Information compliance and libraries: part 1

data protection[1]

Terry O'Brien

An Leabharlann
22–1
March 2013

Abstract

Data protection for librarians and information workers is considered in the context of information compliance, legal obligations and library values. This article seeks to address one specific aspect of information compliance – data protection (DP), and to give some practical insight into what we need to be aware of and what we need to know.

Keywords: *Data Protection, Libraries, Ireland; Information compliance, Ireland*

Introduction

Issues of privacy and personal information are very much a la mode at the moment not just in library and information work but in society generally. This is due to the relative ease of access to the internet, the willingness and apparent eagerness to 'share' (or conversely unawareness), the escalation of social networks, social media, mobile devices and online engagement and interaction.

In his most recent Annual Report (2011) the Data Protection Commissioner stressed the high demands put on the resources of his office in recent years. He attributes this to the presence of some of the world's largest technology companies in Ireland (and the

1 Part 2 dealing with Freedom of Information will appear in the October issue.

substantial requirements of the recent Facebook Audit), but also as a direct result of heightened awareness around the issues of personal information and data protection generally. There were 1,161 complaints in 2011, up 33% on 2010, 562 requests for access, 28 audits carried out and 1,167 data protection breaches (the most serious of which was by the HSE).

The consequences of an open and participatory internet have blurred the lines of privacy and what is perceived as private and personal information for many citizens. Those of us working in the library and information field have perhaps more than most, long-standing experience of managing information, and a general appreciation of the importance of ethical and compliant usage of information. With the increasing use of personal information, both our *own* and our *users*, either voluntarily or involuntarily, the corollary is that librarians are more and more dealing with issues of information compliance and the obligations that come with that. It is timely that information professionals give more consideration to the importance of what could broadly be called 'information compliance'. Information compliance is primarily concerned with the legal requirements and responsibilities of organisations in maintaining the confidentiality, integrity and availability of information under Freedom of Information (FoI) and Data Protection legislation. More widely it also refers to responsibilities around records management (often financial or retention related), archives and re-use of public sector information in the case of public bodies.

What is Data Protection about?

Data protection (DP) is essentially about individual rights to privacy. Companies, bodies, organisations hold personal information about us in many guises – data protection law means that this personal information must not be misused, must be accessible to us on request (with some restrictions), must be accurate, should not be passed on to anyone else without our consent and should be kept safely. This places firm duties and statutory responsibilities on those that hold this information – known as *data controllers* (or alternatively those that hold our personal information on their behalf – known as *data processors*). These obligations persist across the full 'life cycle' of this information from the initial gathering of the information to its final disposal. Increased public consciousness towards privacy and rights to personal information along with a number of high profile DP cases has resulted in data protection increasingly coming centre stage (e.g. the Facebook Ireland Audit Report, recent court cases with direct marketing companies, concerns about Google and its privacy policies, obligations placed on companies by the new 'cookie' laws).

Data protection is concerned with personal information; it applies to all public bodies and companies, both public and private. Whilst there continue to be many bodies exempt from the law under Freedom of Information legislation, there are no organisations exempt from data protection obligations (save for the DP office and the Office of the Information Commissioner). There are some restrictions in a general sense particularly if the data is of a sensitive nature or covered by legal privilege, but in the main data protection is universal.

