Data Protection: Compliance in Practice

is published by Ark Group

UK/EUROPE OFFICE
Ark Conferences Ltd
Paulton House
8 Shepherdess Walk
London N1 7LB
United Kingdom
Tel +44 (0)207 549 2500
Fax +44 (0)20 7324 2373
publishing@ark-group.com

NORTH AMERICA OFFICE
Ark Group Inc
4408 N. Rockwood Drive
Suite 150
Peoria IL 61614
United States
Tel +1 309 495 2853
Fax +1 309 495 2858
publishingna@ark-group.com

ASIA/PACIFIC OFFICE
Ark Group Australia Pty Ltd
Main Level
83 Walker Street
North Sydney NSW 2060
Australia
Tel +61 1300 550 662
Fax +61 1300 550 663
aga@arkgroupasia.com

Editor
Evie Serventi
eserventi@ark-group.com

Head of content
Anna Shaw
ashaw@ark-group.com

Managing director
Jennifer Guy
jguy@ark-group.com

UK/Europe marketing enquiries
Robyn Macé
rmace@ark-group.com

US marketing enquiries
Daniel Smallwood
dsmallwood@ark-group.com

Asia/Pacific marketing enquiries
Steve Oesterreich
aga@arkgroupasia.com

ISBN: 978-1-908640-07-9 (hard copy)
978-1-908640-08-6 (PDF)

Copyright
The copyright of all material appearing within this publication is reserved by the author and Ark Conferences 2011. It may not be reproduced, duplicated or copied by any means without the prior written consent of the publisher.

ARK1905

Chapter 1: The Data Protection Act in plain English

Busting the jargon

Few people will actually have a copy of the Data Protection Act 1998 (DPA)[1] on their desks at work. It is very legalistic: full of jargon and appearing to go around in circles. The DPA constantly refers back to other parts of itself, and thus the user goes through a long, winding trail to determine what it is trying to say among different schedules, principles and sections.

If you bust through all these schedules and principles, the DPA essentially says that you must retain personal data if someone gives it to you, keep it accurate and up to date, and get rid of it when you no longer need it. This latter requirement is one on which many people are lax. In addition, you must let people have access to their own data and only share it when you are allowed to do so by law.

In public services in particular, where money is not attached to this data, organisations can be extremely poor at keeping information accurate and up to date, and at getting rid of data. They have lacked adequate resources and there are often fragmented structures in large organisations that have built up their own access databases, or they have databases that are many years old. They might send out mass mailings and get 50 per cent of the letters back marked 'Not at this address', but do not have the resources to remove these details from the databases. Undoubtedly, this will also be the case in some private companies, too.

Some organisations may also find that they have databases and systems from which data cannot be deleted; once the records are there, they are there for good. There might be an archive facility, but the older versions of these facilities were not designed to deal with deleting records. If an individual states that they want you to delete their record – which they are entitled to do – and if you have no business reason to keep it, you must consider what will happen if you cannot delete it. This includes thinking about when you should put new IT systems in place, and whether or not they have the facilities to archive and delete records.

Principles of the DPA

There are eight principles of the DPA that you must always abide by and come back to:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Schedules in the DPA

The very first principle of the Act often immediately confuses staff as it states the following: Personal data shall be *processed fairly* and *lawfully* and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Referring immediately to another part of the Act that you need to look up starts sending you off in circles. In plain English it means that for normal personal data you must be able to say one of the following is applicable:

- The individual who the personal data is about has consented to the processing.
- The processing is necessary:
  - In relation to a contract which the individual has entered into; or
  - Because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's 'vital interests'. This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the 'legitimate interests' condition.

For *sensitive* personal data you must also have a condition from Schedule 3, which is usually consent from the person to process their data, as well as one of the above conditions. This must be explicit opt in.

Other conditions in Schedule 3 are as follows:

- The individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of: the individual (in a case where the individual's consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld).
  The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.

- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Sensitive personal data

Sensitive personal data means personal data consisting of information as to:

- The racial or ethnic origin of the data subject;
- His political opinions;
- His religious beliefs or other beliefs of a similar nature;
- Whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- His physical or mental health or condition;
- His sexual life;
- The commission or alleged commission by him of any offence; and
- Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The ICO website now gives quite comprehensive guidance about all the different aspects of the DPA and examples of what it all means. See http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx.

Rewriting the Act

The DPA comes from the European Data Protection Directive (95/46/EC), which is currently under consideration for an overhaul. An Article 29 Working Party is looking to modernise the DPA in Europe because it is not fit for purpose. It was written in the 1990s before IT really took off and, as a result, had paper-based files in mind; it did not cater for transferring data through CD-ROMs and via the internet. In an ideal world, when the Directive is amended, the DPA could be rewritten it in a simplified way that people understand.

