Legal Information Management, 18 (2018), pp. 21–28
 doi:10.1017/S1472669618000051

FOCUS ON GDPR

The General Data Protection Regulation: the Next Generation of EU Data Protection

Abstract: This article, written by Sahar Bhaimia, presents an overview of the General Data Protection Regulation (EU) (*2016/679*) (**GDPR**) which will apply automatically across the EU on 25 May 2018. The GDPR is an update and reform of existing EU data protection law, first established by the Data Protection Directive (*1995/46/EC*). The article is for knowledge managers and information services professionals who may be asked to take on responsibility for GDPR, and focuses on the UK. It covers the fundamentals of EU data protection law, highlights key changes brought about by the GDPR, and provides practical tips and suggestions for knowledge managers.
Keywords: data protection; privacy; General Data Protection Regulation; GDPR

INTRODUCTION

On 25 May 2018, the General Data Protection Regulation (EU) (*2016/679*) (**GDPR**) will apply automatically in the UK and other European Union (**EU**) Member States, replacing the Data Protection Directive (*1995/46/EC*) (**Directive**). For a law firm, the GDPR will affect it in two ways: its own data protection compliance, and its advice to and support of clients on their data protection compliance.

Headlines in the media reference eye-watering fines and onerous obligations. Such claims can trigger unease and uncertainty about an organisation's compliance, but should be fact checked. There have been so many incorrect or misleading claims about the GDPR that the UK's regulator had to set up a 'myth-busting' blog[1]. Such claims exploit other people's lack of understanding of EU data protection law.

The GDPR is an update of existing EU data protection law – it replaces the Directive but continues the principles and rules established by the Directive as this article will explain. As with any law reform, there are changes but also continuity. Accordingly, preparing for compliance with the GDPR has meant auditing an organisation's current data protection compliance, identifying gaps between that and the GDPR, and implementing remedial steps. If an organisation's current level of compliance is somewhat *lacking*, then the remedial steps may be extensive and may even require additional resources. This is likely to continue even after the GDPR applies on 25 May 2018.

As such, the GDPR has a powerful gravitational force, drawing in newcomers. This article is written for the knowledge management professional or information services professional (**knowledge manager**) in a law firm who (willingly or not) is drawn into the GDPR as a newcomer.

This article will provide you with a head start.

BUILD THE FOUNDATION

EU law provides the structural foundation. Those with background in areas of law which are similarly influenced by EU law (such as financial services) will have transferable knowledge. For others, learn the basic concepts of the EU, its laws (and the forms they take), its legislative institutions and key bodies, and the role of the Court of the Justice of the European Union (**CJEU**)[2].

Knowledge of the basics of EU law is useful because:

- The Directive had to be implemented in member states' laws. This has led to variation across the EU. In the UK, it was implemented by the Data Protection Act 1998.
- The GDPR, as a regulation, is 'directly applicable' so applies automatically in each Member State. One reason for use of a regulation was harmonise the laws of member states. However, national law will still be required, even if only to enact the national derogations in the GDPR and to repeal or amend national law implementing the Directive. See below for the UK's Data Protection Bill.
- When interpreting an article of the GDPR, recitals to the GDPR must also be taken into account as an aid to interpretation of the article.

- The Court of Justice of the European Union (**CJEU**) will answer questions from national courts of Member States on the interpretation of the GDPR, but also on the directive. Because the same rule may continue in the GDPR, CJEU decisions on interpretation of the Directive remain relevant.
- Advocate-Generals of the CJEU submit non-binding opinions for some cases. Even where the CJEU has not followed the opinion, it provides essential background to the decision.
- The Directive applies to the European Economic Area (**EEA**) – the GDPR will eventually.

In most law firms, data protection is the domain of IT/IP/commercial lawyers, employment lawyers and dispute resolution lawyers. In addition to EU law, a broad understanding of these laws will provide context.

