EU general data protection regulation: the impact on English local authorities

ADSHEAD, Deborah <http://orcid.org/0000-0002-1331-1794> and SLACK, Frances <http://orcid.org/0000-0001-6638-798X>

Published version

ADSHEAD, Deborah and SLACK, Frances (2017). EU general data protection regulation: the impact on English local authorities. In: 17th European Conference on Digital Government (ECDG 2017), Proceedings. Academic Conferences and Publishing International Limited, 1-9.

EU General Data Protection Regulation: the Impact on English Local Authorities

Deborah Adshead, Frances Slack
Sheffield Hallam University, Sheffield, UK
d.adshead@shu.ac.uk
f.slack@shu.ac.uk

Abstract: The European Union (EU) General Data Protection Regulation (2016/679) will come into force in May 2018, and its expected impact on local authorities in the UK, specifically England, is explored. The key objectives are to identify how the changes to data protection legislation might impact on current compliance procedures and policies, and to suggest ways for English local authorities to minimise the risk of non-compliance with the new law by being better informed of the obligations the new rules impose on data controllers.

The study provides a context for the political and legal background regarding data protection and compares previous and existing legislation to the GDP Regulation to evaluate the amount of change likely. It then examines the current compliance situation in local authorities, through studies conducted by the British Information Commissioner's Office. Major problems in some local authorities are identified, with breaches of the Data Protection Act resulting in considerable fines totalling millions of pounds.

Findings indicate that, although principles of data protection will remain the same, the Regulation will introduce important changes requiring greater vigilance over compliance if fines are to be avoided. One change is the compulsory requirement to report data breaches, which could pose a serious problem in many local authorities. Just over one third reported never having had a breach; at best this means they have little experience of dealing with one, at worst there could be more fines to come.

The new law imposes a change of direction, from educating organisations after a breach has occurred to requiring proof that they took adequate measures to avoid one. Recommendations include implementing clear policies, recording incidents, staff training and having full accountability throughout the organisation. To avoid further losses to public sector services it is essential that local authorities make the needed changes to meet the new law.

Keywords: data protection, data breaches, EU regulation, local government compliance, legal changes, sanctions.

1. Introduction

The information revolution lacks sufficient regard for the civil liberties of people whose information is being collected. The expanded use of data-mining profiling techniques and data sharing has increased public discomfort at how much personal information organisations have access to, often without consent. Governments and citizens' interest groups recognise that allowing the current practices to continue unregulated may cause serious damage to the fabric of society. Data protection legislation is governments' answer to the problem. It may have flaws but it allows some redress to the individual who without it would have to resort to civil action against companies deemed to be breaching privacy.

In April 2016, after 4 years of negotiations and lobbying, the European Government adopted revised data protection legislation. The reform comprises three pieces of legislation: a regulation aimed at private and public sectors; a directive to facilitate cooperation in police and criminal justice matters; and a directive to strengthen national security in member states by sharing passenger travel information. The Data Protection Regulation 2016/679 (the Regulation) replaces existing data protection laws in all EU member states by 25th May 2018. The impact of the Regulation on English local authorities (LAs) is the focus of this paper.

The current EU Data Protection Directive (95/46/EC) (the Directive) provides a set of minimum requirements that all EU countries must meet. In the UK the Government ratified the Directive by introducing the Data Protection Act 1998 (the Act). However, the European Commission has expressed concern over the inability of the UK's enforcement body, the Information Commissioner's Office (ICO) to impose effective compliance measures and penalties on organisations. Current practice of voluntary breach notifications falls short of criminalising individuals for breaches of the Act; information and enforcement notices and monetary fines imposed by the ICO are the main punishment when breaches do occur. In the private sector a fine may be enough incentive to implement robust compliance measures; the potential damage to a company's reputation another. However, in the public sector these consequences do not have the same impact, particularly given that the taxpayer, the victim of the wrongdoing, ultimately pays any financial penalty imposed. In a report on

the findings of a survey of 16 LAs, the ICO (2014) stated that in 2013 almost £2.3M had been levied from the public sector alone, which inevitably impacts frontline services. Lloyd (2014) argued that the general absence of criminal sanctions in the current legislation is somewhat justified, but the data landscape has changed significantly since their inception. The widespread adoption of information technology, exponential growth in the use of the Internet and cloud storage providers, have contributed to a culture of data capture, processing, storage and sharing that has little regard for sovereign borders and poses many security risks.