The EU Justice Commissioner Viviane Reding, vice-president of the European Commission and the German Federal Minister for Consumer Protection, Ilse Aigner, have come forward with a joint statement claiming that proposals to reform the 1995 Data Protection Directive will be published by the end of January 2012. (European Commission, MEMO/11/762, Brussels, 07 November 2011) Kenneth Clarke, UK's Cabinet Minister responsible for data protection indicated in a recent speech, however, that the UK will oppose any radical changes proposed to the DPA. (Speech by Lord Chancellor and Secretary of State for Justice Rt. Hon Kenneth Clarke MP26th May – source: http://www.justice.gov.uk/news/features/feature260511b.htm.)

There are a number of modern issues to do with cookies, a separate electronic addendum from 2003 and points from other acts that will need to be considered in the new DPA. For example, the Government may look at privacy because we do not currently have a privacy act in the UK; how such an

act would tie in with human rights issues would be a further consideration. It is not a straightforward job to ensure that the issues faced by the UK fit in with the rest of Europe.

Who controls the data? Controllers and processors

If you collect data on behalf of your organisation, you are a controller. You must be registered with the Information Commissioner as a data controller, and this must be renewed every year for a fee depending on the size of your organisation; it might be £35 for a sole trader or £500 for a large organisation. If that data is then outsourced to a company that puts the data on its server, that company is the processor. It has not collected the data and is not using it for its own purposes, but processing it on your behalf. To notify go to: http://www.ico.gov.uk/for_organisations/data_protection/notification/notify.aspx.

You can complete a notification online, print it out and send it to the ICO. You must include the notification fee or your direct debit instruction to The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

You can also ask the ICO to send you a notification form by emailing notification@ico.gsi.gov.uk. They will send you a notification form for you to fill in.

You can telephone the notification helpline on 0303 123 1113 between 9.00am and 5.00pm, Monday to Friday. You will be asked to provide your name, address and contact details, and to specify the nature of your business. They will then send a notification form to you

If you give data to someone under an information sharing agreement and they can use it for their own purposes, control can change. People are only just starting to understand that the original controller does not always have to be the only controller. The Article 29 Working Party has put together a very helpful document looking at who is the controller throughout an entire process, and how it changes along the way[2]. The group came to the conclusion that there is no absolute answer; it is different in every case. There is no finite answer in data protection because it is based on legal interpretation, which can be very frustrating for data protection officers. However, as long as you can show why you came to your decision and give a valid argument, the ICO will not censure you; it might disagree with you decision, but will see that you made a value judgment based on the facts you have.

References

1. For the full text of the Data Protection Act 1998 visit: http://www.legislation.gov.uk/ukpga/1998/29/contents.
2. Article 29 Data Protection Working Party, Working Paper No169, as a part of the World Data Protection Act report, 16 February 2010.

Chapter 2: Interaction with other laws

The Human Rights Act 1998

As well as the DPA, there are a number of other laws that affect data protection. In relation to CCTV there are the Human Rights Act 1998 (HRA)[1] and the Regulation of Investigatory Powers Act 2000 (RIPA)[2] because privacy is becoming increasingly important. Although people want CCTV cameras to help them feel safe, they do not want to be spied upon; getting that balance right is very difficult.

People are becoming much more aware of using the HRA because of the potential value of claims; for an alleged breach of the DPA you could be taken to small claims court, which costs only £30 but the case is likely to be dismissed unless you can prove damage and distress, often in financial terms. With the HRA, however, breaching privacy can result in a significant case. Several high profile cases in recent years have started out tentatively as data protection cases, but the introduction of human rights issues proved crucial to the eventual outcome. Naomi Campbell was photographed coming out of a Narcotics Anonymous meeting[3] and, as is often the case with celebrities, the press argued that the subject matter was in the public interest and that she was in a public place, coming onto the street; street scenes are usually deemed fair game. But the Court decided that the photograph was an invasion of her privacy because it clearly showed where she had been, and that in turn clearly identified that she had a drugs problem. Campbell eventually won the case. JK Rowling took the press to court over her child being photographed (*Murray v Big Pictures (UK) Ltd*, 7 May 2008). She said, "I am fair game and I do not mind people photographing me in the street. I am a celebrity and I have chosen that, but my child has not consented, and on behalf of my child, I am saying he has a right to privacy." You will see in photographs now that her children's faces are blurred.

Unlike in Europe, there is no privacy act in the UK. When Sarah Ferguson had her toes sucked by John Bryan, the story was widely reported in the tabloids. That was perfectly acceptable in the UK due to freedom of the press; that right was won in the original DPA. Ferguson was able, however, to sue under privacy laws in France when the photographs were published there and she and Bryan won $2.1m. Princess Caroline of Monaco also sued the press in Germany for taking photographs of her on the beach (*Von Hannover v Germany* [2004] ECHR 294).

Until the UK has a privacy act, a balance between data protection and human rights must be achieved by the courts.

