The draft Data Protection Regulation (the Regulation) proposes to overhaul the existing European data protection regime and introduce a number of fundamental changes. A key proposal of the draft Regulation is the introduction of a time-sensitive mandatory breach notification to the supervisory authority in each member state. All data controllers will be required to report a data breach to the relevant supervisory authority without undue delay, which is described as “presumably within 72 hours” (based upon the current proposed draft). Furthermore, where a personal data breach is likely to adversely affect the protection of the personal data, privacy rights or legitimate interests of the data subject, the controller must communicate the data breach to the data subject without undue delay.

With these new obligations, European legislators are trying to address growing concerns amongst European citizens about the safety of their personal data, and in particular, their financial data. This takes place against the backdrop of increasing numbers of data breaches and hackings. Recent examples include the eBay data breach of May 2014 during which hackers exposed the data of nearly 150 million eBay users and the recent Jennifer Lawrence’ Apple iCloud hacking in September 2014, which resulted in a large amount of data records in the Apple iCloud being compromised and the publication without consent of a number of nude celebrity photos. Needless to say that such a breach is a company’s worst nightmare, which can lead not only to a substantial costs, including fines in certain jurisdictions (such as the US), but may also cause serious reputational damage. The latter may affect, over time, the profitability of a company more than any monetary hit which may immediately follow a data breach or hacking incident.

This article will examine the current requirements for breach notification (or lack thereof) under the Data Protection Directive (the “Directive”) and other laws, the proposed changes under the Regulation, and practical steps companies should consider in anticipation of the new legislation.

**Breach Notification Today**

The current Data Protection Directive does not contain mandatory data breach notification requirements and the Data Protection Act 1998 is silent on this point. However, a large number of European data protection authorities, as well as the EU Article 29 DP Working Party, have recognised that current legislation is lagging behind, and issued non-binding guidance urging data controllers to notify serious data breaches and incidents and defining levels of seriousness. In the UK, the Information Commissioner’s Office (the ICO) recommends data controllers report any serious data breaches, without specifying a time period, to enable the ICO to offer specific guidance as to the management of any adverse consequences. In practice, however, data controllers have been reluctant to air their dirty laundry in public, and tend to treat information about data breaches as confidential unless the facts have become public through the press or due to a mandatory notification to another regulator.

However, breach notification in itself is not a new concept. In the US, health care data is tightly regulated by a federal national health privacy law, mandating governmental and individual notifications if there is a security breach of individually identifiable information in the custody of health care providers or payment processors. More broadly, more than 45 states have laws requiring private or government entities to notify individuals, credit bureaus, and/or regulators of security incidents which involve specific categories of data, going from generally personally identifiable information, particularly where the affected data set was unencrypted and therefore more susceptible to exploitation by identity thieves or other bad actors. These laws typically have provisions regarding which types of data are covered, who must comply with the law, what specifically constitutes a reportable breach, and when the requirements for notice is triggered, including the timing, contents, and method of notice. Because data breaches are in point of fact the companies handling personal data have practicalities of preserving evidence, which included workload lists, file notes and template documents but still contained sensitive personal data, in his new role.

The ICO emphasises that this is a criminal office under section 55 of the DP Act. In this case, the data theft resulted in a fine of £300, a £30 victim surcharge and £438.63 prosecution costs. 

Laura Linkomies

---

**EVEN THE BEST PREPARED COMPANIES ARE VULNERABLE TO DATA BREACHES**

No matter how good your organisation’s data security, there is always a threat posed by employees as they are often the weakest link in an organisation’s data protection procedures and practices. The ICO recently warned organisations about employees that steal their employer’s personal information when changing jobs. Earlier this month, a paralegal, who previously worked at Jordans Solicitors in Dewsbury, Yorkshire, was prosecuted for illegally taking the sensitive information of over 100 people before leaving for a rival firm in April 2013. The information was contained in six emails sent by James Pickles in the weeks before he left the firm, the ICO says. Pickles had hoped to use the information, which included workload lists, file notes and template documents but still contained sensitive personal data, in his new role.

The ICO emphasises that this is a criminal office under section 55 of the DP Act. In this case, the data theft resulted in a fine of £300, a £30 victim surcharge and £438.63 prosecution costs.

Laura Linkomies
matching the right forensics investigators to the circumstances of the breach, and communicating with affected parties and regulators. For European companies facing the prospect of very short mandatory notification periods, there is much practical learning available in the US market, from a selection of vendors and counsel, to managing compliance and notifications.