The Regulation is intended to strengthen the protection afforded to individuals whilst making it easier for organisations to realise the potential that new data management technologies offer. How well the Regulation meets this goal remains to be seen. With an increase from 34 articles in the Directive to 99 in the Regulation, Koops (2014) is certain that legislation is about to become even more complex for many outside the legal profession to grasp, thereby increasing the risk of widespread non-compliance. Article 31 of the Regulation introduces the statutory requirement of notification of data breaches but Treacy warned it has the potential to overwhelm the ICO with notifications as the law "does not specify the criteria for deciding what constitutes a data breach" (In: Carey 2015). In the private sector competitors offer alternatives to poor data management but there is no alternative to interacting with local authority systems, especially if there is a legal obligation to do so, such as registering a birth. It is essential that compliance policies are robust, safeguards are preventative, and minimise the risk of breaches occurring.

There is little guidance on the imminent changes for LAs and in an attempt to make savings services are going digital wherever possible. Over 2 million employees work in 400 LAs in England, many of which contract out IT services to third parties. According to Public Sector Executive (2016) outsourcing is rising up to 23% year by year, increasing data sharing risks. It is essential that those able to access the data take every precautionary measure to ensure it is not compromised. Article 30 of the Regulation extends the obligation to demonstrate adequate security measures to both the Data Controller (the entity legally responsible for defining what data is processed and how) and the Data Processor (any entity excepting employees of the Controller undertaking data processing functions on behalf of the Controller). According to Treacy this "is likely to lead to a reassessment of risk, and the reallocation of risk in outsourcing and other contracts" (In: Carey 2015). The aim of this research was to identify and assess the changes in policy and procedures likely to be needed by implementing the Regulation in LAs and the potential impact on data management and maintenance.

In section 2 the background of data protection legislation and development of key pieces of legislation specifically related to the protection of data and the requirements of the Act are presented. Section 3 briefly presents the research methods used. Section 4 discusses the reformed data protection legislation and compares this to the Directive and the Act. Before discussing the compliance requirements of LAs (section 6) and drawing conclusions on the success or otherwise of these organisations to avoid breaches, it was important to add section 5 on the changed landscape resulting from the decision in the UK Referendum to withdraw from the EU and how this might affect the data protection framework in the UK. The main assumption throughout this report is that the UK will decide to implement something very similar to the Regulation in order to facilitate the passage of any trade negotiations with the EU. Section 7 concludes by summarising the key findings of the Regulation in relation to the impact this is likely to have on LAs in the UK if adopted.

2 Data protection legislation

The last 60 years has seen the exponential growth in personal data and private correspondence in existence. The rise of computers and invention of the Internet significantly increased the opportunity to violate the right to privacy and is a chief influence on the development of data protection legislation. Globalisation and the emergence of large multi-national conglomerates has allowed super companies with enormous wealth and power to take advantage of deregulation and greater cooperation between governments to access data, transfer it across borders and make it easily available to others, without oversight. Those within the knowledge industry that commoditise and trade in information and data pose a clear and specific threat to individual privacy.

The Directive is the central piece of EU legislation dealing with the processing of personal data and its cross border transfer. To overcome complex legislation in the US that many deemed inadequate for protecting EU citizens' data and ineffective for those who felt their rights were being breached, the EU and US authorities entered into an agreement (US Adequacy Decision 2000/520/EC commonly known as the Safe Harbor Agreement) to allow companies, willing to adhere to a strict set of principles, to process EU citizens' data legitimately. However, this was nullified after a successful challenge in the EU court and recently replaced by the EU-US Privacy Shield Agreement (2016). Central to all legislation aimed at protecting personal data is the need for the individual to have some control over the processing of their data, to have the ability to consent to

data being used for reasons other than those originally intended, and to limit the possibility for organisations and governments to interfere unduly with the privacy of a data subject. Privacy impact assessment (PIA) has been used regularly in the UK for the past decade and more recently made mandatory for some central government processing activities. According to Wright (2012) PIAs are more than a tool for taking corrective action to avoid or minimise the negative impacts of a project on privacy. He states they should be seen as a process that begins early on in a project "while there are still opportunities to influence the outcome" and last beyond deployment. Proactive privacy by design (PbD) is recommended by Kroener and Wright (2014) as a means to ensure accountability of activities.

