and filings. The EC has made no secret of its desire to overhaul the European Union's (**EU**) data protection regulatory regime. Recently, its botched attempt to introduce new cookie/tracking technology laws in a harmonised way has led to an additional desire for a single set of EC-drafted laws to apply across Europe.

In its draft Regulation published on 25 January 2012, the EC set out the new laws that it would like to be introduced. Once these have passed through the European parliamentary system, because they are in the form of a "Regulation", they will have direct effect in every EU Member State with minimal further scope for debate, or rationalisation. While a more harmonised data protection regulatory landscape sounds appealing, the uncompromising approach taken by the EC's draft Regulation is a cause for concern for business.

Key points proposed by the EC's draft Regulation include the following:

(a) **Fines** – national data protection regulators will be given the ability to impose significantly higher fines of up to 2% of global turnover where basic knowledge/consent obligations or requirements to adopt good policies and procedures are not followed.

(b) **Data Protection Officers (DPO)** – private sector companies with more than 250 employees, or whose core activities involve regular monitoring of individuals, as well as public authorities will all be required to formally appoint a DPO. The DPO must be empowered by their organisation to act as an independent assessor of its compliance with data protection laws and report to the board of directors in doing so. The Regulation specifically requires the DPO to co-ordinate data protection by design and privacy impact assessment initiatives (see below for more details on both) and to be responsible for data security initiatives generally. Responsibility for training staff is also mentioned as important. In short, the DPO must ensure that his/her organisation has adopted good data governance policies and procedures.

(c) **Audits, data protection by design and privacy impact assessments** – organisations will be required to demonstrate that they have undertaken regular data protection audits and privacy impact assessments (PIAs) using recognised industry standards (such as ICO's PIA criteria). Key to achieving compliance will be an ability to demonstrate that new processing systems and activities

European data protection – what's around the corner and how you can prepare

have been introduced only after privacy compliance and risk mitigation steps have been implemented. A key role of an organisation's DPO will likely be co-ordinating such privacy by design initiatives. Regulators will be empowered to designate processing activities in respect of which organisations should always proactively run a PIA before processing commences. The Regulation sets out a starting point list which includes any activities using data about an individual's "economic situation, location, health, personal preferences or reliability of behaviour".

(d) **Security breach notification** – organisations will have to notify data protection authorities within 24 hours of establishing that they have suffered a data breach or explain why it is not possible to provide full details of the breach. Slick internal procedures will therefore be required to verify suspected breaches and establish what has been lost or subject to unauthorised access.

(e) **Expanded consent requirements** – the EC's proposals include a radical overhaul of the level of consent that is required before organisations process data. At the heart of this change is the requirement that consent to use personally identifiable information should always be obtained *in advance* and *on an opt-in basis* before it is used. Thankfully the EC has pulled back from requiring parental consent to be obtained from under 18 year olds, as required by an earlier draft of the Regulation leaked in November. The bar (in respect of on-line consents only) is proposed at 13 in the draft Regulation published in January.

(f) **Data portability** – individuals will be given the right to demand that an organisation should transfer any or all information held about them to a third party organisation in a format which the individual determines. This increases the control that individuals have over data which identifies them and makes it easier for them to transfer business or employment relationships. It remains to be seen who will be required to cover associated costs of such an exercise, but it seems very likely that the transferring organisation will be expected to do so.

(g) **Jurisdictional reach and supplier responsibility** – the new laws will apply to anyone processing data in the EU as well as those outside Europe who offer goods or services to EU citizens or who "monitor their behavior". For a multi-national organisation, the location of its European HQ will determine which EU Member States' laws bind it, and which regulatory authority will have jurisdiction over it. That said, individuals will be given wider ranging powers to bring action personally against an organisation (either in the country where a non-compliant organisation is located or in the individual's local courts). Trade associations will also be empowered to bring class actions on behalf of their members. For the first time data processors will share equal responsibility and liability for compliance with the new laws raising the stakes for IT service suppliers.

(h) **Data transfers** – Europe's painful data transfer laws will be relaxed in that more options will be made available to enable organisations to share data with non-European third parties. Specifically, the policy implementation known as Binding Corporate Rules will be formalised as a mechanism enabling data transfer compliance, which is good news for multi-site, multi–national businesses.

(i) **The right to be forgotten** – individuals (children, defined as under-18 year olds, are mentioned in particular) will have the ability to demand that information published about them online is deleted and is not republished. Organisations which receive such a demand must take all reasonable efforts to inform other website operators of the existence of the complaint which they have received. The right, which is particularly relevant to social media businesses, is subject to some exemptions. These including one benefiting journalists publishing stories in the public interest, raising the question of whether a blogger or someone who posts an opinion on a website a journalist? But questions remain about how practical the regulation is and who would bear the costs of complying with it.