Closer to home, European telecommunication service providers have been obliged to notify regulators in cases where they suffer a data breach. This obligation was introduced in an amendment to the e-Privacy Directive and transposed to the UK via an amendment to the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426). Regulation 611/2013 has been published as a supplement to the e-Privacy Directive, setting out measures which require providers of publicly available electronic communications services to notify, in the event of a data breach, the relevant national authorities and in certain cases, the subscribers and individuals whose personal data has been affected. Under Regulation 611/2013, the service provider must, where feasible, notify all personal data breaches to the competent national authority no later than 24 hours after the detection of the personal data breach. Detection of a breach is deemed to have taken place when the service provider has sufficient awareness that a security incident has occurred that led to personal data being compromised. The service provider must notify the subscriber or individual whose data has been affected if the breach is likely to adversely affect the personal data or privacy of the data subject unless certain exemptions apply. In the UK, the ICO website provides clear and concise guidance for telecommunications and Internet service providers in respect of the notification requirement, including a downloadable template log to assist service providers in keeping tracking of personal data breaches and a downloadable security breach notification form.

In addition, the European legislators recently included data breach notification requirements in the latest draft of the EU Cybersecurity Directive which require so-called “market operators”, i.e. providers of information society services and operators of critical infrastructure in the fields of energy, transport, banking, stock exchanges and health, to report security incidents.

Further, in the UK specifically, there are also breach notification requirements in other fields of law. For example, principle 11 of the Financial Conduct Authority (FCA) Handbook requires that financial services organisations regulated by the FCA disclose to the appropriate regulator anything relating to that firm of which the regulator would reasonably expect notice, which has at times been taken to include a major data breach. FCA fines may be especially onerous for financial institution who do not properly protect data – the highest on record is a £2.3 million fine to the UK branch of Zurich Insurance for loss of an unencrypted backup tape.

EU DP REGS – NEW BREACH NOTIFICATION REQUIREMENTS

The current proposal for the EU Regulation states that any data controller must report a data breach to the supervisory authority without undue delay. In the recitals to the Regulation, it is specified that “undue delay” is presumed to be no more than 72 hours. If a breach is likely to adversely affect the personal data or privacy interests of the data subject, those data subjects should also be notified without undue delay. In the Regulation, a “personal data breach” is defined as “the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. In addition, the Regulation specifies that a “breach which adversely affects the personal data or the privacy of the data subject” as a breach which could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification to the supervisory authority must at least (1) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (2) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (3) recommend measures to mitigate the possible adverse effects of the personal data breach; (4) describe the consequences of the personal data breach; and (5) describe the measures proposed or taken by the controller to address the personal data breach and mitigate effects. The latest version of the relevant clause now provides that this information may if necessary be provided in phases. If a notice to data subjects is required, this communication must be comprehensive, use clear and plain language and must describe the nature of the personal data breach as well as including the parts of the notification to the supervisory authority described in (2) to (4) above and describing the rights of the data subject, including how their right to redress can be exercised.

The data breach notification requirement has been a part of the wider debate surrounding the new Regulation. Professional lobbying groups, such as Digital Europe, have proposed a watering down of the notification requirement to cover only “material” breaches and remove the time limitation. Many organisations, from the Royal Mail to the European Banking Federation, objected to the 24-hour deadline for breach reporting in previous drafts of the new Regulation. Telefonica has proposed that there needs to be further clarification of the definition of “personal data breach” so that the mandatory reporting requirements will only extend to cases where the breach is due to the fault of the data controller, as opposed to a breaches where the data subject voluntarily grants access to the deceptive activity, for example, phishing. Telefonica also noted that there is a potential for “notification fatigue” on the part of businesses and proposes instead that businesses should create an internal log of data breaches that may be viewed at any time by the supervisory authority.

The UK government assessed the proposals made by the European Commission in June 2013. While the European Commission predicts that harmonisation of the European data protection laws will bring savings totalling €2.3 billion each year, the UK
The costs of the new notification requirements are especially significant in light of the fact that the Regulation also abolishes the fee that all data controllers are required to pay the ICO, a potential loss of £15 million income.\textsuperscript{15} This debate has caused the data breach notification clauses in the draft Regulation to keep evolving. The current draft has continued to generate much discussion on scope and application. For example, whilst European legislators seem to have had large security breaches and hackings in mind when drafting, small-scale breaches, such as a letter sent to the wrong address, would also be caught by the current drafting and need to be notified. If the drafting stays as it is, the new obligation would cause an avalanche of notifications to the supervisory authorities, drowning them in extra administrative work. According to leading practitioners in the field, this may lead to an overload of administrative work for the supervisory authorities negatively impacting the time and attention necessary to address the large data breaches with a serious impact on data subjects’ rights and interests.