Tip box:

- Use an online version of the GDPR which hyperlinks relevant recitals to articles.
- Read Advocate-General opinions to CJEU cases on data protection.
- Check CJEU decisions on the Directive.
- Keep data protection in context: eg if the individual is an employee, employment law is also relevant.
- Track the UK Data Protection Bill.

UNDERSTAND THE DEFAULT RULE

At its heart, EU data protection law (both under the Directive and the GDPR) has one simple rule of thumb: an organisation cannot do anything with the personal data of an individual unless it is permitted by the law. The permissions are known as fair processing conditions or lawful grounds and written in EU data protection law as an exhaustive list (see below).

In other words, the default position is a prohibition. But why? The reason lies not in protection of economic or ownership rights. Rather, it is to protect individuals in light of the European experience in the 20th century of persecution and genocide based on certain personal characteristics (*personal data*) and mass surveillance, enabled and facilitated by automated processing and private companies. The list of 'special categories of data' below (considered sensitive enough to warrant additional fetters) reveals this history.

After the Second World War, the Council of Europe adopted the European Convention on Human Rights which enshrined a right to privacy[3]. Though data protection and privacy are not the same thing, they interrelate. A right to protection against the collection and use of personal data also forms part of the right to respect for private and family life, home and correspondence. Claims for breach of data protection law may sometimes also include claims for breach of the right to privacy. Accordingly, it is important to keep up to date with relevant decisions of the European Court of Human Rights[4].

In light of technological advances, there was a growing need for more specific data protection laws. In 1981 (and after Sweden and the German state of Hessen had enacted specific data protection laws), the Council of Europe adopted the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108[5]). This is a key international instrument, setting out many of the principles of EU data protection law later written into the Directive and reiterated in the GDPR.

In recent years, data protection has been categorised as a 'fundamental right' under the Charter of Fundamental Rights of the European Union[6]. This provides that 'everyone has the right to the protection of personal data concerning him or her'[7].

Knowledge of these rights is important to prevent data protection law being treated as just another tick box for compliance purposes, and to challenge the sinister fallacy: 'if you have nothing to hide, you have nothing to fear'.

Tip box:

- Remember the default rule of thumb: an organisation cannot do anything with the personal data of an individual unless permitted under the law. A fair processing condition or lawful ground for processing must be satisfied.
- Keep up to date with the case law from the European Court of Human Rights on the Convention right to privacy.

IDENTIFY THE LEGISLATIVE LANDSCAPE

As with any law reform, a key step is to identify the existing legislative framework in the EU and the UK. A list of laws is set out at the end of this article.

The Directive is not alone. The laws on direct marketing via electronic means (email, text, telephone) are set in the Privacy and Electronic Communications Directive (*2002/58/EC*) (**PECD**). E-mail marketing by a law firm of its services and seminars must comply with these rules. The PECD also covers the rules for website cookies, privacy of telecommunications data, and provides for mandatory notification of data breaches by communications companies. The PECD was implemented into UK law by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

The PECD will eventually be replaced by a future E-Privacy Regulation, announced by the European Commission in January 2017, and this is a key reform to track.

In the UK, another important law is the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (*SI 2000/2699*) which provides the conditions under which organisations are permitted to monitor and record communications (eg for regulatory compliance purposes), which would otherwise by prohibited by the Regulation of Investigatory Powers Act 2000. This statutory instrument will also be replaced (see below).

Tip box:

- Map EU law to its UK equivalent.
- Use the consolidated EU version of the PECD, as the rules on cookies were added later.
- Track additional law reform (EU and UK), in particular the EU reform of the PECD.

UK Data Protection Bill

The Data Protection Bill was introduced to the House of Lords in September 2017 to begin its legislative passage. Responsible Government departments are the Department for Digital, Media, Culture and Sport (DCMS) and the Home Office.