The EC has set a two year timetable from publication of the Regulations for implementation of its proposals through the European parliamentary system.

Your first steps to compliance

So how should businesses prepare for the tougher standards which they are likely to be expected to meet? Here are our recommended initial points of action. Regardless as to how the EC's proposals are implemented, we already see European regulators encouraging companies to adopt many of the measures which follow.

Step 1: Implement good data protection governance measures

(a) **Appoint a data protection officer (DPO)**– Already a requirement under the laws of some EU Member States (notably Germany), the obligation for private sector organisations of more than 250 employees to appoint a DPO is likely to be the most visible change which results from the review of the current law. DPOs are expected to play a key role in designing a company's data governance program and to have clear access to decision makers and resources in order to do so. They will need to fully understand the obligations imposed by data protection laws and be empowered to stay abreast of developments.

Publication number 13778679

European data protection – what's around the corner and how you can prepare

Points of action
Consider who in your organisation is best suited to fulfil the role of its DPO. Does an existing member of staff fit the bill or will you need to recruit someone?

- If you operate in more than one European country where should your DPO be located? Do you need to have more than one?
- What should your DPO's job specification be? Who should they report to? How will you ensure that the requirements of independence and board access set out in the EC's proposals are facilitated?

(b) **Review policies and procedures** – An organisation's policies and procedures are a key yardstick against which, already, its compliance is judged by regulators. The thought given to both indicate how seriously data privacy compliance is taken. Information provided in policies, whether staff or customer facing, and the practices which they encourage are also at the heart of achieving compliance with two frequently breached principles of data protection law, namely:

(i) **Data security obligations** which require "appropriate technical and organisational measures" to be in place to prevent data loss and unauthorised access to data. In other words, companies need to be well organised when it comes to information security.

Points of action
- Do your current policies clearly guide staff as to what is expected of them when it comes to access to and use of data?
- Identify the most sensitive data that your organisation holds (both as defined by law and as determined by common sense). Are best practice protective measures in place to minimise the risk of loss of that data or unauthorised access to it?

(ii) **Knowledge/consent obligations** which require an organisation to inform its staff, customers and suppliers what data it processes about them, and what it uses that data for. Again, internal and externally facing policies provide a key mechanism for supplying that information.

Points of action
- Are key processing activities sufficiently described in your staff and customer facing policies?
- When were your staff policies last updated? Are they up to date? Have they been future-proofed? For instance, do they include information about all circumstances when your organisation monitors staff activities? More and more businesses are allowing staff to connect their own laptops, tablets and mobile devices to their work networks (a so called 'Bring Your Own Device' approach). If your organisation has done this or is considering doing it, are your staff aware of what data you could access on their devices and are you clear about what your HR and IT departments are, and are not, entitled to look at?

- Are your staff and customer policies clear about circumstances in which data might be shared with other organisations? Failure to have correctly notified and to have obtained consent could make disclosures illegal. Examples of staff data sharing arrangements which provide cause for concern include the following:
  - If data is to be shared with group companies (perhaps with a parent company's HR team as part of an investigation into Bribery Act breach allegations) then affected individuals will need to have been pre-notified of this possibility;
  - Whistle blowing schemes, whether or not implemented under law (including Sarbanes Oxley), are required to be clearly explained in policies and consented to. Some countries' regulators also require scheme details to be approved by them; and
  - When were the website privacy policy and privacy notices that you use in customer facing materials last reviewed and updated? Europe's laws regarding the use of cookies were overhauled in May 2011 to require prior opt in consent for cookies that are not strictly necessary to deliver a service. Is it time to audit what cookies you use and whether you are being sufficiently clear about their use to visitors to your website? See Step 3 below for more on cookie compliance measures.

European data protection – what's around the corner and how you can prepare

(c) **Training** – Regular and well thought through training programs for staff who handle valuable data, whether run online or in person, provide an extremely useful enforcement risk mitigation tool. The existence of a staff training program will not persuade a regulator to cease bringing enforcement action, but it will impress it and assist settlement negotiations. The EC's proposals go further and require organisations, through their DPOs, to organise staff compliance training.

Note: Of the 25 enforcement undertakings issued by the UK data protection regulator (ICO) between 1st July and 30th September 2011, 18 imposed an obligation upon the errant organisation to roll out data protection training sessions to its staff.

Point of action

- Consider developing or purchasing a training program, especially for staff who have access to the most sensitive data held by your organisation. A number of external providers (including Osborne Clarke) offer companies such training programs.

(d) **Audits and Privacy Impact Assessments (PIAs)** – A similar point applies in respect of audits and PIAs. If an organisation can show that it has taken data compliance seriously by running regular audits or a PIA (following, in the UK, ICO's recommended PIA procedure) before introducing significant data processing activities, this will assist its discussions with a regulator should disaster strike. An example of circumstances which lend themselves to an audit or PIA would include an outsourcing (in particular an offshore outsourcing) where valuable data (perhaps HR data) will be accessible by third party providers.

