Number 87

socitm insight

briefing

... a Socitm *Research* service

Data protection: <Control><All><Delete>?

Preparing for anticipated changes in data protection legislation is a timely topic this month. In January the European Commission (EC) unveiled the newly agreed draft European Data Protection Regulation to replace the current Data Protection Directive 95/46/EC. The three month hiatus caused by the European Court of Justice (ECJ) striking down the Safe Harbour agreement with the USA was resolved by a new EU-US Privacy Shield. What do these changes mean for the UK public sector?

No harbour is safe

Following the revelations by Edward Snowden about American snooping, in October 2015 an Austrian privacy campaigner, Max Schrems, mounted a legal challenge in Europe's highest court, the ECJ, to the Safe Harbour Agreement that operated between the European Union (EU) and the United States. The Safe Harbour agreement, signed in 2000, bridged cultural and political differences regarding online privacy. The EU sees protection of personal data as a human right, while America considers it mainly in terms of consumer protection; these different approaches provide opportunities for ambiguous interpretations. The agreement allowed firms to transfer data from the EU to America if they provided safeguards equivalent to those required by EU Directive 95/46/EC. When it was negotiated, transatlantic data flows were relatively small. Accordingly, the EC accepted an agreement based on self-certification: firms could write a privacy policy and declare themselves compliant.

The ECJ struck down the agreement, arguing that "legislation permitting [American] public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." The judges also ruled that national data protection authorities within the EU do have the right to independently examine organisations that transfer personal data to the US. In short, local data protection regulators were not absolved from their responsibility to protect their citizens' data by Safe Harbour.

That ruling appears to have triggered legal proceedings by an advocacy group called Digital Rights Ireland against the government of the Irish Republic and its data protection commissioner for failing to implement the EU's Directive, or to ensure that the Irish Data Protection Commissioner was independent of the government: one of the fundamental human rights of the European Union. Legal challenges like this impact the UK because many American technology companies and cloud service providers used by UK businesses and public services are based in the Irish Republic, and may store the data in the US (or elsewhere) and are subject to the USA PATRIOT Act (Act of Congress, entitled 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001'). UK cloud service users and suppliers must, of course, comply with the UK Data Protection Act's eighth principle: "Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

EU-US Privacy Shield (a.k.a. Transatlantic Privacy Shield)

In January 2014, after Edward Snowden's revelations, Barack Obama announced new measures giving foreigners' data some legal protections, including the establishment of a US data ombudsman and the right for Europeans to have access to legal redress in US courts. However, at this stage, the Privacy Shield framework is a political agreement between the EU and US, and not yet a legal one. European Commission and US negotiators are working on the implementation details now. This may prove difficult. The Irish High Court findings were that the US was engaged in "indiscriminate mass surveillance" through Prism, a programme brought under the spotlight by the Snowden revelations, that gives the US access to an individual's internet activities through agreements with technology companies including Microsoft, Google, Facebook, Yahoo, YouTube and Skype. Computer Weekly quoted a London solicitor: "Without cancelling Prism there can be no new agreement".

Questions remain over the practicalities of the Shield; principally, what is the point in Europeans having judicial redress if they cannot prove that their data has been spied upon? European privacy activists question whether an US government agency that operates in secret can be trusted to follow any agreement.

The Economist newspaper opines that the new deal will be tested in the ECJ but, if the ECJ tells the court that US privacy protection is now adequate, it will be difficult for judges to argue otherwise.

Operationally, it looks like it will be at least as safe as before for UK public services to use US cloud service providers.

EU data protection reforms

The new General Data Protection Regulation (GDPR) comes into force in about two years. As a regulation and not a directive, it will be automatically enshrined in UK law under EC Treaty (Article 249) and supersedes previous legislation that implemented EU Directive 95/46/EC. It updates the law to accommodate technologies and trends that were scarcely apparent when the UK's own Data Protection Acts were drafted in the mid-1990's, such as pervasive online business transactions, social media and cloud computing. The new legislation is a long time coming – it is now over a year behind schedule – and we still only have a draft set of proposals to work with. As well as bringing legislation up to date for the digital age, the new regulation harmonises the legal framework across Europe. The underlying principles are to:

- increase digital security for individuals
- make the data protection legislation suitable for the digital age
- ease business by reducing bureaucracy and harmonising legislation across all EU member states.