The Bill:

- Implements the UK's national derogations in the GDPR (Chapter 2, Part 2). It does not write out the GDPR, so must be read side-by-side with the GDPR.
- Implement the GDPR in areas not subject to EU law, such as immigration (Chapter 3, Part 2). A mark-up of the GDPR as amended by this Chapter has been published by DCMS (a Keeling Schedule[8]).
- Implement the Law Enforcement Directive (Part 3). Only public and some private organisations are caught by the Law Enforcement Directive (see below).
- Implement a new data processing regime to apply to the intelligence services (Part 4).

The Bill must receive Royal Assent by early May 2018, due to the earlier implementation deadline of the Law Enforcement Directive.

IDENTIFY THE MAIN ACTORS

The 'data controller' (*Article 4(7)*) is the person who, alone or jointly with others, determines the purposes and means of processing personal data. All organisations will be controllers in respect of their own employees' personal data.

The 'data processor' (*Article 4(8)*) is the person which processes personal data on behalf of the controller, but does not determine the purpose or means of processing. Employees of a controller are not processors for their employer. Under the Directive, a processor faced no direct regulatory liability, but will do so under the GDPR (see below).

The 'data subject' (*Article 4(1)*) is the identified or identifiable individual to whom the personal data relates. The individual can be an employee, a business contact at a client, or a consumer.

The 'supervisory authority' (*Article 4(21)*) is the independent regulator for data protection in each Member State. In the UK, it is the Information Commissioner's Office (ICO). The ICO has a statutory duty to promote good practice by controllers, and to publish information about good practice, including codes of practice (*Section 51, DPA 1998*). ICO guidance covers existing law[9] and the GDPR[10], and should always be checked.

The Article 29 Working Party (WP29) (established under Article 29 of the Directive) is an influential advisory group, comprising representatives of each member state's supervisory authority, representatives of the EU institutions, and a representative of the European Commission. It publishes non-binding opinions and guidance, also essential reading. As well as its materials on the Directive, the WP29 has published guidance on key aspects of the GDPR[11].

Under the GDPR, the WP29 will become the European Data Protection Board (*Articles 68–76*) (**Board**). The Board must ensure the consistent application of the GDPR and to achieve this, the GDPR sets out a lengthy list of tasks, including issuing guidance, recommendations and best practices in order to encourage consistent application of the GDPR (*Article 70(e)*), and issuing binding decisions in cross border enforcement cases (*Article 70(t)*).

The Committee on Civil Liberties, Justice and Home Affairs (LIBE) is the committee of the European Parliament most relevant to data protection and privacy at EU level. It scrutinises draft legislation in this area.

Tip box:

- Check the ICO and WP29 websites if they have published guidance on a topic.
- Save key WP29 pages as favourites: as at the date of writing, it has a page with materials published before 2017[12], and a page with materials (including GDPR) since 2017[13].
- For the WP29 website, consider use of a free online "website watcher" to pick up new publications as the webpage is changed.

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

Cont.

- Read ICO enforcement decisions for what could have been done to prevent the breach.

IDENTIFY THE KEY CONCEPTS

'Personal data' *(Article 4(1))* is data relating to an identified or an identifiable living individual, whether on its own or in combination with another data set, and whether directly or indirectly. Personal data can include unique identifiers (such as a passport numbers) and the GDPR puts beyond any doubt that it will also include online identifiers (such as IP addresses). The concept of personal data is non-exhaustive.

One particular group of personal data is exhaustive. Certain types of personal data are seen as more sensitive than others, and under the GDPR these are known as 'special categories of data' *(Article 9(1))*: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation. To this existing list, the GDPR has added two more: biometric data and genetic data. The default rule is explicitly stated – processing such personal data is prohibited, unless an additional lawful ground applies. Personal data about criminal offences must also be treated with greater care (*Article 10*).