2.1 Data protection reforms

Since 2012 the data protection legislation in the EU has been under reform and 2016 saw the introduction of three key pieces of legislation, shown in figure 1. This paper focuses on the Regulation (1); the two Directives (2 & 3) are outside its scope.

Figure 1: EU Data Protection Reform Legislation

2.2 UK data protection

The Data Protection Act 1998 was passed to give effect to the EC Directive 95/46/EC and came into force in the UK in March 2000. It gave clear definitions to the terms, including: processing, data subject, data controller, data processor, personal data, data, paper and other manual records, relevant filing system, public authorities, living individual, and identification. Its 8 Principles included:

- The organisation must have valid and proportional reason for collecting and using personal data
- Personal data must be obtained only for one or more specified and lawful purposes
- Data controllers are obliged to obtain and use only those pieces of information that are necessary for their purposes for processing such information
- Data controllers ensure the accuracy of personal data processed by them, keeping such information up to date
- Once an organisation has completed business with a customer and any other legal obligation to keep the data has been fulfilled, it should ensure the customer's records are deleted
- Each person has a right to expect their data to be respected and handled appropriately and at any point they can legally request a copy of the data to ensure it meets the principles set out above
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area (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.

Unless an organisation is deemed exempt, all Data Controllers must be registered with the ICO, a process known as "notification". It is common for most medium and large organisations to employ at least one person who is ultimately responsible for compliance with the Act within the organisation

Data protection law is enforced in the UK by the ICO, which has powers to implement measures against organisations that are in breach of one or more Principles of the Act. These range from advice on how to

better comply with the law to quite severe monetary penalties for more serious breaches or serial offenders. The ICO's preferred approach is education to improve compliance; fines are usually a last resort.

3 Research methods

In order to make the relevant compliance recommendations to LAs, this research was undertaken using doctrinal methods (McConville and Chui 2007). Legislation and case law was analysed to present the current data protection law in the UK and to discuss the development of legislation from its early forms to the most recent to come from the EU and to compare the two.

However, given the UK Referendum results, it is unclear whether the Regulation will be applied in the UK. It was necessary to discuss policy in the area of data protection to make some determination regarding the approach that should be taken by the UK authorities. To do so, it was important to discuss the area of data protection in relation to the application or non-application of the Regulation and the legal problem that either approach would represent.

In the absence of any mandates from government to LAs necessitating they provide a greater level of compliance than required by the DPA, guidelines issued by the ICO were considered together with the review of key changes in legislation, to form the basis of the recommendations for LAs. Penalties issued by the ICO and cases brought before UK and EU law courts relating to data breaches that have occurred within LAs were also evaluated to determine whether there is a current problem and, if so, what might be the factors leading to the most severe penalties.

4 Reforming data protection by new legislation

The explosion in the amount of personal data available online and its indiscriminate transfer across organisations and borders has meant that the variety of EU member state laws arising from implementation of the Directive are no longer adequate, particularly for non-EU companies processing EU citizens' data. It was clear that a stronger, more consistent update to the Directive was needed to make it fit for purpose. However, whether it is comprehensive or strong enough to be effective is questionable given that the new legislation is in two parts; the Regulation aimed at the private and most of the public sector, and Directives for the police and criminal justice sectors. Discrepancies in how the Directives are implemented are still likely, which could reduce the Regulation's protection. An example is the UK's Investigatory Powers Act 2016 forcing blanket storage of telecoms and online traffic for exploration by law enforcement authorities.

4.1 Key changes in the Regulation affecting Local Authorities

Similar in wording to the Directive but not identical, Article 5(1) sets out the "Principles relating to the processing of personal data", shown in Figure 2.

