The Data Protection Officer

Profession, Rules, and Role

Paul Lambert

"Excellent resource" – Jan Philipp Albrecht

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

The Data Protection Officer

Profession, Rules, and Role

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

The Data Protection Officer

Profession, Rules, and Role

Paul Lambert

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20161021

International Standard Book Number-13: 978-1-138-03193-7 (Hardback)

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

CONTENTS

SECTION 3 ROLE

SECTION 4 TASKS

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

GUIDING POINTS FOR DATA PROTECTION OFFICERS

☐ Preparing for the New Data Protection Regime

- Consider current reporting channels, and any required amendments.
- Consider any amendments to contracts of employment.
- Consider changes required by and necessitated to the current processes and procedures of the organization.
- Spread awareness and acceptance of the new data protection regime throughout the organization.
- Consider inward-facing data protection issues, employees, and human resources (HR), as well as outward-facing issues affecting customers and users.
- Identify and consider the data held by the organization.
- Communicate the updated data protection policies and related information as appropriate within the organization, and to customers and users.
- Review the rights regime under the new GDPR, and appropriate changes that are necessitated.
- Review current access requests and consider any amendments required to the process as well as the time frame.

- Consider future deletion, takedown, forgetting, and erasure issues and requests.

- Review the personal data collected and aggregated, and the legal basis for processing such data.

- Consent issues and recordal need to be reviewed in detail in light of the new data protection regime.

- Children are expressly referred to in the new data protection regime, and the organization needs to consider if, how, and why it may seek to collect the personal data of children.

- Data breach incidents are increasingly problematic and some of the considerations for dealing with same are now encompassed in the new GDPR, including preparedness, risk, and reaction issues.

- Data protection by design and by default, and also data protection impact assessments, needs to be embraced within the organization, and will need to have appropriate information disseminated as a result.

- Transfer and international issues will be important for certain organizations, and when personal data are involved, particular additional considerations apply under the new data protection regime (in addition to issues such as the new EU-US Privacy Shield, etc.).

☐ New DPOs

New DPOs may also wish to consider the following:

- Ensure that his or her contract is compliant with the new data protection regime.

- Ensure that he or she is reporting to the appropriate level of management in accordance with his or her duties, tasks, and function, and in accordance with the new data protection regime.

- List or map out all departments within the organization.

- Identify the head or contact point within each department.

- Meet the head or contact point of each department.
- Pay particular attention to departments who interact with personal data and data protection issues more than others.
- Identify and map the categories of personal data collected, used, and stored by the organization, by which departments, for what purposes, and where the data are stored.
- Review current procedures and policies.
- Consider required amendments and updates.
- Review current access requests and other requests.
- Review data deletion policies and consider appropriateness and updates.
- Consider current issues and queries from other departments.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Data Protection Officers (DPOs) play a fundamental role in helping to ensure a high level of data protection.

European Data Protection Commissioner
EDPS website, at https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/dpo_corner

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

ABBREVIATIONS

DPO Data protection officer

DPD95 The Data Protection Directive 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

GDPR The General Data Protection Regulation; EU Data Protection Regulation (Regulation [EU] No. 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR)

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

SECTION 1

A New Profession

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

CHAPTER 1

New Role: New Impact

Introduction

The newly created position of the corporate data protection officer (DPO) is empowered to ensure that the organization is compliant with all aspects of the new data protection regime. Organizations must now appoint and designate a DPO for the organization. This will be a significant appointment and will have long-term benefits for the organization. The specific definitions and building blocks of the data protection regime are enhanced by the new General Data Protection Regulation (GDPR) and therefore the new DPO will be very active in passing the message and requirements of the new data protection regime throughout the organization—including the benefits. It will also be important to highlight the potential cost of getting data protection wrong.