Rules and definitions for data protection

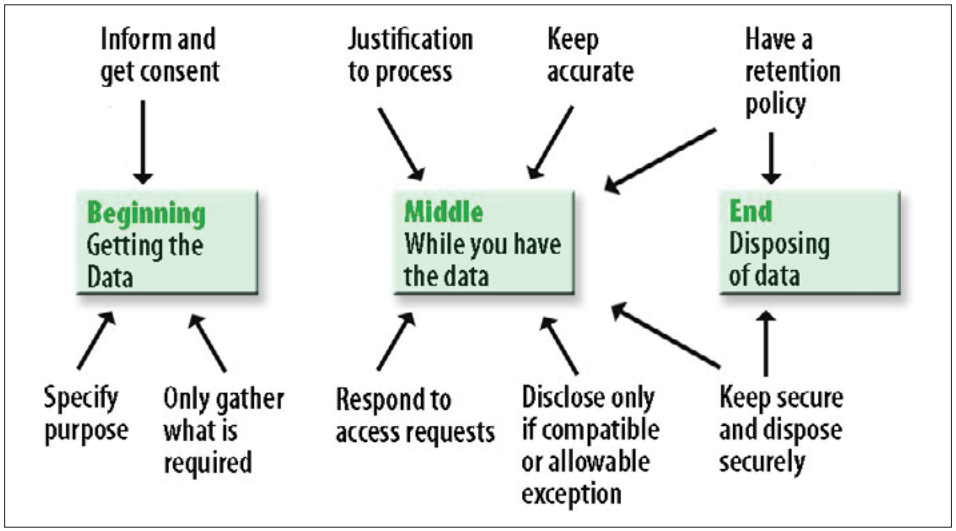
What do we mean when we speak about personal information or personal data? Personal information is unique information specific to an individual that allows that individual to be identified. Personal data is any data relating to a living identifiable individual. This data can be automated or manual (and structured in a way that makes data readily accessible). There are three equally important definitions central to data protection:

Data controller	Data processor	Data subject
"a person who controls the contents and use of personal data" *This can be a company, organisation, public body.*	"a person who processes personal data on behalf of a data controller" *This could be CCTV or outsourced functions such as payroll. In other words the data controller has in effect sub-contracted the controller function to another party. Processing is anything done with personal data from across its lifecycle from collection to disposal.*	"an individual who is the subject of personal data" *Must be living and identifiable.*

If personal information is required or sought there are a number of documented binding rules of data protection that should be applied:

- **Fair obtaining and processing** – data controller should give full information about identity, purpose and the fairness of the data involved. Consent is generally, though not always, required, but where information is sensitive then an explicit consent is usually necessary.
- **Specific purpose** – what is the purpose of obtaining the information? Importantly this cannot subsequently be expanded without reverting to the individual.
- **Non-disclosure** – there are some exceptions (Section 8 exceptions) relating to criminal investigations or legal proceedings, but normally information should not be disclosed for any purpose other than that for which the information was originally sought.
- **Safe and secure** – this is particularly important in the context of library and information workers. Personal data and information must be kept safe and secure. This means taking appropriate security measures, use of encryption if necessary, clear desktop policies, awareness of staff.
- **Accurate, up to date** – personal data should be accurate and not out of date irrespective of how long that data is kept. Data subjects have a right to have personal information errors rectified or erased.
- **Relevant and not excessive** – the key question here is what is really required? Do you need, or need to ask for the information – is it really necessary and proportionate? If it is not personal information clearly relevant to the requirement or service then the answer is no.
- **Retention period** – although there may be specific retention requirements for certain data, information should not be retained any longer than is necessary. For libraries, a clearly defined retention policy fit for purpose should be considered.
- **Right of access** – this is fundamental to data protection. It applies to manual and computer files. Individuals are entitled by law to know to whom data is disclosed, the source of that data, and the purpose for which data is processed.

The rights of individuals should not be compromised in relation to the giving of personal information. Individuals (data subjects) should expect, and are legally entitled to, fairness when giving information, to be able to get a copy of their personal information including computerised and manual files, to have incorrect or out-of-date information about them corrected. Individuals also have the right to opt of unsolicited marketing (mail, phone, web), check their credit rating and to make a complaint to the Data Commissioner.