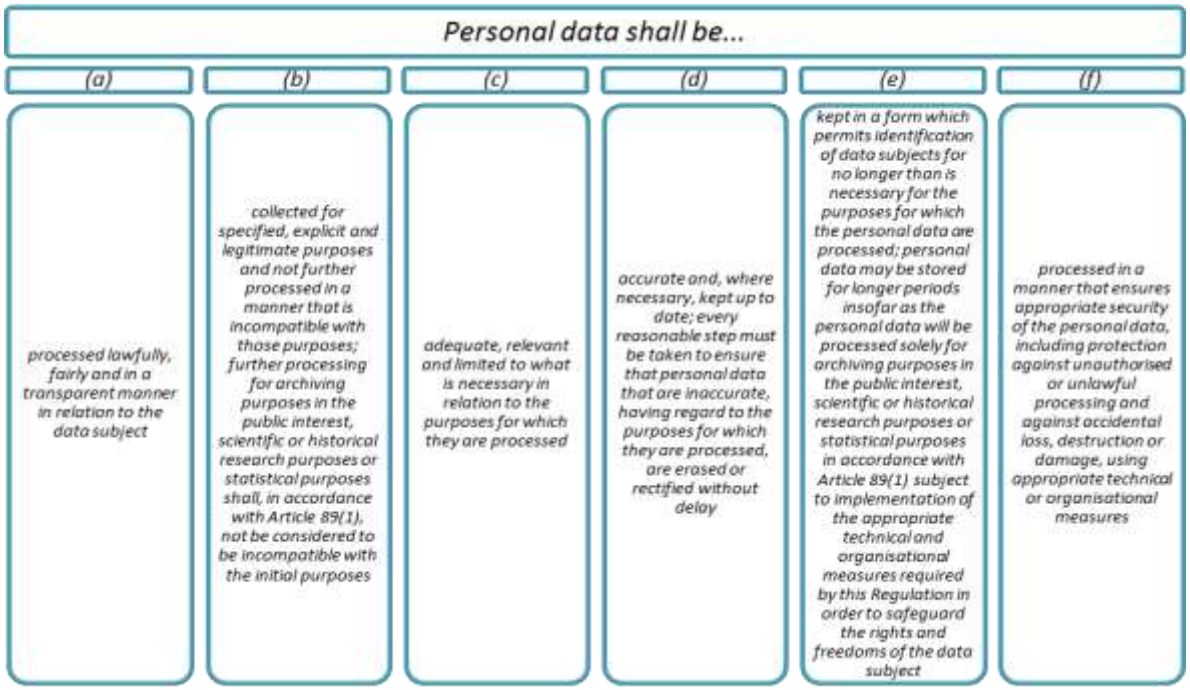

Figure 2: Article 5(1) of the Regulation

The definition of "personal data" is expanded from that of the Directive to include: online identifiers (IP addresses of devices used to access the Internet); location data and genetic information; biometric data; and information regarding sexual orientation, but only if these are used to specifically identify an individual. "Sensitive" data is renamed to "special category" data and the conditions under which it is allowed to be processed are outlined in Article 9. This is likely to include most personal data being processed by LAs.
The following subsections address the important measures of the Regulation and identify where changes will need to be made.

4.1.1 Accountability
Accountability is central to the Regulation; data protection is expected to be part of the shared values and practices of an organisation. The responsibilities for implementing the legislation expressly include: maintaining documentation; implementing security measures; performing data protection impact assessments; designating a data protection officer; consulting with the data protection authority and data protection officer; and establishing transparent communication with data subjects. The requirement to register as a Data Controller is removed, except where processing data poses high risk. To offset this, a requisite is keeping comprehensive documentation of the procedures companies put in place proving compliance before the event. It is also obligatory to provide guidance on how data subjects can make a complaint, object to processing or have data erased.

4.1.2 Data processor and data controller
Data Processors, third party organisations undertaking processing activities for Data Controllers, will become Data Controllers in their own rights and held equally responsible for compliance with the legislation by the Supervisory Authority (SA) – in the UK the ICO – in the event of a data breach, although this does not negate the need for a contract between the two.

4.1.3 Data breaches
Unless it is "unlikely to result in a risk to the rights and freedoms of natural persons" the Data Controller must report a data breach to the SA no later than 72 hours after it has been detected and notify all data subjects individually. Notifying data subjects separately is unnecessary if the data compromised was encrypted, other measures were taken post breach to render the data unusable, or if notification would involve "disproportionate effort" where a public announcement might be more suited. However, exactly what constitutes a breach with serious impact is still open for interpretation and may become an issue that requires further clarification.