The Parties

Organizations need to understand the concepts and parties involved in the data protection regime. The data protection regime involves a number of key parties, namely

- Individuals: Referred to as "data subjects." It is their personal information and personal data that are being protected

- Organizations: Referred to as "controllers," those who wish to collect, use, and process individuals' personal data

- Outsourced Organization: Referred to as "processors." The main controller organization has outsourced or delegated some of its processing activities to a third-party organization; for example, payroll processing regarding employees, or marketing or market research regarding current or prospective customers

In addition, organizations need to consider the following in relation to data protection compliance and data protection issues that arise, namely

- Data protection officer: The individual office holder in the organization tasked with ensuring data protection compliance, education, and so on. He or she is frequently the general point of contact within the organization for queries regarding personal data.

- Board member: Organizations should ensure that data protection compliance is prioritized at organizational board level. The DPO should regularly report to this board member.

- IT manager: Given the importance of security for personal data enshrined in the data protection regime, the information technology (IT) manager needs to be appraised and involved in assisting compliance.

Personal Data Use and Compliance

Appreciation of and compliance with the data protection regime in relation to personal data is important. First, everyone has personal data relating to them. Second, every organization and entity collects and processes personal data of individuals. Sometimes, this is on a small scale. Sometimes, it is on a massive scale. Data protection compliance obligations apply to all organizations, whether small or large, commercial enterprises, official government organizations, or even charities. Obligations also apply to the primary organization involved (the

"controller" organization) as well as to outsource entities such as agents, consultants, processors, and so on.

Furthermore, the instances where personal data are used are ever increasing. For example, every reservation, booking, transaction, and journey involves personal data. Every organization that one deals with, whether governmental, enterprise, or nonprofit, uses or creates data in relation to the person. The volume of such personal data collection and processing is now even more significant with the advent of digitization, social media, and e-commerce. Many commercial organizations realize the value of personal data. Increasingly, new business models are relying on personal data.

The default position is that organizations must inform individuals that they intend to collect and use their personal data, detail the purposes for which the data will be used, and obtain consent to do so. Frequently, tensions arise when organizations do not do this, or seek to do it in a manner that does not fully or transparently respect the rights of individuals. While compliance is always possible, there are many instances of organizations getting it wrong and facing the consequences of audit, penalty, prosecution, or investigation.

Personal data also need to be considered in terms of inward-facing (e.g., relating to employees) and outward-facing (e.g., relating to customers) personal data. Different mechanisms may apply to how organizations deal with personal data, depending on the type of data involved.

☐ What Data Protection Is

Data protection laws protect the personal information of individuals, that is, the personal data of and in relation to individuals. It is therefore similar, in some respects, to privacy. The data protection regime provides a regulatory protection regime around personal information, privacy, or personal data. Personal data are data or information that relate to or identify, directly or indirectly, an individual. Data protection is, in many respects, wider than privacy and confidentiality. Personal data are defined in the European Union (EU) Data Protection Directive 95/46/EC of 1995 (DPD95), the national data protection laws, and now in the new GDPR.

The data protection legal regime governs if, when, and how organizations may collect and process personal data and, where permitted, for how long.

This applies to all sorts of personal information, from general to highly confidential and sensitive. Examples of the latter include sensitive health data, sexuality data, and details of criminal offenses.

The data protection regime is twofold, in the sense of

- Providing obligations (that are *inward facing* and *outward facing*), which organizations must comply with.

- Providing individuals (or *data subjects*, as they are technically known) with various data protection rights that they, representative organizations, and/or the data protection supervisory authorities can invoke or enforce as appropriate. Significantly, the ability to invoke data protection rights on behalf of individuals by privacy groups and collective nongovernmental-type organizations is new (see the new GDPR, replacing the DPD95). The GDPR brings "comprehensive reform"* to the data protection regime and "will put an end to the patchwork of data protection rules that currently exists in the EU."†

Organizations, as part of their compliance obligations, previously had to register or notify the national supervisory authority in relation to their data processing activities (unless exempted). This compliance obligation in the national data protection laws and the DPD95 is changed in the new GDPR. Now, there is generally no need for general registration, unless coming within special categories of data protection risk activities. These activities potentially require a specific amendment to the national data protection laws to reflect the new data protection regime.

Certain sections of industry and specific activities (e.g., data transfers abroad, direct marketing [DM], etc.) have additional data protection compliance rules.