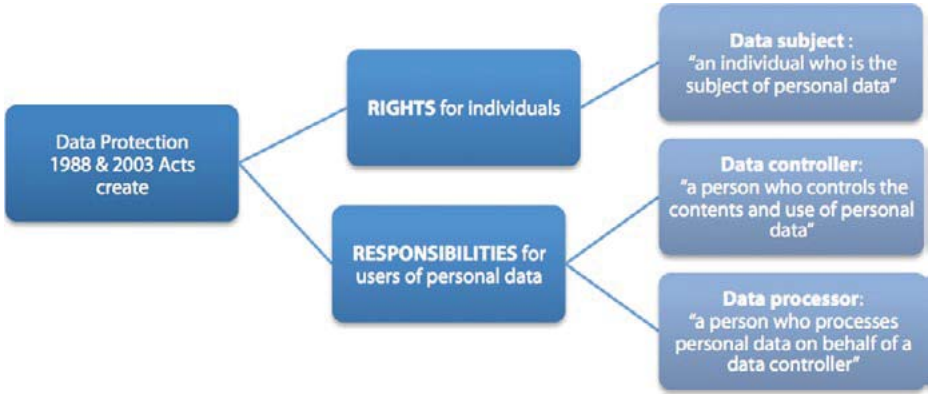


'Data Protection Life-Cycle' Source: DPC website

Policy context

The legal framework around Data Protection in Ireland is well established. Data Protection is a human right, part of the right to personal privacy. This right is not absolute and does depend on context. It can conflict with the rights of others, freedom of expression and depending on 'public interest' is generally superseded by FoI in law. There are two central pieces of legislation, both *rights-based* – the D*ata Protection Act 1988*, and the *Data Protection (Amendment) Act 2003*. Data protection rights are protected by the Irish

constitution[2] but also by a body of European legal instruments including the European Convention on Human Rights, the EU Charter of Fundamental Rights, DP directive 95/46/EC, EC Electronic privacy regulations, Electronic Communications regulations (2011), and ePrivacy Regulations 2011 which deal with data protection for phone, e-mail, SMS and Internet use, giving effect to the original EU ePrivacy Directive 2002/58/EC. Data protection also warrants mention across a range of legislative areas including the *Disability Act 2005*, the Lisbon Treaty and the Good Friday Agreement.



DPC Office and powers

The Data Protection Commissioner office was established in 1989 and has a wide remit with extensive powers. The role of the Commissioner is independent and covers four broad areas - ombudsman (resolution), enforcer (compliance) educational (promotion and advocacy) and registration. This role is generally consistent across the EU, with Commissioners working together in what is known as the Article 29 Working Party, to harmonise Data Protection rules. The DP Office also provides DP audit resources for organisations, a voluntary breach code and is extremely active in awareness raising and promotion. The DPC role involves devising codes of practice, providing wide ranging guidance notes, resources for schools, for individuals and groups, (case studies), audit, advice and public registration services. Powers are significant and although the DPC cannot award damages, it has considerable enforcement and investigative powers to ensure compliance, and can enter, examine and inspect premises. It can, and does, prosecute and can impose fines up to €250,000. The reputational damage to companies in the public eye can often far exceed the financial penalties but it is fair to say that the DPC generally gives every opportunity to comply amicably before a decision is taken to prosecute.

Dealing with an access request

The guidelines for dealing with an access request are clear, and both the rights of access and restrictions are robust. Applications must be in writing with sufficient information to identify oneself and in intelligible format. The Data Controller must comply within 40 days and may charge a minimal fee of no more than €6.35. If a data subject makes a request for the correction or deletion of personal information, no fee should apply. The scope of any request applies to all records in existence at the time of request irrespective of when the record was created. The Data Controller (organisation, company) should disclose all personal data held, the purposes for processing that data (personal information), persons to whom that data is disclosed and if necessary, the logic involved in automated decisions -this is because data protection does not allow decisions made solely based on automated processing of personal data.