4.1.4 Data Protection Officer

The Regulation mandates all public authorities to employ or contract out a Data Protection Officer (DPO). The DPO is responsible for: monitoring and keeping all compliance records up to date; educating others of their responsibilities in processing data; carrying out internal audits; acting as the central contact point for responding to requests for information from data subjects; advising on data protection requirements during process and system development projects. They also have a key role in conducting Data Protection Impact Assessments.

4.1.5 Consent

Consent must be purpose limited and is no longer valid when this is accomplished. Consent must be requested in a clear, legible format for each different type of processing that occurs and unless it is needed to fulfil a contract cannot be made a condition of one. It must be possible for the data subject to withdraw consent at any point using a simple process.

This change in acquiring consent may lead to reengineering of websites to ensure that visitors to the site are explicitly opting in to processing, such as having a cookie file installed on their computer rather than simply displaying a cookies policy notification.

Unless, as with adults, a legal obligation or legitimate interest means consent is not required, such as for preventative or counselling services, then the consent must be sought of a parent or guardian to process a child's data.

4.1.6 Rectification and erasure

A data subject has the right for incomplete or incorrect data to be amended and for any adverse decisions made using the incorrect data to be redressed. Moreover, if data is no longer required for a legitimate reason or consent has been withdrawn, a data subject has the right for data to be erased or, in the specific context of a processing medium such as a search engine, to be removed from the search results.

4.1.7 Right to object and automated decision-making

A data subject may have the right to object to personal data being processed if a Data Controller states that processing is being undertaken in the interests of the public or for legitimate reasons but these are not made clear. If there is a legitimate reason for a profiling activity it may not be possible to object to it taking place. Nevertheless, any decision based solely on automated means can be challenged.

4.1.8 Anonymisation and pseudonymisation of data

Anonymised and pseudonymised data (the process of rendering information until it is no longer possible to identify the individual to whom the data belongs) is no longer bound by the Regulation if it is not possible for the processor to reconstruct the data. Identifying data must be removed and deleted altogether in anonymised data sets. In pseudonymised data the identifying data, replaced with a random key (identifier), must be removed and must be kept separately to the data set, and only reconstructed when necessary.

4.1.9 Privacy and security by design and default

Organisations are required to address data protection risks associated with the various processing activities when creating or reengineering business processes and developing new systems. Privacy by design (Kroener and Wright, 2014) and "Design by default" methods might include pseudonymisation of data, and only capturing or disclosing data at the point where it is absolutely necessary to complete a task.

4.1.10 Data Protection Impact Assessments

Article 35.1 of the Regulation states that Data Protection Impact Assessments (more commonly known as PIAs) are required for any organisation where an act of processing "is likely to result in a high risk to the rights and freedoms of natural persons". If the outcome indicates a high risk and the Data Controller is not able to sufficiently mitigate against this the SA must be informed prior to any processing being undertaken. There is no "one size fits all" approach to PIAs, but Wright's (2012) summation of best practice across a number of sectors in various countries is a useful guide to follow, particularly when coupled with the guidelines and templates available on the ICO website.

5 Implications post BREXIT

It is improbable that negotiations for the UK to withdraw from the EU will be completed by 25th May 2018 when the Regulation comes into force. In the intervening period the UK will be bound to meet this obligation. Failure to provide a data protection landscape offering the same protections afforded by the Regulation risks affecting the ability to transfer data internationally and thereby limiting the opportunity for a thriving global digital economy to flourish. If the UK is not accepted by the EU as a "Safe Country" sanctions could be placed on the UK regarding processing of EU citizens' data. Any alternative data protection law introduced by the UK Government or any agreement entered into will need to meet the same "adequacy" test that each of the "Safe" countries outside the EU has had to undergo.

Once the UK is no longer a partner in the EU-US Privacy Shield agreement, UK citizens' data being transferred to the US becomes vulnerable. If the Regulation is adopted post Brexit the simplest solution would be to expand the agreement to include the UK. Failure to negotiate this could affect the network traffic currently using transatlantic pipelines located in the UK, routed from the EU to the US. It would also be necessary for the UK to negotiate a separate agreement with the US.