Pseudonymised data is that which can no longer be attributed to a specific individual without the use of additional information. Although strictly still personal data, there are benefits under the GDPR from doing this. Anonymised data is not personal data because the individual is no longer identifiable and can never be re-identified, so it can help take an organisation outside EU data protection law entirely (though the act of anonymization is still processing of personal data).

'Processing' (*Article 4(2)*) has incredibly wide meaning – nearly anything that could be done to or with personal data constitutes processing.

Identify the territorial scope

The GDPR extends the jurisdictional scope of the EU's data protection laws to controllers or processors outside the EU if the organisation is offering goods or services (including free goods or services) to individuals within the EU, or if it is monitoring the behaviour (within the EU) of individuals in the EU. This extraterritorial scope means that overseas companies (particularly internet and technology companies, who were in mind when this rule was added) may find themselves caught by its laws.

UNDERSTAND THE LAWFUL GROUNDS

The fair processing conditions (**lawful grounds**) are exhaustive. For all personal data, there are only six lawful grounds for processing, at least one of which must apply. The three most useful to organisations are that the processing is: necessary for performance of the contract with the individual or in order to take steps at the individual's request before entering into a contract (*Article 6(1)(b)*); necessary for compliance with a legal obligation which applies to the controller (*Article 6(1)(c)*); and necessary for the 'legitimate interest' of the controller or a third party but which are not overridden by the rights of the individual (*Article 6(1)(f)*). Personal data processed in employment generally fall within one of these three lawful grounds. The GDPR prevents public authorities relying on the legitimate interest lawful ground for processing in the performance of their tasks.

Consent of the individual for specified purposes is another of the six conditions (*Article 6(1)(a)*). The GDPR tightens the rules on what constitutes a valid consent: it must be freely given, specific, informed and unambiguous, not bundled with other terms and conditions, evidenced by the controller, and the individual can withdraw it at any time (*Article 7; Recitals 32, 42–43*). Under the GDPR, consent is also not an appropriate ground where there is a clear imbalance of power between the organisation and the individual (*Recital 43*).

Under the Directive, it was not necessary to tell an individual the lawful ground for processing his personal data. However, under the GDPR, it will be necessary to tell them as part of the principle of transparency (see below) and because a data subject's rights may flow depending on the specific lawful ground. Determining the appropriate lawful ground(s) for processing is one of the important work streams for GDPR compliance.

For processing special categories of data, there are an additional exhaustive list of lawful grounds, at least one of which must be found before processing such personal data. These include the explicit consent by the individual (*Article 9*).

Tip box:

- When considering which lawful ground in Article 6 applies, consider consent last.
- Remember that processing of special categories of data will require another additional lawful ground – the rules are stricter for such sensitive data.

UNDERSTAND THE PRINCIPLES

Rather than set out prescriptive rules on how to process, EU data protection law is a principles-based regime. Data export is treated as a principle here, for consistency with the Data Protection Act 1998 and organisations familiar with that. In effect, the GDPR only adds one new principle - accountability.

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

Lawfulness, fairness and transparency (Article 5(1)(a))

Personal data shall be processed lawfully, fairly and in a transparent manner.

To process lawfully means to find a lawful ground, but also not breach other law (including the Article 8 Convention right to privacy). As part of transparency, the GDPR significantly expands the list of information that must be provided to the individual when collecting personal data (*Article 13*), or when receiving personal data from a third party (*Article 14*). These are known in practice as privacy notices or fair processing notices.

Purpose limitation (Article 5(1)(b))

Personal data shall be collected for specified, explicitly and legitimate purposes, and not processed in a manner incompatible with those purposes.

The GDPR sets out rules when processing for another (secondary) purpose and the factors to be taken into account when assessing whether the secondary purpose is compatible with the initial purpose (*Article 6(4)*).

Data minimisation (Article 5(1)(c))

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Data minimisation is a key aspect of the GDPR's 'data protection by default and design' (*Article 25*), which requires controllers to consider data protection at the design stage of projects and products (not at the end).