Restrictions

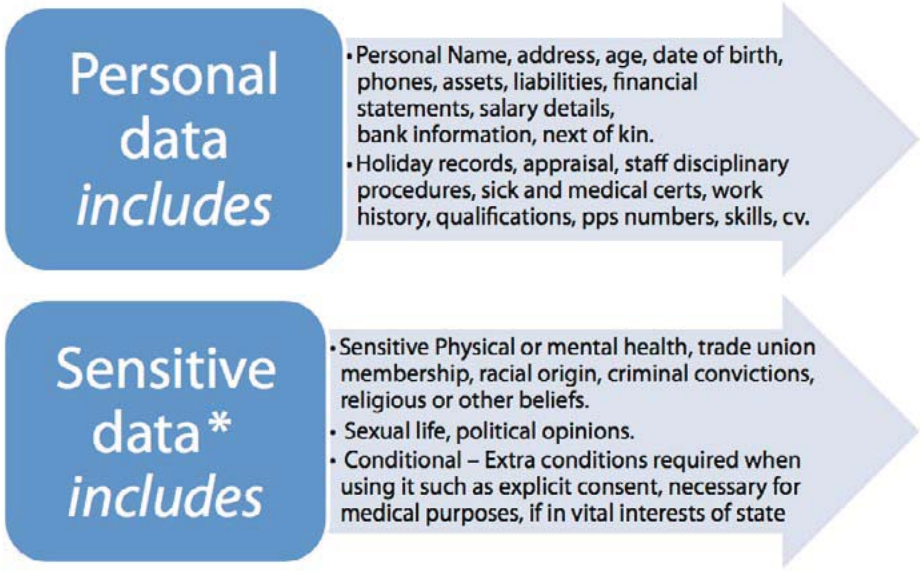
There are restrictions and exemptions to access requests but a high threshold is required. For example references are generally not exempt; interview panel notes and work performance reports are accessible. If the expression of an opinion was given in confidence or under the belief that it was confidential these would be exempt from access. Personal data relating to liability claims, international relations of the State, legal privilege and criminal investigation are amongst others exempt from access requests. There are special provisions that apply to health and social work data.

2 Article 40.3.1 - implicit rights to personal privacy

Consent

For a data controller or processor to release or disclose personal information to another party, consent is generally required. However it can be disclosed without consent if it involves the security of the state, investigating offences, by order of court, or to prevent injury or damage. Inherent in data protection is the presumption in favour of access to one's own data. Data subjects are entitled to expressions of opinion by third parties without third party consent, unless that opinion was given in or on the understanding of, confidence. Under data protection, protection of the individual's privacy is dominant, but the "public interest" test central to FoI legislation does not apply. The purpose of FoI legislation is to enable members of the public to obtain access to records held by public bodies to the greatest extent possible consistent with the public interest and the right to privacy.

Personal & Sensitive data



***Sensitive data may still be disclosed – if in the public interest (under FoI), if consent is given, if part of a criminal investigation or if part of an employment contract.**

Why is information compliance and data protection important to libraries?

Apart from legal obligations and moral responsibilities, it is self-evident that information compliance is intrinsically important for those working in and using libraries, whether public or private. Librarians are information professionals (often public servants, funded by the taxpayer), spending public money and in this regard transparency is imperative. Libraries use, acquire, mine, harvest people's information on our own and other people's behalf (vendors) or they on our behalf, and this brings obligations and duties. Libraries exist within wider organisational structures that have legal information compliance obligations even if the library itself does not have its own policies. Our customers are the public, we use their personal data – we must be accountable and trust is very important, despite the "tension between privacy issues and library's need to collect user data[3]". Libraries keep and retain records – are we clear about our obligations, do we need to keep this information, could we retrieve it if necessary? Although we are required to give users opt-in, opt-out options when it comes to reading history, do we do this? Do we retain patron information, borrower records for excessive periods? Do we know where the data on our ILS sits? The advent of cloud technology and third party hosting has made a complex area even more complex. Multi-tenancy hosting, data ownership, data preservation, service level agreements, international requirements if data is hosted in another jurisdiction, technical and legal issues are extremely convoluted and will require the development of increased expertise in the information professions so as to ensure that libraries and their users are not exposed. Libraries as data controllers, rather than processors, still retain the bulk of responsibility for ensuring the integrity, safety and accessibility of this data. More importantly our users perceive this. Libraries accumulate huge data banks from library systems and services – how this is potentially utilized is often outside our control, particularly where the

3 Coombs, Karen A. (2005) 'Protecting user privacy in the age of digital libraries', *Computers in Libraries*, v. 25, 6, 2005 http://www2.hawaii.edu/~donnab/lis670/coombs_2005.html

library is used as an intermediary to access externally provided content.