In addition, data breaches are often less straightforward than envisaged by the current draft. In most cases, the real cause of a breach, and sometimes even the fact that a breach has taken place, will only emerge after thorough investigations have taken place. As a factual matter, the 72-hour window will prove quite challenging in practice. It may not be possible to identify the relevant experts, and have them present at the breach site within 72 hours, or make serious headway analysing log data, scanning the network, and rendering a sensible judgment about breach impact. Also, every data breach is different, and the first forensic assessment of the key facts about who is potentially acquired what personal or sensitive data, is very often wrong, even though the sales, valuation, and reputational stakes are potentially extremely high. In crafting notification strategies, there are many stakeholders to consider – from supervisory authorities to customers and shareholders to law enforcement, financial regulators, private attorneys, policymakers, and media. As currently drafted, it is also not clear how soon notification should take place as the current draft does not specify when the 72-hour period will start running. In addition, the 72-hour period is now stated in the Recitals which means that this is merely an interpretative guide of the meaning of “undue delay”, as Recitals explain the reasoning behind a measure and can be used for interpretation but are not part of the (binding) legislative text of the Regulation. The European Parliament seems also to have toned down the time period even further by using the word

\begin{center}
\textbf{REFERENCES}
\end{center}

\begin{tabular}{|l|}
\hline
1 Proposal for Regulation COM (2012)0011 of the European Parliament and the Council of 25 January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation; the most current version of the text was the compromise text adopted by the European Parliament on 12 March 2013. A comparison between previous and current versions of the Data Protection Regulation is available at www.europarl.europa.eu

2 Previously 24 hours in the European Commission’s draft; this time period has been removed from Article 31, and replaced with “undue delay”. The 72-hour window is now specified in Recital 67, whereby the Parliament seems to attempt to meet a number of concerns in various industries about the strict timeframes for notification. Being 24 hours is not always practical, as demonstrated by data breaches in the banking sector, where the 72-hour window was insufficient.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The current draft has continued to generate much discussion on scope and application. For example, whilst European legislators seem to have had large security breaches and hackings in mind when drafting, small-scale breaches, such as a letter sent to the wrong address, would also be caught by the current drafting and need to be notified. If the drafting stays as it is, the new obligation would cause an avalanche of notifications to the supervisory authorities, drowning them in extra administrative work. According to leading practitioners in the field, this may lead to an overload of administrative work for the supervisory authorities negatively impacting the time and attention necessary to address the large data breaches with a serious impact on data subjects’ rights and interests.

In addition, data breaches are often less straightforward than envisaged by the current draft. In most cases, the real cause of a breach, and sometimes even the fact that a breach has taken place, will only emerge after thorough investigations have taken place. As a factual matter, the 72-hour window will prove quite challenging in practice. It may not be possible to identify the relevant experts, and have them present at the breach site within 72 hours, or make serious headway analysing log data, scanning the network, and rendering a sensible judgment about breach impact. Also, every data breach is different, and the first forensic assessment of the key facts about who is potentially acquired what personal or sensitive data, is very often wrong, even though the sales, valuation, and reputational stakes are potentially extremely high. In crafting notification strategies, there are many stakeholders to consider – from supervisory authorities to customers and shareholders to law enforcement, financial regulators, private attorneys, policymakers, and media. As currently drafted, it is also not clear how soon notification should take place as the current draft does not specify when the 72-hour period will start running. In addition, the 72-hour period is now stated in the Recitals which means that this is merely an interpretative guide of the meaning of “undue delay”, as Recitals explain the reasoning behind a measure and can be used for interpretation but are not part of the (binding) legislative text of the Regulation. The European Parliament seems also to have toned down the time period even further by using the word

\begin{center}
\textbf{REFERENCES}
\end{center}

\begin{tabular}{|l|}
\hline
1 Proposal for Regulation COM (2012)0011 of the European Parliament and the Council of 25 January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation; the most current version of the text was the compromise text adopted by the European Parliament on 12 March 2013. A comparison between previous and current versions of the Data Protection Regulation is available at www.europarl.europa.eu

2 Previously 24 hours in the European Commission’s draft; this time period has been removed from Article 31, and replaced with “undue delay”. The 72-hour window is now specified in Recital 67, whereby the Parliament seems to attempt to meet a number of concerns in various industries about the strict timeframes for notification.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The current draft has continued to generate much discussion on scope and application. For example, whilst European legislators seem to have had large security breaches and hackings in mind when drafting, small-scale breaches, such as a letter sent to the wrong address, would also be caught by the current drafting and need to be notified. If the drafting stays as it is, the new obligation would cause an avalanche of notifications to the supervisory authorities, drowning them in extra administrative work. According to leading practitioners in the field, this may lead to an overload of administrative work for the supervisory authorities negatively impacting the time and attention necessary to address the large data breaches with a serious impact on data subjects’ rights and interests.