6 Local Authority Compliance in England

Digitising public services poses many risks in the UK; despite legislation existing since 1984 LAs have received some of the largest fines for data protection breaches. Currently voluntary, except for central government bodies and the NHS, the Regulation will make reporting data breaches mandatory for all organisations including LAs. It is probable that without improvements the number of fines will increase, ultimately hurting frontline services that are struggling due to cuts in government funding.

The compliance regime must be improved within the public sector by increasing awareness of legislation and introducing robust policies that promote and encourage best practice.

6.1 Data protection responsibilities

The type of data held by a particular LA will depend on the services it provides; much is classified special category. Some of the more common types are:

- names, addresses and dates of birth
- financial details relating to payment of council taxes, rent, library charges
- special needs and health requirements relating to social services, education, housing, transport
- criminal records and debt management
- education records
- family circumstances relating to births, deaths, marriages, civil partnerships, divorces
- any involvement with family and social services.

6.2 Current data breach reporting

The ICO releases quarterly data relating to data breaches it is aware of but it is difficult to obtain an accurate account of just how many occurred in LAs due to the way organisations are categorised into sectors. For the same reason it is also difficult from this data to determine with any precision what breaches occur most frequently or attract the greatest fines.

A study (ICO, 2014) focusing on audits conducted in 16 LAs showed a mixed picture with some worrying results. Of the 16 none offered a high level of data protection assurance; only 9 of them had reasonable safeguards in place, the rest reported limited or very limited assurance against data breaches occurring.

A further study (Big Brother Watch, 2015) reported over 4,000 data breaches in LAs in 2011-2014, and called for tougher sanctions for breaches, particularly for deliberate or easily avoidable acts. They suggested a lack of a consistent approach to breach management, punishments and corrective action may distort the perception that those organisations following the correct protocol and reporting breaches are the worst offenders. The data, obtained using Freedom of Information requests, revealed that 167 (38%) of LAs reported having no data breaches during the 3-year period, which might seem to suggest these LAs have a perfect data protection governance structure with no mistakes, thefts or incidents of unauthorised access ever having taken place. If this is accurate these LAs are clearly in a good position to share best practice with those reporting a high number. However, when they are compared to similar size LAs over the same time period a more realistic picture emerges. It is much more likely that these organisations either kept insufficient records to provide information or were wary of disclosing breaches via the study that had not been reported to the ICO (2014). In a previous Big Brother Watch study (2011) 100 LAs acknowledged over 1,000 data breaches but only 55 of those were actually reported to the ICO, suggesting voluntary reporting is masking the truth. This is an area

that warrants greater study and scrutiny of procedures currently in place to compare these to those implemented post-May 2018 to develop a more accurate trend analysis.

7 Recommendations and conclusions

No statutory guidelines exist binding LAs to behave in a particular way so best practice should be sought and followed where possible. It is recommended that a gap analysis be undertaken to consider which changes are necessary. Figure 3 shows key areas for LAs to focus their attention before May 2018.

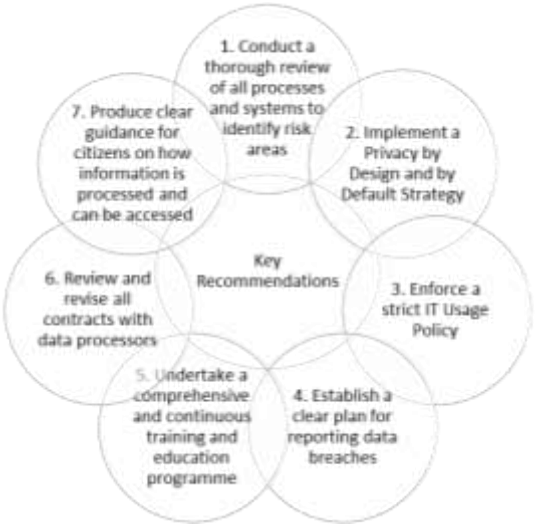

Figure 3: Key recommendations for Local Authorities in England

To ensure compliance with the forthcoming legislation it will be necessary for all LAs to review their data protection compliance and assess which policies and procedures may need producing or amending. These recommendations to English LAs comprise the following details:

