computing.co.uk

Print this page
Save to disk

Protect and survive: an essential guide to data protection regulation

08 May 2012, Andrew Charlesworth, Computing

http://www.computing.co.uk/ctg/feature/2172099/protect-survive-essential-guide-protection-regulation

Data privacy has been more in the spotlight than ever recently, with potentially game-changing announcements from both sides of the Atlantic. These have ramifications for any organisation holding personal data.

Viviane Reding, vice-president of the European Commission (EC) and EU Justice Commissioner, announced the overhaul of the EU's Data Protection Directive on 22 January 2012, billing the move as "a fundamental reform of the common European rules that govern the free movement of personal data in Europe's single market and the best possible protection of such data in the digital age".

A month later, the White House announced that the US government is to draw up a Privacy Bill of Rights, trumpeted as "a comprehensive blueprint to improve consumers' privacy protections and ensure that the internet remains an engine for innovation and economic growth".

The UK government, meanwhile, has announced its determination to have far greater access to citizens' data. In such a complex environment, clearly, the CIO needs to remain in the driving seat of any organisation's policy.

"There is no doubt that the new data protection proposals will impact all aspects of data handling, irrespective of whether that data relates to staff or customers," Vinod Bange, partner and data protection law expert at Taylor Wessing, told *Computing*. "CIOs will need to be aware of this impact, and the consequences along the whole data lifecycle."

"Tougher rules around data collection, consent and transparency will challenge the lawful basis for collecting the data in the first place and potentially encourage a regulatory environment geared towards data minimisation," Bange adds.

"This may mean that CIOs will need to revisit current data classification policies …to ensure such policies correctly capture all information that should be regulated."

Europe first

EU data protection regulations were formulated in 1995, the year Facebook's Mark Zuckerberg celebrated his 11th birthday. The majority of consumer internet connections were dial-up, and cloud was a meteorological phenomenon. Scott McNealy, then chief executive of Sun Microsystems, achieved brief notoriety by saying: "There is no such thing as privacy on the internet. Get over it."
Since then, personal data has become a currency that consumers trade for services. Surrender your name, email address, date of birth, job title, education, location, photos, purchasing choices, holiday destinations, likes, and dislikes – and you can play with your acquaintances online.

The EC is keen to dispel any notion that the General Data Protection Regulations will stifle online innovation, and is presenting them as an enabler of e-commerce. The EC wants to create a single digital market across member states. To achieve that, Europe needs a single set of data protection regulations.

"Like any currency [personal data] needs stability and trust," says Reding. "Only if consumers can trust that their data is well protected, will they continue to entrust businesses and authorities with it, buy online, and accept new services."

But this isn't just about keeping credit card details safe. By addressing the trust underlying ecommerce, the new rules throw a wide net. The Commission has widened the definition of personal data, so more elements of information will fall under the regulations, says Bange.

"Detailed rules around data collection and use will be just as important as the strategic decisions on global data flows," he adds. "Failure at either end of the data regulatory spectrum will now attract much tougher penalties, so CIOs can ill afford to ignore this."

The Commission's proposed changes introduce a number of new measures (PDF). Fundamentally, they take control from the data collector and hand it to the data subject.

"The new proposals will shift power into the hands of individuals," says Jonathan Nugent, data protection specialist at PwC Legal. "In theory, once the proposals are implemented it should be much easier to access, move or delete whatever personal data companies hold on you."

Among the powers individuals will have over their data are the rights to portability and deletion – the right to be forgotten.

The right to data portability will make it easier for users to move to a different provider since their switching costs will be effectively reduced, says Lukas Feiler, associate at Wolf Theiss law firm in Vienna and a fellow at Stanford University and the University of Vienna Transatlantic Technology Law Forum (TTLF) and Forum on Contemporary Europe (FCE).

The right to be forgotten means a data subject could withdraw consent to the processing of his or her data at any time. "Once consent has been withdrawn the data has to be deleted," Feiler says.

Regulate to save

The EC estimates the new regulation will save businesses around €2.3bn a year. But all companies that handle personal data and employ more than 250 people will have to appoint a corporate data protection officer (CDPO), as they already do in Germany. Feiler reckons this role will fall to the CIO in many organisations.