Privacy continues to be a key value to libraries,

Libraries have compliancy and confidentiality obligations like other public bodies, and private companies,

Many libraries now use multi-functional smartcards that are traceable and retain large amounts of personal information not just relating to the library but access to buildings, shopping, spending even location based networking,

Libraries recruit, interview and employ people like any other organisation – be aware of what this means and what the personal data implications are,

Libraries are involved in tendering and public procurement; it must be clear and transparent,

Information ethics and behaviours are part of our world - people who use (and work in) libraries should have an expectancy that we are doing things 'right' and not just copyright,

Libraries are seen as a positive social force, civic minded – libraries/librarians are traditionally compliant, conscientious professionals – it is important that we retain this integrity,

Libraries are at the forefront of technology, web 2.0 and social media applications – are we clear on the consequences and implications for privacy and personal information. With the advent of the participatory and user generated web – huge amounts of PII – 'personally identifiable information' is willingly displayed but do people understand (or care) about this? Do libraries? Do we have a role in this[4]; do we need to develop new information literacy skills for our users, for ourselves? Libraries traditionally have a culture of privacy, control, but this is shifting … How we would feel if something similar to the Patriot Act was imposed?[5]

4 Magnuson, L. (2011) 'Promoting privacy – online and reputation management as an information literacy skill', *College & Research Library News*, pp. 137-140, March, 2011.

5 http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact

Data Protection – what practical things can we do

- Awareness, education, training – if your organisation has a Data Protection, FoI or Information Compliance officer, ask them to come and speak with you. Attend seminars or workshops on data protection if possible. Visit the DPC website, download the best practice guides, there is a wealth of information and resources freely available.
- Promote a culture of strong records management, records retention when necessary, archiving, record keeping.
- Put a statement on your website stating what information your gather, how you gather it, if your relevant third party vendors have data protection policies upload them, whether you use analytics services, mailing lists, email lists, SMS alerting etc. This is positive, transparent and pre-emptive (Sligo County Library Service[6] is a good example).
- Check if your organisation has got an up to date DP policy? Have you read it? Do you know what to do in the event of an access request under DP or who to contact?
- If you work in Higher Education, it is likely that there will be an institutional research ethics committee to monitor and evaluate the impact of research on its participants – data protection forms a key part of this particularly in the sciences, health research and social sciences. Librarians are ideally placed to input into these groups.
- If you require personal information or data, make sure it is proportionate and always seek consent at the point of capture on registration forms, applications, websites, online forms etc.
- If there is a data protection breach inadvertent or not, seek to remedy damage before it escalates and becomes a serious issue resulting in potential enforcement and civil liability. Notify the DPC immediately and inform clients (stakeholders) without delay.
- Use common sense – make staff and library users aware of DP policy, make sure staff have clear desk and screen, use lock & key for sensitive information, password protect, encrypt files and computers, dispose and destruct data when required and in an environmentally sustainable way.
- Use security measures for data taken off-site (check with your DP Officer if you are unsure).
- If working in Health libraries or libraries that interface with particularly sensitive data and personal information, be aware that there are additional obligations on you and that personal information of vulnerable groups are afforded more protection. Similarly those carrying out research in these areas have increased responsibilities.[7]

Data Protection in summary

Organisations or individuals that hold your personal data owe you a duty of care. In short this means:

- Data Protection has high privacy thresholds.
- Compliance is a legal requirement for all organisations, public and private.
- Any personal information/data held should be accurate.
- Organisations should have an understanding of data protection and awareness of their obligations – contact the DPC if you need assistance.
- Personal data should be retained no longer than necessary.
- Data subjects have rights of access to personal data on computer and manual data.
- Data should only be available to those that need to have it and used only for specified purposes
- Outsourcing of functions does not diminish responsibilities - obligations still apply
- Security should be appropriate to potential harm and nature of data. Encryption is particularly important in the case of financial and personal records, and for vulnerable groups (children, OAPs).

6 See http://www.sligolibrary.ie/sligolibrarynew/text/DataProtection/

7 See http://www.dataprotection.ie/documents/guidance/Health_research.pdf

AL
An Leabharlann
22–1
March 2013

- It is generally good and sensible practice to have procedures in place before problems arise and protocols if problems arise – this avoids negative publicity, potentially damaging liability, enforcement orders from DPC, and worse - reputational damage.