1. Develop data flow diagrams to identify what data is processed and how, who has access to it, and when it is deleted. Assess the likelihood of breaches occurring and their potential impact.
2. Amend processes and/or systems to minimise any identified risks, including restricting access to personal data unless necessary. Ensure data protection impact assessments (PIA) are undertaken for any development of new or amendments to existing systems and business processes and build-in privacy features (PbD) wherever possible.
3. Provide employees with clear acceptable behaviour guidance on using IT equipment and services provided for business use, including limiting or forbidding employees from using LA systems for personal use and use of own devices for work purposes. Encrypt all portable devices.
4. Ensure employees know what constitutes a breach and how to report one. Identify a clear swift course of action for responding to one and act afterwards to reduce any risk of reoccurrences.
5. Educate employees to fully understand the consequences of non-compliance. Tailor training to individuals' roles and data types they access. Appoint data owners responsible for maintaining data integrity, reporting to the Data Protection Officer.
6. Ensure legal experts administer contracts and due diligence is undertaken. Agree processes for reporting data breaches and responding to requests from data subjects.
7. Provide clear information to data subjects on: what data will be processed and how; when it will be deleted; who it might be shared with; how to request copies of their data; and how to object to and opt-out of processing activities.

This move towards a risk-based approach to managing data places the burden of proof on organisations to show all measures were taken to avoid breaches occurring, therefore comprehensive documentation must be kept. It will be compulsory to acquire unambiguous consent from data subjects for some processing activities, which may involve reengineering of websites and data systems.

In most cases it will no longer be necessary for Data Controllers to register processing activities prior to any taking place unless they are deemed to be of a significantly risk. However, reporting any breach will become

mandatory for all organisations where it is likely that any disclosure of the data may adversely affect the data subject(s). This mandatory reporting should in time provide a more accurate picture of non-compliance, which currently varies significantly from private to public sector and from authority to authority, likely due to some organisations not voluntarily reporting breaches. However, more research is needed in this area to ensure a more accurate trend analysis can be provided.

In the public sector there is no risk of customers protesting by going elsewhere. The risk here is that fines for breaches will affect funding available for frontline services, which may be why some LAs choose not to disclose any. If the trend towards digitised services continues, the situation regarding data protection must improve significantly to ensure victims are not punished twice.

It is still unclear which laws will be adopted once the negotiations to withdraw the UK from the EU have been completed. However, as the UK is obligated to adopt the Regulation in the interim, and will require something very similar afterwards if it wishes to service EU consumers, it is fairly safe to assume Regulation (EU) 2016/679 is here to stay and LAs have some way to go to ensure citizens' data is secure in their hands.

References

Big Brother Watch (2011) Local Authority Data Loss, November 2011 ed., London, England, Big Brother Watch.

Big Brother Watch (2015) A Breach of Trust, August 2015 ed., London, England, Big Brother Watch.

Carey, P. (2015) Data protection: a practical guide to UK and EU law, Oxford, Oxford University Press.

European Commission (1995) 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, Official Journal L 281, 23/11/1995 P. 0031 - 0050. Luxembourg.

European Commission (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 32016R0679 OJ L 119/1 27.04.2016. Brussels, Belgium.

Information Commissioner's Office (2014) Findings from ICO audits of 16 local authorities: January to December 2013, London, UK, Information Commissioner's Office.

Information Commissioner's Office (2016) Data Security Incidents, [online] Last updated 29 April 2016, https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

International Trade Administration US (2016) EU-US Privacy Shield Framework, Key New Requirements for Participating Companies, [online] Last updated 2016, https://www.privacyshield.gov/Key-New-Requirements.

Koops, B-J. (2014) The trouble with European data protection law, [online] International data privacy law, Vol 4, No.4, p 250.

Kroener, I. and Wright, D. (2014) A Strategy for Operationalizing Privacy by Design. The Information Society, Vol 30, No.5, p 355-365.

Lloyd, I. J. (2014), Information technology law, [online] Oxford, Oxford University Press.

McConville, M. and Chui, W.H. (2007) Research methods for law, [online] Edinburgh, Edinburgh University Press.

Public Sector Executive (2016) Council spending on outsourcing rises 23% year-on-year, Manchester, England, Cognitive Publishing Ltd.

UK Houses Of Parliament (1998) Data Protection Act 1998, London, England.

UK Houses Of Parliament (2016) Investigatory Powers 2016, London, England.

Wright, D. (2012) The State of the Art in Privacy Impact Assessment. Computer Law & Security Review. Vol 28 (2012) p 54-61.