In terms of individuals, they can invoke their rights directly within organizations, with the supervisory authority, and also with the courts in legal proceedings. Now, particular requests may also be made by representative organizations on behalf of groups of individuals. Compensation can also be awarded, and injunction relief can also arise.‡ In addition, criminal offenses can be prosecuted. Data protection compliance is therefore very important. Indeed, penalties are significantly increased under the new data protection regime.

---

* "In Brief," *Communications Law* (2012)(17) 3.

† EU Commission, Press Release, "Agreement on Commission's EU data protection reform will boost Digital Single Market," 15 December 2015, at http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

‡ Such as in Sunderland Housing; Kordowski and Microsoft v. McDonald (t/s Bizards). Sunderland Housing Company v. Baines [2006] EWHC 2359; Law Society v. Kordowski [2011] EWHC 3185; Microsoft Corp v. McDonald (t/s Bizads) [2006] EWHC 3410.

As regards the implementation of compliance frameworks, organizations must have defined structures, policies, and teams in place to ensure that they know what personal data they have and for what purposes; that they are held fairly, lawfully, and in compliance with the data protection regime; and that they are safely secured against damage, loss, and unauthorized access.

The cost of loss, and of security breach, can be financially significant, both brand-wise and publicity-wise. A 2015 IBM study estimated the cost of data breach to average $3.8 million per data breach incident. A data breach at the telecommunications company TalkTalk (in 2015) was estimated to cost £35 million. One Target (a US retail chain) data breach was estimated to cost $162 million, plus a 5.3% drop in sales. Breaches can also give rise to criminal offenses, which can be prosecuted. In addition, personal liability can be attached to organizational personnel, both separate and in addition to the organization itself.

Need for Data Protection

Why do we have a data protection regime? We have a data protection regime because of the legal and political recognition that society respects the personal privacy and informational privacy of individuals. In the context of data protection, this means respect for, control of, and security in relation to informational personal data. The data protection regime protects personal data relating to individuals, which includes employees, contractors, customers, and users.

Data protection exists in order to ensure

- Protection in relation to personal information
- Consent of individuals is obtained to collect and process personal data
- Security in respect of personal information
- Protection against personal informational abuse
- Protection against personal information theft and identity theft
- Protection against unsolicited DM
- Protection for the data protection rights of individuals

- Increased protection and recognition of certain technological threats and "big data" to individuals

The threats to personal data and informational protection (and privacy) have increased as the ease with which personal data can be collected and transferred electronically increases. This has increased further with digital technology, computer processing power, Web 2.0 (i.e., the second generation of Internet websites and services), aggregation, new signals, and social media.*

Growing Importance of Data Protection

Data protection compliance is important for all organizations, large and small. An example of this importance is the national supervisory authority investigation of various multinationals in relation to certain general and specific data protection issues. This example also emphasizes the significant and growing importance of data protection.† Some countries now specifically designate a minister for data protection. The budget of many national supervisory authorities has also increased. More international organizations are being approved under the EU binding corporate rules (BCR) procedure for exemption from the EU transfer ban in relation to personal data.‡

* Note, for example, the comments of one supervisory authority in relation to data protection by design and by default, and the report Privacy by Design at https://ico.org.uk. The GDPR refers to data protection by design and by default (DPbD) in Article 23.

† One example is LinkedIn. A facial recognition feature used by Facebook was turned off in Europe, partly as a result of the supervisory authority audit. The supervisory authority also reported that Facebook had introduced more transparent tools and preferences in relation to users' personal data, again apparently on foot of the supervisory authority audit. See audit reports at http://www.dataprotection.ie.

‡ For example, Intel is now approved under the BCR regime. The BCR procedure is one of the mechanisms by which an organization can export or transfer personal data outside of the EEA. Without the BCR (or a similar exemption mechanism), the organization would not be permitted to make such a transfer. These transfers are sometimes referred to as *transborder data flows*. The default position is that transborder data flows may not occur from the EEA to non-EEA countries, unless exempted. See supervisory authority commentary at http://www.dataprotection.ie/docs/20/1/12_Commissioner_approves_Intel_Corporation_Binding_Corp/1190.htm. Also Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (OUP, 2012).