In conclusion

It is equally important to know that data protection is not based on an anything goes approach. Not all access is permissible, and although I have highlighted the high privacy thresholds for personal information, there are occasions in which we should say no or at the very least seek clear consent. Library staff should have clear disclosure awareness around the following areas – external companies, marketing companies, even alumni organizations should have explicit consent to access personal data or information (and by this I mean access to a personal phone number, email, home address etc.). Police also require consent even though this is quite common for vetting and recruitment purposes. Similarly most DP policies will have a clear protocol on how to deal with an enquiry from police even if consent is not necessary in the course of a criminal investigation. Other areas to be cognizant of include CCTV (should be proportionate, for specific use, only kept for 28 days and clearly advised), and specific guideline for biometrics which is gradually mainstreaming into schools and public spaces such as museums. It would seem that monitoring of employees in certain circumstances without consent can be legitimate although it may depend on policy or conditions of employment. This can relate to acceptable email usage, social media and internet usage. It is not a free for all - monitoring should be proportionate, not unduly intrusive and should be based on reasonable grounds. There may also be a little irony in that many people seem content to 'share' extremely personal information and images (knowingly or unknowingly) on social media platforms, where privacy is in reality a fallacy, yet seem perturbed if their usage is monitored in the workplace, unpleasant as that may feel.

There have been a significant number of high profile DP breaches and prosecutions over the last number of years. In addition to high impact, high publicity interactions with Google (privacy and street view) and Facebook, (Twitter, Instagram, LinkedIn have all had their own 'privacy' related backlashes internationally too), the Irish DPC has taken prosecutions against Tesco, An Post, Dell; against public bodies such as local authorities, the Revenue service for inappropriate accessing of files by staff, against the Department of Education and Skills for misuse of trade union details in order to withhold pay. Insurance companies, telecommunications/mobile operators and the Banking sector have been seriously tackled in recent years. Investigations are listed publically. There have been major DP breaches in the Bank of Ireland, the HSE, the Department of Social Protection amongst many more. This name and shame approach can result in very adverse reputational and business damage for those listed, as happened in 2008/9 when the M50 toll company as it was at the time subsequently lost its contract. It is important to stress that prosecution is very much a last resort for the DPC.

Terry O'Brien, MA, DLIS, (PhD candidate at University College London) is Deputy Librarian at Waterford Institute of Technology[8]

Further reading

- Data Protection Commissioner www.dataprotection.ie
- Re-use of Public sector information www.psi.gov.ie
- Office of the Information Ombudsman www.oic.ie
- Goldner, Matt "Winds of Change : Libraries and Cloud Computing", EMEA Regional Council Meeting 2010 http://www5.oclc.org/downloads/presentations/EMEA_Regional_Council_2010/matt.pdf
- O'Brien, Terry " Information Compliance – FoI, DP and libraries", presented at the European/Irish Innovative Interfaces conference, Institute of Technology Blanchardstown, June, 2009 http://www.slideshare.net/TerryOBrien100/infocompliancejune25-autosaved

8 Currently on secondment as EU Projects Manager at the South-East Regional Authority. Previously worked as Information Compliance Officer at Waterford Institute of Technology.

Rare books in Irish Libraries:

an investigation of current challenges in providing access to historical collections

David Parkes and Clare Thornley

Abstract

Special collections are a long standing part of library history but the changing nature of libraries and their associated technologies have led to new challenges. This article aims to identify the challenges facing the preservation of rare books in Irish Libraries and to determine if these are similar to those discussed in related international research.[9]

Keywords: *Special Collections, Ireland*

9 Based on a Masters in Library and Information Management dissertation (Parkes, 2011), Dublin Business School.

Introduction

In their influential publication, *Exposing Hidden Collections* (2004), Jones and Panitch explored these issues in the light of the changed technological and political context and provided a new and important focus on the role of special collections and rare books. Their work on special collections prompted the Association of Research Libraries (ARL) to set up a Special Collections Working Group which raised awareness of many of the challenges facing the preservation and cataloguing of rare books. These challenges include

- the uncoordinated approach to rare book collecting and digitization efforts
- the existence of 'hidden collections'[10]
- competition for scarce funds
- diminishing budgets

These problems, identified by the ARL bring into question the survival of historic records which are crucial in accurately understanding and

10 Hewitt and Panitch (2003) define 'hidden collections' as 'unprocessed archival, manuscript, and rare book materials.'

AL
An Leabharlann
22–1
March 2013