Accuracy (Article 5(1)(d))

Personal data shall be accurate, kept up to date (where necessary), and every reasonable step should be taken to ensure that inaccurate data are erased or rectified without delay.

Storage limitation (Article 5(1)(e))

Personal data shall be kept for no longer than is necessary for the purpose of processing.

Data security (Article 5(1)(f))

Personal data shall be processed in a manner that ensures appropriate security, including protection from unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR will introduce a mandatory data breach notification regime across the EU (in the UK, voluntary notification is encouraged, but other Member States may already have mandatory notification) (*Article 33*). This will require a controller to notify the regulator no later than 72 hours of becoming aware of a data breach likely to result in a risk to rights of individuals, and to notify individuals if the data breach is likely to result in a high risk to their rights (*Article 34*). Processors must also notify their controllers on becoming aware of any breach. Encryption of personal data (though not a mandatory requirement under the GDPR) would significantly mitigate the risk to individuals were a data breach to occur.

Accountability (Article 5(2))

The controller shall be responsible for and be able to demonstrate compliance with the above principles.

This is probably the GDPR's most significant new rule, because requires an organisation to demonstrate and evidence that it complies with the data protection principles. This must be done by way of internal governance, putting in place measures proportionate to the type of processing it does and the risks it may face.

Three new governance requirements are worth highlighting. First, there is an obligation to keep internal records of processing activities (*Article 30*). Second, there is an obligation to conduct a Data Protection Impact Assessment (DPIA) for processing likely to result in a high risk to the rights of individuals (*Article 35*). Finally, an organisation may be required to appoint a data protection officer (DPO) in certain circumstances, including if the processing is carried out by a public authority and where core activities of the organisation consist of regular and systematic monitoring of data subjects on a large scale (*Article 37*). The DPO's role includes informing and advising the organisation on data protection and monitoring compliance with the GDPR and the organisation's policies.

Data export (Chapter V)

The default rule of thumb is that no personal data can be transferred to a third country (outside the EEA) unless it has been formally designated as 'adequate' or the organisation uses one of an exhaustive list of mechanisms which provide necessary safeguards. Under the UK Data Protection Act 1998, an organisation could self-assess the adequacy of a recipient, but this will no longer be permitted.

Adequacy is particularly relevant for Brexit: if the UK leaves the EU, it will be a third country. The best way to enable data exports from the EEA to the UK would be for the UK to be formally designated as adequate.

Probably the most frequently used mechanism is the European Commission's model clauses. Existing model clauses will be 'grandfathered' under the GDPR until such time as new clauses are published[1]. Another (rarer) mechanism, 'binding corporate rules', can be used for intra-group transfers, and the GDPR will extend this to

[1] Article 46(5), GDPR.

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

apply to a group of enterprises engaged in a joint economic activity.

Exports to the USA remain a source of controversy. The current mechanism is the Privacy Shield, so transfers are permitted to US companies who have signed up to those principles. This was put in place after its predecessor 'Safe Harbour' mechanism was declared invalid by the CJEU after a challenge by an individual (Mr. Schrems) against Facebook's transfers to the USA in light of revelations about access by US national security bodies[14].

As a result of another challenge by Mr Schrems, the CJEU has now been asked by the Irish High Court[15] to consider the use of model clauses for data exports to the USA. There is a risk that any negative decision may cross-contaminate model clauses for transfers to other countries.

UNDERSTAND THE RELATIONSHIPS

The data controller and his data subject

Data protection law applies to the controller to ensure the individual's personal data is collected, used and protected in compliance with the law. The individual is also given rights against the controller, including the right of access to personal data relating to him (*Article 15*), to rectification of inaccurate data (*Article 16*), to object to direct marketing (*Article 21(2)*), and to not have automated decisions made against him which have legal effects (*Article 22*). The GDPR expands the list of rights, including a right to erasure (the right to be forgotten, an existing right under case law) (*Article 17*), to data portability (*Article 20*), to object to profiling (*Article 21(1)*), and to restrict processing (*Article 18*).