The increasing "centralisation of information through the computerisation of various records" has made the right of privacy a fundamental concern.* Data protection is important, increasingly topical, and an issue of legally required compliance for all organizations. More importantly, it is part of management and organizational best practice. Individuals, employees, and customers expect that their personal data will be respected. They are increasingly aware of their rights, and increasingly enforce these rights. An editorial notes that "Privacy and data protection issues are never far from the horizon at the moment. There are waves of discussion in this area … and currently that wave is riding high."† The significant attention focused on the fallout of the EU-US Safe Harbor regime being declared void, its impact on transatlantic business, and the complex political negotiations required for the new EU-US transfer regime (entitled the EU-US Privacy Shield) highlight the mainstream significance of data protection law.

Data protection is increasing in coverage in mainstream media. This is due in part to the large number of recent data loss and data breach incidents. These have involved the loss of the personal data of millions of individuals by commercial organizations, and perhaps more worryingly, by trusted government entities.

The issue of online abuse, which involves among other things privacy and data protection, has also been hitting the headlines.‡

Data protection is also in the headlines because of national supervisory authority concerns with the damage of certain online permanent data. The Court of Justice, on foot of such concerns, issued an important decision in the *Google Spain* case and the right to be forgotten (RtbF; described later in this chapter) directing that certain personal online data had to be deleted from search engine listings.§

The Court of Justice also pronounced on the often contentious area of official data retention. This is the obligation placed by countries on Internet service providers (ISPs) to retain certain customer data in

---

* Personal Data Protection and Privacy," *Counsel of Europe*, at http://hub.coe.int/web/coe-portal/what-we-do/rule-of-law/personal-data?dynLink=true&layoutId=35&dlgroupId=10226&fromArticleId=.

† Editorial, Saxby, *Computer Law & Security Review* (2012)(28) 251.

‡ Tragically, such online abuse can and does result in and contribute to actual suicide. This is a particular concern in relation to children and teenagers. See, generally, Lambert, *Social Networking, Law, Rights and Policy* (Clarus, 2014); Lambert, *International Handbook of Social Media Laws* (Bloomsbury, 2015); and Philips, *This is Why We Can't Have Nice Things, Mapping the Relationship Between Online Trolling and Mainstream Culture* (MIT Press, 2015).

§ *See Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Court of Justice (Grand Chamber), Case C 131/12, 13 May 2014.

relation to telephone calls, Internet searches, and so on, so that (certain) official agencies can ask to access or obtain copies of such data in the future. Debate frequently surrounds whether this should be permitted at all, and if so, when and under what circumstances, how long ISPs must store such data, and so on. The strongest argument for an official data retention regime may relate to the prevention or investigation of terrorism. Serious crime might come next. There are certainly legitimate concerns that the privacy and data protection costs are such that official data retention, if permitted, should not extend to "common decent crime." On one end of the spectrum is the Court of Justice decision in *Digital Rights Ireland*, striking down the EU Data Retention Directive as invalid.* By implication, this also undermined certain national measures.† It remains to be seen how challenges to new data retention legislation may transpire, and how courts and policymakers will react. The various Snowden revelations and their ripple effects lean against the data retention regime, or at least an overly broad and overreaching one. In addition to debate on legitimate data retention, there is a separate but related debate‡ on encryption, encryption by default, encryption by service providers, personal

* Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Court of Justice, 8 April 2014. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L105, p 54). Rauhofer and Mac Sithigh, "The Data Retention Directive Never Existed," *SCRIPTed* (2014)(11:1) 118.