Importantly, the new laws apply to those companies based outside the EU which store and process the personal data of all those resident within the EU.

Two instruments

In detail, the proposed reforms to the EU data protection legislation consist of two instruments:

- The **General Data Protection Regulation**, enabling individuals to have better control of their personal data. The aim is also for a modernised and unified set of rules to allow businesses to make the most of the opportunities of the digital single market by cutting red tape and benefitting from reinforced consumer trust.

- The **Data Protection Directive** for the police and criminal justice sector, to ensure that the data of victims, witnesses, and suspects of crimes are duly processed in the context of a criminal investigation or law enforcement action. Harmonisation will facilitate cross-border cooperation to combat crime.

Individuals' rights are being strengthened, empowering them with more control over their personal data, most notably:

- easier access to one's own data: individuals will have the right to more information on how their data is processed, and this information should be available in a clear and understandable way
- a right to data portability: it will be easier for individuals to transfer their personal data between different service providers
- a clarified right to be forgotten: when individuals no longer want their data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted
- the right to know when your data security has been compromised: companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible so that affected users can take appropriate measures.

"Today's agreement is a major step towards a Digital Single Market. It will remove barriers and unlock opportunities. The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information. And they can enjoy all the services and opportunities of a Digital Single Market. We should not see privacy and data protection as holding back economic activities. They are, in fact, an essential competitive advantage. Today's agreement builds a strong basis to help Europe develop innovative digital services. Our next step is now to remove unjustified barriers which limit cross-border data flow: local practice and sometimes national law, limiting storage and processing of certain data outside national territory. So let us move ahead and build an open and thriving data economy in the EU – based on the highest data protection standards and without unjustified barriers."

Andrus Ansip, EC Vice-President for the Digital Single Market

"Today we deliver on the promise of the Juncker Commission to finalise data protection reform in 2015. These new pan-European rules are good for citizens and good for businesses. Citizens and businesses will profit from clear rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market. And harmonised data protection rules for police and criminal justice authorities will ease law enforcement cooperation between Member States based on mutual trust, contributing to the European Agenda for Security."

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality

Clear modern rules for businesses

Personal data has acquired enormous economic significance in today's digital economy, particularly in the area of big data. By unifying Europe's rules on data protection, lawmakers are creating a business opportunity and encouraging innovation.

- **One continent, one law:** the regulation establishes one single set of rules, which will make it simpler and cheaper for companies to do business in the EU. National supervisory authorities will be empowered to enforce the EU regulations both locally and consistently across the EU. They will be able to impose significant penalties for non-compliance:
  - up to €250,000 or up to 0.5% of annual worldwide turnover for failure to provide mechanisms for requests by data subjects, or not responding promptly, or not in the required format, or charging a fee for the information in violation of the rules and limitations.
  - up to €500,000 or up to 1% of annual worldwide turnover for intentional or negligent failure to:
  o provide information in a sufficiently transparent manner
  o rectify personal data, or communicate the relevant information
  o comply with the right to be forgotten or to erasure (or take all necessary steps to inform third parties that the data subject requests erasure of links to, copies of, or replications of any personal data)
  o provide a copy of the personal data in electronic format, or allow the data subject to transmit the personal data to another application
  o determine the respective responsibilities with the data controllers
  o maintain documentation
  - up to €1 million, or up to 2% of global annual turnover for those who:
  o intentionally or negligently process personal data without any or sufficient legal basis
  o do not comply with an objection, comply with the conditions on profiling, adopt internal policies or implement appropriate measures for ensuring and demonstrating compliance
  o fail to designate a representative and a data protection officer, or process or instruct the processing of personal data in violation of the obligations in relation to processing on behalf of a controller
  o fail to alert or notify of a personal data breach
  o do not carry out a data protection impact assessment

- misuse a data protection seal or mark
- carry out or instruct a data transfer to a third country or an international organisation that is not allowed under the legislation
- do not comply with an order or temporary ban on processing or suspension of data flows
- fail to comply with the rules for safeguarding professional secrecy by the supervisory authority

- **One-stop-shop:** businesses will only have to deal with a single supervisor: the local regulator in their home state. It will only be necessary to deal with one supervisory authority in order to operate anywhere within the EU.