ICO is offering private sector organisations the option to allow it to run an audit of their operations with the incentive that the organisation will be given credit for being open, which should stand it in good stead if a compliance issue were to arise in the future. ICO has the right to require public sector bodies (and their suppliers) to undergo one of its compliance audits and it is not inconceivable that this right could extend to all private sector organisations.

Points of action

- Consider whether activities or processes already active within your organisation would benefit from a PIA to mitigate the risk of regulator action should a data protection breach occur.
- Should you run a data protection audit on all or part of your operations to identify and cure data non-compliance? An audit would also help your organisation demonstrate that it takes data protection seriously should you be the subject of regulator enforcement action in the future.
- A number of security standards now exist, which companies can incorporate into their audit and PIA plans (e.g. the Direct Marketing Association's DataSeal service and The British Standards Institute's data protection compliance standard - BS 10012:2009). Osborne Clarke's data audit team would be happy to help you design your own audit or to run an independent audit of your operations.

(e) **Data transfer compliance** – Europe's current data protection laws prohibit data transfers to destinations which do not have EU strength data protection laws save where specific compliance steps have been taken. Whilst, if implemented, the EC's proposed revisions to those laws would provide businesses with greater options to deal with this prohibition, this remains a difficult area for organisations to achieve compliance. The increasing use of cloud and outsourced solutions and the large number of businesses which have their own overseas operations or share data with third parties overseas means that more and more data is being transferred. Accordingly, it would be sensible to build in to any compliance review a specific assessment of your organisation's data transfer compliance.

Step 2: Supplier / partner audit

A fundamental principle of data protection law has always been that an organisation remains responsible (and liable) for the compliance acts and omissions of its suppliers, even if not culpable for a compliance breach. Many recent regulatory enforcement actions have resulted from situations where a supplier to the organisation which ends up on the receiving end of enforcement action has caused the breach. The EC's proposals to make suppliers as responsible as their customers for such breaches will not change this position – it will likely lead to enforcement action being meted out to both suppliers and their customers.

European data protection – what's around the corner and how you can prepare

The principle of responsibility for a supplier's acts or omissions is also repeated in many important industry codes, such as the Payment Card Industry's (**PCI**) Data Security Standard. Indeed a recent PCI's guidance note on the use of cloud IT services[1] stressed that a company's PCI compliance standing would be jeopardised if its cloud service provider was responsible for a data breach. Given that the ultimate sanction for PCI non-compliance is the withdrawal of rights to use debit and credit payment facilities, this is an extremely important risk issue for many companies. The risk of withdrawal of payment facilities would likely hit an organisation harder than a regulator's fine.

Whilst responsibility for a supplier or a partner's non-compliance cannot be avoided, mitigation measures can be adopted to reduce the fallout of a supplier induced security breach. These include the following:

(a) **Encryption** – European regulators regularly impose onerous and expensive obligations on businesses following a data breach, requiring the adoption of encryption technology at short notice. Accordingly, it is sensible for organisations to review their own internal procedures and policies relevant to staff access to, and protection of, valuable data, and to consider what security measures suppliers have undertaken to meet. Deployment of encryption is advisable where data is transported on portable devices or, in the case of particularly sensitive data (again, "Sensitive" at law **and** sensitive to data subjects), where it is sent by email.

Points of action

- Review your organisation's deployment of encryption. Are portable devices (laptops, tablets, PDAs) encrypted. Do your policies make it clear to staff and suppliers that they should not download personally identifiable data to unencrypted memory sticks and disks?
- It would also be sensible to impose similar assessments and requirements on suppliers who access your organisation's data, including at Request For Tender stage in procurement exercises.

(b) **Service levels** – Data protection laws expressly require companies to have strong written service levels in place with suppliers who are given access to personally identifiable information. A failure to have agreed such measures is viewed in a dim light by regulators when data breaches occur.

Points of action

- Review arrangements with key suppliers who access valuable data. Do they contain strong data protection and security service levels? If not seek to rectify this situation with a side letter agreement.
- Ensure that contracts oblige your suppliers to inform you if data is shared with sub-contractors and/or is sent offshore. You need to be aware of transfers of your data made outside Europe so that you can ensure compliance with EU data transfer laws. You should ensure that data security service levels are passed through to sub-contractors – you may even want to put in place rights to enforce those service levels yourself, for instance using third party rights provisions.

(c) **Data breach notifications** – Laws requiring regulators and those individuals affected by a breach to be notified, should one occur, already apply in some European countries and/or to organisations operating in some sectors (notably financial services and telecoms). But the EC's proposals show a clear intention to formalise these requirements across all organisations. Is your business ready to meet these requirements?