In addition, data breaches are often less straightforward than envisaged by the current draft. In most cases, the real cause of a breach, and sometimes even the fact that a breach has taken place, will only emerge after thorough investigations have taken place. As a factual matter, the 72-hour window will prove quite challenging in practice. It may not be possible to identify the relevant experts, and have them present at the breach site within 72 hours, or make serious headway analysing log data, scanning the network, and rendering a sensible judgment about breach impact. Also, every data breach is different, and the first forensic assessment of the key facts about who is potentially acquired what personal or sensitive data, is very often wrong, even though the sales, valuation, and reputational stakes are potentially extremely high. In crafting notification strategies, there are many stakeholders to consider – from supervisory authorities to customers and shareholders to law enforcement, financial regulators, private attorneys, policymakers, and media. As currently drafted, it is also not clear how soon notification should take place as the current draft does not specify when the 72-hour period will start running. In addition, the 72-hour period is now stated in the Recitals which means that this is merely an interpretative guide of the meaning of “undue delay”, as Recitals explain the reasoning behind a measure and can be used for interpretation but are not part of the (binding) legislative text of the Regulation. The European Parliament seems also to have toned down the time period even further by using the word

\begin{center}
\end{center}
“presumably” which indicates that there may be exceptions to this rule.

These ambiguities in the current draft of the Regulation lead us to think that the text of the data breach notification provisions is not yet final, and that further changes are still to be made, or interpretative guidance to be issued to clarify the what, how, and when of notifying data breaches under the Regulation. In a July 2014 note, the Italian Presidency of the Council of the European Union invited delegations to confirm that the proposed risk-based approach, where businesses would not have to notify individuals of every single data security breach, still meets their views\(^1\).

**PRACTICAL STEPS TO PREPARE FOR THE NEW REGULATION**

Until further clarification is provided, it will be difficult for data controllers to prepare for the specific characteristics of the Regulation's reporting obligations. However, it seems clear that a mandatory data breach reporting obligations of some sort is on its way in Europe and it is therefore important that companies start preparing for this fact. Companies in Europe will need to ready their processes and procedures to prevent, address and promptly notify any data breach and to prevent or mitigate its consequences.

This can be done by setting up a global all-encompassing data breach response plan, specifying an internal response team of board members, alongside legal, IT security and press liaison representatives. Companies should consider interviewing and selecting external forensic, crisis management, and legal advisors available who can investigate the breach or assist and advice on the legal or strategic aspects of taking decisions. In addition, the written plan should set out the steps that need to be taken to investigate the breach, and mitigate/respond to both the breach and the consequences. Every member of the internal response team should have his or her own action plan for assessing, mitigating and responding to certain types of risk. As soon as such a plan is put in place, the plan will need to be practised, hopefully through data breach simulation exercises, and continuously improved and updated. By having such a plan in place and having trained staff through table top exercises, companies will be well ahead of the game when the provisions of the new Regulation are finalised and they will be ready to deal with security incidents and data breaches.

**ICO to MoJ: More balanced DP debate needed**

In its response to the Ministry of Justice’s call for evidence on the review of competencies between the UK and the EU on Information Rights, the ICO said data protection compliance is still regarded by some businesses and organisations, particularly SMEs, as a complex activity. This complexity is sometimes ascribed to data protection’s EU basis. However, the ICO explains that the UK would require comprehensive data protection legislation to trade in the globalised economy, whether it was part of the European Union or not.

The Commissioner believes the challenges we face today would probably exist regardless of the basis of the law. The Commissioner said that he is neutral on the question of whether a Regulation is the best form of legislative instrument; there are benefits of both options and both could successfully deliver the desired data protection framework.

“Our focus is on the text rather than the form. The debate about the benefits, costs and burdens of the proposal has become highly polarised, with some of the estimates on both sides hard to justify, including the figure for the benefits proposed by the European Commission,” the ICO says. A more balanced debate is needed.

The ministry’s consultation closed in July. A report on the Balance of Competences on Information Rights and what this means for the national interest is due to be published by the end of 2014.

---

**AUTHORS**

Lore Leitner and Frances Stocks, Associates, Latham & Watkins LLP.
Emails: Lore.Leitner@lw.com
Frances.Stocks@lw.com

---

**Privacy Laws & Business recruitment service**

*Privacy Laws & Business* specialises in placing skilled data protection and privacy staff in permanent or contract positions, including short-term projects. We can recruit for all types of vacancies ranging from global to Europe, Middle East, Africa and UK roles.

Having established a leading presence in the data protection and privacy recruitment market, we offer an unrivalled service to our clients. *Privacy Laws & Business* has become market leader because unlike other recruitment agencies, we understand data protection and privacy.

For further information, visit [www.privacylaws.com/recruitment](http://www.privacylaws.com/recruitment) or contact Glenn Daif-Burns on tel: +44 (0)20 8868 9200 or email: glenn@privacylaws.com

---