† For example, the Regulation of Investigatory Powers Act 2000 (RIPA) in the United Kingdom. The UK government proposed a new amending regulation entitled the Data Retention and Investigatory Powers Act 2014 (DRIPA). However, two MPs (David Davis and Tom Watson), successfully challenged DRIPA in the High Court. The court held that sections 1 and 2 of DRIPA breached rights to respect for private life and communications and to the protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The decision gave the (United Kingdom) government until March 2016 to rectify the DRIPA problems. The Queen's speech has also promised a "snooper's charter," which would replace DRIPA. See Whitehead, "Google and Whatsapp will be forced to hand messages to MI5," *Telegraph*, 27 May 2015, at www.telegraph.co.uk/news/politics/queens-speech/11634567/Google-and-Whatsapp-will-be-forced-to-hand-messages-to-MI5.html. Since then, a draft of the Communications Data Bill has been issued. No doubt argument, debate, and research will ensue. In relation to data protection as a fundamental right, see for example Rodata, "Data Protection as a Fundamental Right," in Gutwirth, Poullet, de Hert, de Terwangne, and Nouwt, *Reinventing Data Protection*? (Springer, 2009) 77.

‡ Especially, but not exclusively, in the United States and the United Kingdom.

encryption, and encryption back doors for law enforcement authorities.* This remains, if anything, a contentious issue.

However, every time there is a terror-related event, and at the time of writing we are in the immediate aftermath of the Brussels, Paris, Egypt, Palestine, San Berdino, and Mali attacks, the calls and arguments for data retention/extended data retention are at their strongest.†

While the issues of *official data retention* are important, they may not be direct issues for every DPO but can be more relevant to companies in certain technology sectors.

A further reason as to why data protection is important and increasingly the focus of press attention is that organizations are increasingly using security and respect for data protection as an advantage and commercial differentiator in the marketplace. Apple has repeatedly announced that it does not operate a data-intrusive model for collecting user data. In fact, it has even criticized some of its technology competitors. Microsoft has, for many years, promoted the data protection and privacy-friendly policy of data protection by design and by default (DPbD). Post Snowden, many US technology companies have been heavily lobbying the US administration for a roll back of certain activities and practices, particularly those felt to be extrajudicial and extralegal, on the basis that it will disadvantage the US-based cloud and cloud storage industry. Many cloud companies have been highlighting that they are non-US-based. Even US companies are now promoting that they have—or are building—EU-based cloud storage facilities, and in some instances that EU data will remain located in the EU.

All organizations collect and process personal data. Whether they are big organizations or new start-ups, they need to comply with the data protection regime. Bear in mind also that even a new technology start-up can scale relatively quickly to millions of users. Many issues enhance the importance of getting the organizational data protection

---

* A Harvard study suggests, inter alia, that an encryption back door would in any event be ineffective. See Schneier, Siedel, and Vijayakumar, "A Worldwide Survey of Encryption Products," (Harvard, 11 February 2016). Also Barrett, "Bill Aims to Stop State-Level Decryption Before it Starts," *Wired*, 10 February 2016. Also note Grauer, "The Government Wants to Listen In On Your Smart Home," *Wired*, 14 February 2016, referring to connected Internet of things (IOT) devices in the home.

† Prime Minister Cameron has made statements to advance data retention proposals, in particular the UK Communications Data Bill, labeled by some as a "snooper's charter." Critics also increasingly suggest that research indicates that data retention does not demonstrate that data retention works. However, official sources in various jurisdictions refer to terror attacks being prevented, and that retained data are invaluable. The link or proof of positive effect is not necessarily specified. This debate also crosses over to issues of unauthorized access or tapping by official agencies of technology companies and their customers' data, and public and industry arguments that official access must be regulated, transparent, and proportional.

understanding and compliance model right from day one. These include legal obligations; director, board and officer obligations; investigations; fines; prosecutions; being ordered to *delete* databases; adverse publicity on the front pages of the press media; commercial imperatives; and even commercial advantages. If one also considers some of the large-scale data breach incidents, there are examples of chief technology officers as well as managing directors/chief executive officers (CEOs) losing their employment positions as a result of the incident.

In addition, organizations often fail to realize that data protection compliance is frequently an issue of dual compliance. They need to be looking at both *inward* and *outward* data processing issues.

Internally, organizations have to be data protection compliant in relation to all of their employees' (and contractors') personal data. Traditionally, this may have related to human resources (HR) files and employee contracts, but now includes issues of electronic communications, social media, Internet usage, filtering, monitoring, on-site activity, off-site activity, company devices, employee devices, vehicles, and so on. The consequences of getting it wrong are now more significant.