Under the GDPR, member states can provide that independent organisations acting in the public interest can make complaints and bring claims on behalf of individuals whose rights may have been infringed (*Article 82(2)*). The UK does not intend to bring this into effect, but there is pressure from consumer rights bodies to do so.

Tip box:

- Identify what is an existing right (whether arising out of legislation or case law), and what is a new right.
- Identify which rights are absolute, which rights are conditional (and the conditions), and exemptions.

The data controller and his regulator

A key change under the GDPR applies to organisations with more than one establishment across the EU. The GDPR will introduce a 'one stop shop' for enforcement - a Lead Supervisory Authority (LSA) located in the country of its main establishment will supervise all the processing activities of the organisation throughout the EU.

The reform which received the most attention is the introduction of fines of up to 4% of annual global turnover for certain breaches. However it is important to bear in mind that the GDPR also sets out various factors that must be taken into account before imposing any fine (let alone of that amount), including whether the breach was negligent or intentional, nature of the affected personal data, and steps taken to mitigate the damage (*Article 83*). The focus on fines means that there is a danger the other (more realistic) sanctions under the GDPR might be missed, such as the ability to impose a ban on processing (*Article 58*).

The data controller and his data processor

Under the Directive, a processor had no direct regulatory liability – he was, in effect, the agent of his principal (the controller) who was solely responsible for regulatory compliance. However, under the GDPR, a processor will have direct regulatory liability, an important change.

The GDPR will also extend the list of mandatory terms that must be included in a contract between a controller and his processor (*Article 28*).

The data controller and another data controller

The GDPR expressly envisages 'joint controllership' which is where two controllers jointly agree the purpose and means of processing (*Article 26*). The most important consequence of such a joint controllership is that the data subject can exercise his rights against either controller.

In the UK another relationship is envisaged - that of two controllers acting 'in common', each determining its own purposes and means of processing. Despite it being one of the most common relationships, it is not expressly discussed in the GDPR nor are there (as with processors) any mandatory contract terms.

TAKE ON THE GDPR

The knowledge manager plays a vital role in a law firm helping others. It is hoped the this article, and the suggested approach it outlines, will help the knowledge manager help others in this important area of law, but also to understand data protection as a fundamental right of every individual in the EU.

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

LEGISLATION LISTS

EU laws

- Data Protection Directive (*1995/46/EC*)
- The Privacy and Electronic Communications Directive (*2002/58/EC*) and Regulation (EU) 611/2013 on measures applicable to the notification of data breaches under the PECD. This will eventually be replaced by the E-Privacy Regulation.
- General Data Protection Regulation (EU) (*2016/679*).
- Directive on processing of personal data by competent authorities for law enforcement purposes (EU) (*2016/680*) (Law Enforcement Directive). The Law Enforcement Directive creates a parallel regime for processing by competent authorities, which are entities in public and private sectors who process personal data for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The private sector will be in scope where they are able to exercise public powers. This must be implemented by 06 May 2018 and will be implemented in the Data Protection Bill.
- Network and Information Security Directive (EU) (*2016/1148*). This must be implemented by 09 May 2018.

UK laws

- The Data Protection Act 1998 and its statutory instruments, including the Data Protection (Processing of Sensitive Personal Data) Order 2000 (*SI 2000/417*)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (*SI 2000/2699*), issued under the Regulation of Investigatory Powers Act 2000. This will be replaced by the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018, issued under the Investigatory Powers Act 2016.
- The Digital Economy Act 2017, for provisions allowing the ICO to impose a new registration fee (which falls away under the GDPR), rules on some public sector data sharing, and provisions requiring the ICO to publish a new statutory code of practice on direct marketing.
- The Data Protection Bill

Footnotes

[1] See the ICO's blog: [online] https://iconewsblog.org.uk/tag/gdprmyths/ Accessed 9/2/18

[2] See EU website: [online] https://europa.eu/european-union/law_en Accessed 9/2/18

[3] The Article 8 right to privacy in the European Convention on Human Rights right is not absolute – it must be balanced against other rights.