Points of action

- Review key contracts to ensure that your suppliers have been required to proactively warn you if they suspect that they have suffered a data breach (and likewise their sub-contractors). Data breach notification laws impose tight timescales within which regulators and affected individuals should be informed of the breach, so you need to react quickly should data be lost. The EC's proposed new data laws talk of regulators being notified within 24 hours of the breach coming to light (unless a good reason can be given why this is not possible).
- Do you have internal procedures in place to ensure that data loss scenarios can quickly be evaluated and courses of action established? If not should you now develop disaster management plans?

(d) **Supplier due diligence** - If a security incident occurs which involves a supplier, regulators will be interested in seeing what pre-contract due diligence was undertaken on the supplier in question.

[1] see https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

European data protection – what's around the corner and how you can prepare

Points of action

- Review data management questions routinely included in Requests For Proposals. Should improvements be made?
- Check contractual arrangements made with existing key suppliers. Have benchmarking clauses or an obligation to comply with future security best practice been included in long-term agreements?

Step 3: Cookie compliance and other marketing activities

Since May 2011, Europe's new cookie laws have regulated the use of any technology which enables device or internet usage to be tracked. Significantly the laws oblige opt-in consent to be obtained before such technology is placed on a device, unless it is strictly necessary to enable service provision. For many businesses the biggest challenge faced as a result, is how to put in place mechanisms to explain and obtain consent for cookie usage without putting users off visiting their website.

From May 2012 a UK amnesty on enforcement of the new laws will come to an end. Regulators are urging businesses to ensure that their websites are compliant and are threatening enforcement action if steps are not taken.

Steps which should be considered include the following:

a) **Cookie audit** – Assess what cookies are used by your business's website(s) and why they are used.

Points of action

- Create an inventory of tracking technologies used (or likely to be used in the future) and the purposes for which they are used.
- To what extent could it be argued that those uses constitute an activity strictly necessary for the operation of the site? Which cookies are the most intrusive or would a user be most surprised to learn about? The more doubtful you are as to necessity, and the more intrusive or surprising the use, the more likely it is that you should obtain prior consent for its use.
- Grade the technologies that you identify by intrusiveness. The more intrusive, the more likely that regulators will expect clear information to be provided to your users and their prior consent obtained.

b) **Privacy Policies/Notices**

Points of action

- Review what your privacy policy says about the cookies deployed on your site and notices presented to users.
- Customer facing staff in B2C businesses also need to have a clear understanding of what they should say to anyone who enquires what cookies their company deploys and how that information is used.
- Europe's cookie laws are not uniform. To what extent do you operate websites in other EU jurisdictions? Local cookie law advice may be required.

c) **Review marketing activities**

Points of action

- Other marketing activities which often trip organisations up and which should therefore be assessed are as follows:
  - Trying to persuade 'opt outs' to change their mind: contacting customers who have opted out of receipt of marketing materials by email to enquire if they would like to change their minds and opt in to future mailings.
  - List purchase: buying lists, in particular email addresses, without checking and obtaining contractually binding confirmation that those named have given sufficient consent to enable marketing materials to be sent to them. In the UK, consumer focused email and SMS marketing for a third party's products or services may only be sent to those who have opted in to its receipt. In some European countries opt in is also required for unsolicited marketing sent to business recipients.
  - Minors: care also needs to be taken when marketing to minors.

European data protection – what's around the corner and how you can prepare

Conclusion

Europe's law makers are sending a clear signal to businesses that they will be expected to demonstrate how seriously they take data protection compliance.

Yes, there will be costly compliance measures and, potentially, eye-watering fines of up 2% of worldwide turnover for data compliance failures. But, for many businesses, there will also be considerable upsides.

By taking the right actions your business can start to benefit from the positive effects of good data governance right now. These include avoiding regulator enforcement action, satisfying public demands that well-run businesses respect customer data and, by no means least, demonstrating to shareholders that you have data governance covered.

Taking even a few of the measures detailed in this paper will enhance the value of your data as a business asset. Perhaps even more importantly, following our suggested action plan will send a powerful message to your shareholders and customers, helping your on-going efforts to build all-important trust in your brand.

Contact

If you would like to discuss any aspect of data protection compliance, please contact James Mullock, partner and head of Osborne Clarke's Information Law Group.

James Mullock
T +44 (0)117 917 3322
F +44 (0)117 917 3324
E james.mullock@osborneclarke.com

About Osborne Clarke

We are known for our ability to turn legal expertise into commercial advantage for our clients by applying imaginative thinking to their issues and challenges.

With over 700 staff and 112 partners, we have offices in the City of London, Bristol and Thames Valley, Cologne and Munich and Silicon Valley in California.

Publication number 13778679