Separately, organizations have to be concerned about personal data relating to persons outside the organization such as current and prospective customers. Comprehensive data protection compliance is also required for those outward-facing issues. The consequences are significant for noncompliance.

Substantial fines have been imposed in a number of cases. In some instances, organizations have been ordered to delete their databases. In a new technology start-up situation, the database can be the company's most valuable asset.

Until recently, the issue of data loss was a proverbial small back-page story. However, the loss of personal data files of tens of millions of individuals in a single instance—and including from official governmental sources—makes data loss a front-page issue. There is increased scrutiny from the supervisory authorities and others, and new regulation of data security issues, preparedness, and reactivity. Organizations must look at security issues with increasing rigor. Organizations can face liability issues in breach incidents, but also in the aggravating situation where a vulnerability may have been already known and highlighted internally but was not acted on, thus contributing to the breach incident. As well as official investigation, fine, and sanction, organizations also face issues of liability to users and, in some instances, potential liability to banks and financial intermediaries. Target, for example, was sued not just by data subjects but also by financial intermediaries. Issues such as this are likely to increase. While individuals have grouped together in US cases for some time, this will likely increase in the EU as the new

GDPR expressly recognizes the possibility of data subject representative organizations.

There are enhanced obligations to report data breaches, data incidents, and data losses.* There are also enhanced financial penalties. In some instances, personal director responsibility for data loss can arise. The need for compliance is now a boardroom issue and an issue of senior corporate compliance. Proactive and complete data protection compliance is also a matter of good corporate governance, brand loyalty, and a means to ensuring user and customer goodwill.

The frequency and scale of breaches of security, such as those for LoyaltyBuild, Adobe, TalkTalk, Target, Home Depot, Sony Playstation (70 million individuals' personal data in one instance and 25 million in another†), the Sony "Interview" breach, Office of Personnel Management (OPM) (US official; 22 million individuals), the insurer Anthem (80 million individuals), the affair dating website Ashley Madison (37 million individuals, apparently), the toymaker VTech, political parties, and even the security/hacking firm Hacking Team, make the topicality and importance of data security compliance for personal data ever more relevant. Even official agencies have been involved in data loss incidents involving the personal data of millions of individuals.‡ There are many cases involving substantial fines for data protection breaches. A number of hospitals and medical facilities have been fined, including one organization that was fined £325,000.§ Zurich Insurance was fined £2.3 million for losing data in relation to 46,000 individual customers.¶

---

* Unless exempted.

† See, for example, Martin, "Sony Data Loss Biggest Ever," *Boston Herald*, 27 April 2011, at http://bostonherald.com/business/technology/general/view/2011_0427sony_data_loss_biggest_ever; Arthur, "Sony Suffers Second Data Breach With Theft of 25m More User Details", *Guardian*, 3 May 2011, at http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

‡ The UK Revenue and Customs loss of discs with the names, dates of birth, and bank and address details for 25 million individuals. See, for example, "Brown Apologises for Record Loss, Prime Minister Gordon Brown has said he 'Profoundly Regrets' the Loss of 25 Million Child Benefit Records," *BBC*, 21 November 2007, at http://news.bbc.co.uk/2/hi/7104945.stm. Millions of personal details of government employees, including security personnel, were hacked in the United States in 2015.

§ The Brighton and Sussex University Hospitals NHS Trust had a fine of £325,000 imposed by the Information Commissioner's Office (ICO) in relation to a data loss incident. See, for example, "Largest Ever Fine for Data Loss Highlights Need for Audited Data Wiping," *ReturnOnIt*, at http://www.returnonit.co.uk/largest-ever-fine-for-data-loss-highlights-need-for-audited-data-wiping.php.

¶ See, for example, Oates, "UK Insurer Hit With Biggest Ever Data Loss Fine", *The Register*, 24 August 2010, at http://www.theregister.co.uk/2010/08/24/data_loss_fine/. This was imposed by the Financial Services Authority (FSA).