The main financial saving, argues Reding, will come from the fact that pan-European data handlers will have to deal with only one set of rules and one data protection authority – the one in their country of origin. In the UK, that is the Information Commissioner's Office (ICO). Supposedly, all member state's authorities will apply the law consistently.

"One of the biggest flaws with the current regime is that it does not deal well with businesses operating across more than one country," Guy Wilmot, solicitor at Russell-Cooke Solicitors told Computing. "Once the regulation is enacted, businesses operating in more than one EU country will have the comfort of operating with one set of rules and will be able to deal with one regulator," he adds.

Fines and punishment

Critics of the regulations have been quick to highlight the fines the EU wants to levy on organisations in breach of the new regulations – up to two per cent of annual worldwide turnover. An early draft pitched the ceiling for fines at an eye-watering five per cent.

But what is more likely to be a shock to European companies is the level of transparency required by the new regulations. Companies that suffer a data leak must inform the data protection authorities and the individuals concerned – as they already have to do in some US sectors – "without undue delay", a phrase Reding handily translates as "within 24 hours".

"That's going to be tough for some companies to adhere to," says Lisa Banyard, PwC data protection leader. "Those that don't already have a well-oiled reporting mechanism in place will need to implement measures to flag breaches in time."

Fit for purpose?

The proposed overhaul of the Data Protection Directive was adopted by the Commission on 25 January. Inevitably, it has been subject to concerted lobbying from data handling companies who think it places onerous burdens on them.

More significantly, the proposals were given a thorough drubbing by Europe's independent Data Protection Supervisor (EDPS), Peter Hustinx. He called the EU's proposed rules governing how law enforcement agencies will handle personal data "unacceptably weak".

Hustinx found numerous other holes: a lack of legal certainty about how law enforcement will be allowed further use of personal data beyond the initial purpose for collecting it; possible derogation for transferring data outside the EU; and the excessive power vested in the European Commission's role to enforce consistency of data protection rules at the expense of member-state data protection officers.

"We are unfortunately still far from a comprehensive set of data protection rules on national and EU level in all areas of EU policy," he concluded.

This stinging critique doesn't mean the overhaul of the regulations won't happen. It's just transparent

democracy in action. The broad intent to harmonise EU data protection measures still stands.

Besides, companies will be foolish to oppose the new EU regulations, says David Bradshaw, research manager for SaaS and cloud at analyst firm IDC.

"Critics have focused on the stick – the implications if companies don't abide by these new regulations," he told Computing. "But they've ignored the carrot of Germany, where most of these regulations are already in place.

"Germany is the EU's biggest market, and by complying with these regulations companies will be able to operate in the lucrative German market," Bradshaw adds.

Transatlantic data traffic

When they come into force, the European regulations will cover not just European organisations, but all bodies that process the data of European citizens. That means companies from outside the EU will have to comply with the regulations if they want to do business in the EU that involves handling personal data.

"Companies that target the EU market will need to consider their existing data handling procedures and assess the extent to which they meet the EU's proposed rules," says Chris Watson, head of telecoms at law firm CMS Cameron McKenna.

However, how the EU will enforce its regulations on non-EU entities still needs to be addressed, Watson adds.

The need to enforce regulations made in one territory on companies operating across several will result in greater international co-operation in enforcement, says Wilmot.

"The price to be paid for this clarity and harmonisation is that the enforcement regimes on both sides of the Atlantic will be 'beefed-up'," he says.

EU regulators have already started to act in unison. By way of example Wilmot points to the way in which Europe's data protection regulators coordinated their response to Google's new privacy policy, allowing the French regulator to take the lead.

With data regulation becoming more extra-territorial than ever, the regulatory environment will tend to flow with the data, says Bange.

"Where CIOs have ownership of data estates straddling either side of the Atlantic, it's hard to see how that data will not be pooled, especially where lines of business span geographical borders," he says.

"The question is whether CIOs are ready to address the increasing data regulation that is also pooled with the data, and flows with the data, whichever side of the Atlantic the data touches," he adds.

Back in the late 1990s, lengthy negotiations between the EU and US led to the Safe Harbour provisions (which also include Switzerland) and act as a framework for sharing data between the two regions. But ever since the terrorist attacks on 11 September 2001, the US has put emphasis on security above privacy.

The US Patriot Act was implemented in the aftermath of September 11 by the US government to fight international terrorism, and it means the US can obtain data from European companies that have their data stored in US owned datacentres, even if the datacentres are on EU soil.