[4] The European Court of Human Rights: http://www.echr.coe.int. The ECHR publishes factsheets on the right to privacy: http://www.echr.coe.int/Pages/home.aspx?p=press/factsheets&c=

[5] Convention 108: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[6] The European Agency for Fundamental Rights (http://fra.europa.eu/en) publishes a *Handbook on European Data Protection Law* (2nd edition, June 2014).

[7] The Article 8 right to data protection in the Charter of Fundamental Rights of the European Union right is not absolute – it must be balanced against other rights.

[8] The Keeling Schedule is here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/648957/2017-10-02_GDPR_Keeling_schedule.pdf

[9] See the Guidance Index for Data Protection and Privacy and Electronic Communications on the ICO website: https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/

[10] See the Guide to the GDPR on the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

[11] The ICO incorporates WP29 guidance into its own maintained GDPR guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

[12] All WP29 Opinions and recommendations before 2017: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[13] All WP29 materials since 2017, including GDPR guidance: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[14] Case C-362/14 Schrems v Data Protection Commissioner

[15] Schrems v Data Protection Commissioner [2014] IEHC 310

https://doi.org/10.1017/S1472669618000051 Published online by Cambridge University Press

Biography

Sahar Bhaimia trained and worked a solicitor at Simmons & Simmons LLP in commercial, consumer protection, data protection, and IT law until 2007. After completing her Masters in 2008, she worked as an editor for Practical Law Company (a publisher of legal know-how) until 2014. Since then, she has worked as a contract lawyer and professional support lawyer on various assignments covering commercial, consumer protection (particularly recent consumer law reforms), data protection, and retail finance. Her current assignment is in-house as a data protection and privacy lawyer.

Legal Information Management, 18 (2018), pp. 28–34

doi:10.1017/S1472669618000063

Data Protection in UK Library and Information Services: Are We Ready for GDPR?

Abstract: Against a backdrop of increasing data security and privacy concerns, current data protection law will soon be overhauled by the General Data Protection Regulation (GDPR). Previous research has indicated a lack of data protection management in libraries, however, it has been nine years since the latest study. This article by Josephine Bailey aims to provide an updated review of the extent of data protection management in UK library and information services and gauge preparation for the incoming GDPR.
Keywords: data protection; privacy; General Data Protection Regulation; GDPR; libraries

INTRODUCTION

This article is drawn from a recent Master's thesis at the University of Sheffield Information School. Thank you to everyone who participated in the survey for making this research viable.

PRIVACY V SECURITY

Online privacy and security, or the lack of it, is becoming a growing concern. In 2017, YouGov surveyed participants about their internet use and reported that 66% of respondents were concerned about cybercrime, 49% were concerned about cyberattacks and 39% were concerned by companies collecting and sharing personal data[1].

The same poll found that while 26% thought more should be done to protect privacy, an opposing 32% felt more should be done to fight crime at the cost of privacy and 24% thought the current balance was just right.

Such awareness is likely fuelled by recent high profile cybercrime and data breach incidents. In 2017 alone, well known organisations such as BUPA, Wonga payday loans, Three Mobile, Sports Direct and NHS England Trusts have suffered large data breaches compromising millions of records containing personal information.[2]

The Office for National Statistics began reporting cybercrime as part of the Crime Survey for England and Wales for the first time in 2016 and reported 2.5 million cases of bank account or credit card fraud and nearly 2 million cases of computer misuse offence, which includes unauthorised access to personal information, hacking and intentional spreading of malware or viruses[3].

In addition, the Information Commissioner's Office enforcement page provides a constant parade of businesses,