- **European rules throughout the continent:** companies based outside of Europe will have to apply the same rules when offering services anywhere in the EU.

- **Risk-based approach:** the new rules avoid a burdensome one-size-fits-all obligation. Compliant solutions are to be tailored to the respective risks to be managed instead. The aim is reduce the red tape that business has to deal with, thereby saving an estimated €2.3 billion per year. The need to report the (currently increasing) number of data security breaches is to be relaxed somewhat. In place of the current requirement for all companies to notify all data protection activities to all the relevant data protection supervisors, the new regulation places more responsibility and accountability upon those who process personal data. Serious breaches will still need to be reported to the local supervisor (the Information Commissioner in the UK) as soon as possible and, if feasible, within 24 hours. Unsurprisingly, but perhaps inevitably, what is serious is surely going to be open to argument between the parties involved/affected by a given compliance failure, and will be established by case law.

- **Rules fit for innovation:** the regulation will guarantee that data protection safeguards are built into products and services from the earliest stage of development (the new principle of data protection by design). Privacy-friendly techniques such as pseudonymisation and anonymisation will be encouraged, to reap the benefits of big data innovation while protecting privacy.

Practical implementation

The current position is that the trilogue discussions between the EU Parliament, the national ministerial Council of the EU and the European Commission have concluded with two new instruments to put in place. The next steps cover a two year transition period, with enforcement likely to start in 2018. Primary legislation to adopt the new directive in member state parliaments has to be completed in the same timeframe if the new instruments are to come into force at the same time. Socitm members in the public and third sectors, therefore, should be using the transition period to plan and implement changes in processes and staff training in order to be compliant with the new regime. Supplier members should likewise be planning for more demanding compliance enquiries from their customers in local public service delivery, and from the citizen/business customers of those services too.

Accommodating some changes will be a matter of amending existing processes rather than inventing new ones. Others could be onerous and problematic. For example, a data storing and processing organisation (a council, say, and/or its cloud service provider) must be able to deal correctly and completely with right to be forgotten requests - perhaps the single greatest challenge in an almost ubiquitously networked and distributed computing world. How difficult might it be to trawl though all databases and emails etc. in order to redact personal references to an individual?

Organisations would be well advised to examine how robust and representative their information governance function is, and ensure that it reviews (or creates) compliant information strategies covering the full information lifecycle (create, collect, classify, control, store, search, publish, use, amend, archive and destroy). Particular points to cover include:

- a code of conduct for those who can access and/or use personal data
- encryption policies, especially concerning minimising damage in the event of data loss
- building-in rather than adding-on privacy to meet the requirement for privacy by design
- managed relationships along the full length of your (and your business partners') supply chains where the personal data of others is shared or otherwise exchanged.

Finally, we recommend that councils communicate to their employees the responsibilities that they will have, and how the council will support them through the strategies and codes of conduct.

References and further information

- *EC publishes proposed data protection reforms*, ComputerWeekly.com accessed 16/02/2016
- *European court rules 'Safe Harbour' treaty that saw Facebook hand over data to US is invalid, after challenge by student*, The Independent, accessed 16/02/2016
- *Get off of my cloud: A European court ruling presages a transatlantic battle over data protection and privacy*, The Economist
- *Irish row over safe harbor deepens*, ComputerWeekly.com accessed 16/02/2016
- *New EU privacy rules could widen the policy gap with America*, The Economist
- *Sending personal data outside the European Economic Area (Principle 8)*, The Information Commissioner's Office
- *The Economist explains: The new transatlantic data "Privacy Shield"*, The Economist
- *How To Prepare Your Organisation For EU Data Protection Reform*, TechWeekEurope UK

socitm insight

Socitm *Insight* is a subscription service to which over 400 local authorities and other public and private sector organisations now belong. It identifies and encourages good ICT management practice.

Socitm *Insight* has produced a series of comprehensive and detailed guides on all major ICT themes linked to the critical issues of the day, which provide valuable advice and support for ICT practitioners and all involved in application of ICT.

Socitm *Insight* Programme
Andy Hopkirk Tel: 01604 709456 E-mail: insight@socitm.net

Reference: 16004