The EU's proposed General Data Protection Regulation "raises the stakes in the ongoing privacy-versus-security debate between the EU and the US," says Feiler.

"The EU's draft proposal of a General Data Protection Regulation would make clear that so-called National Security Letters (NSL) issued by the FBI pursuant to USA Patriot Act Section 505 are not to be recognised in the EU," he adds.

"For any US company to disclose personal data of EU residents pursuant to a NSL, an approval by the data protection authority of an EU member state would have to be obtained first. Companies that fail to do so would be subject to fines of up to two per cent of their annual worldwide turnover."

Stateside moves

The proposed US Consumer Privacy Bill of Rights is one of four elements of a report, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (PDF), announced by the White House in February.

The other elements include a stakeholder-driven process to specify how these rights apply in particular business contexts; enforcement by the Federal Trade Commission (FTC); and greater privacy interoperability between the US and international partners.

"The [Bill] recognises that privacy is not a 'one size fits all' proposition as its central feature is the call for multiple-stakeholder groups to establish industry-specific or technology-specific codes of conduct," Chris Wolf, Washington partner of Hogan Lovells, told *Computing*.

Indeed, the US and EU measures show a fundamentally different approach to privacy, say legal experts.

"The rules in the US might be more flexible, especially in relation to issues like consent," says Wilmot. "The US may allow more data processing without explicit consent, provided that the processing is consistent with the context in which the data was collected."

The Bill says that at the time of collection, companies should present choices about data sharing, collection, use, and disclosure that are "appropriate for the scale, scope, and sensitivity of personal data in question", irrespective of whether the company uses the data itself or discloses it to third parties.

So the regulations will be more stringent for search engines and social networks that build detailed profiles of individual behaviour which may contain sensitive information, such as personal health or financial data.

Here the Bill calls for user privacy options that are simple, prominent and offer fine-grained control of personal data use and disclosure. But services that do not collect information that is reasonably linkable to individuals will be free to offer more limited privacy options.

Despite its name, the US Bill does not have the force of law, says Feiler. Rather, it is a form of self-regulation specific to the online sector only.

"Companies will be free to declare compliance with [the Bill] and only if they do will the FTC be able to sanction violations as a deceptive business practice under FTC Act Section 5," he says. "[The Bill] is only a set of vague principles that still have to be implemented by codes of conduct … specific to particular types of companies."

Today America, tomorrow the world

Are we now entering a time when global laws will finally catch up with global data traffic? The proposed EU and US data protection policies certainly have global elements to them, says Watson.
Economic reasons – as well as looking after the interests of citizens – are driving the move, says Conor Ward, partner at Hogan Lovells and chair of the recently formed Cloud Industry Legal Forum.

"Inadequate protection will affect [a country's] ability to trade internationally as it becomes difficult for firms to transfer data through that country," he adds.

Ward points out that the UK's 1984 Data Protection Act was passed in response to a lost business opportunity to print credit cards because customer data could not be sent to the UK as it would not be protected.

Some Asian countries have had data protection and privacy laws for some time: Hong Kong (1996), India (2000), Japan (1995), Australia (1988) and New Zealand (1993).

"Some of these offer more protection than in Europe," says Ward. "For example, the Australia Act applies to data collected anywhere relating to Australian citizens."

There has been a flurry of activity across Asia in the last year or so, with laws either updated or, in countries which do not have such laws, proposed for the first time. Again, some of these changes go further than the European equivalents.

Feiler is less ebullient about global co-operation. "The US is continuing its path of sector-specific self-regulation, which has produced questionable results in the past and fundamentally differs from the approach in the EU," he told *Computing*.

His book, *Information Security Law in the EU and the US*, published last year, takes a risk-based approach to analysing cyber security regulation on the two continents and makes recommendations for how regulation could be tightened to improve security.

"In light of these fundamental differences of what it means to 'regulate' privacy, it seems unlikely that a common global standard will emerge anytime soon," he says. "However, as a generation of digital natives is growing up, data privacy is becoming a top political priority worldwide."

The CIO of a global business will benefit from increasing consolidation of data protection laws in Europe, but will still face varying levels of regulation across the globe.

"Planning ahead for fluid movement of data within global organisations means taking a more holistic approach to data laws," says Bange.