Freedom of Information Act 2000

The FoIA applies not only to the public sector but also to organisations in the private sector which carry out statutory functions. This includes, for example, organisations that run parking enforcement for councils and have statutory functions such as providing traffic wardens in order to do this, or waste disposal companies carrying out statutory

waste management functions on behalf of Councils. Organisations carrying out such work, which would otherwise be carried out by a public sector organisation, are covered by FoIA; private companies are increasingly required to think about what information they might have to release.

The FoIA came into force on 1 January 2005 and was, initially, a cumbersome additional task on top of many people's day to day roles. Nobody had really known what it would mean or how big it would be. Since then it has become a full time job for many people. Because there are so many requests for information that contain personal data, it quickly became apparent that there is a considerable amount of data protection embedded within the FoIA; it is difficult to imagine that any FoI officer can get through their job without having an in-depth knowledge of data protection.

When dealing with requests for information, it is important to determine whether they should be considered under FoIA or under DPA instead. For some FOI requests, there may be disagreement as to whether the information is 'personal information' and therefore whether or not it can be released. It is a somewhat grey area. The current Government is keen on transparency, pushing for the publication of more information and more data, and has recently published a code of conduct for transparency.[6] The drive began with councils but the police, fire services and NHS have to publish their spend every month when it is greater than £500. That is a tiny sum for some organisations; it could be thousands of transactions every month. The administration required can therefore be very burdensome, particularly when the FoI officer must decide what can be published when personal and commercially sensitive data is contained therein.

The public sector is increasingly making payments to individuals. With the personalisation agenda in social care and health, that money is given to individuals to buy their own services rather than having carers sent to them. We cannot, then, have monthly accounts showing that Mr Smith receives £575 a month for his mental health needs: that is personal, sensitive data and cannot be revealed. Data must be reviewed line by line if systems are not set up to do this, and all such personal data must be redacted. To complicate matters, a name might denote either an individual or a sole trader. If it is the latter then it is probably fair game for publication, but how do we know whether they are a sole trader or not? Every individual name would need to be looked at on a case by case basis to determine if it could be published.

The commercial sensitivity of some transactions also has to be considered. Imagine, for example, payments being made to a concert hall by a council. There are real commercial sensitivities because the council is in direct competition with private companies in other cities to attract the best artists to the area, and there are individual payments made to artists. Can these payments be disclosed if an artist is not registered as a company or a sole trader? The BBC, for instance, never states what it has paid to individual artists for their performance on a given night. There are many such issues to consider when deciding what can and cannot be released.

Regulation of Investigatory Powers Act 2000

The RIPA was brought in primarily to deal with terrorism and to regulate covert surveillance against terrorists. It can also be used for other matters such as catching fly-tippers and dealing with

security issues when protesters are on construction or demolition sites. Leicester City Council used RIPA during the controversial demolition of a very old bridge in Leicester. Members of local history groups decided to protest, so the council had to deal with site security for both the people protesting around the bridge and the security personnel on site by carrying out surveillance. Councils may also carry out fraud benefit investigations where every avenue has been followed in terms of tracking down an individual who claims that they are not working, or claims to be living at an address as a single occupant. RIPA is sometimes used in such circumstances to permit covert surveillance. Organisations' loss prevention and fraud teams may use surveillance when large insurance claims are made against them, perhaps to make sure that the claimant has not exaggerated the extent of his or her injuries, although this is a very time-consuming activity and must be carried out correctly. Such surveillance has to be proportionate and necessary in order to be legal.

RIPA is concerned with direct, covert surveillance. It is not about CCTV cameras in the street which capture people going about their daily business; it is about the specific targeting of individuals without their knowledge. If you know the names of such individuals, or know that they will be frequenting certain addresses, evidence captured will be inadmissible in court unless you have the correct RIPA application in place. Moreover, if this is not done properly, the individual in question can claim your actions are a breach of their human rights and right to privacy.

Within a public authority organisation there are usually only one or two people who can sign off RIPA applications, and they have to go through quite intensive training. The current Government now wants only magistrates to have the power to sign off applications.

Practical applications of RIPA – Case studies

The following examples illustrate how RIPA can be used in different situations.

Customer data – Car park organisation

"We had one incident around our season ticket books, which is all customer data. One of our employees downloaded the customer data onto her laptop. She took this data, sent it on to her home address and then went to work with a competitor. We then got a complaint from a customer saying he parked with us and had just had a flyer posted to his home address. It was pretty obvious, so we did covert surveillance on her. We wanted to identify whether she was going to work for a competitor and it was going to go right the way through: we hired a big solicitor and it cost us quite a lot of money. As it turned out, we told her either to give us this data back or we would get an injunction against her to stop her using this data."

Employment Practices Code

The Employment Practices Code (the Code)[7] is not law, but it is good practice. It provides that if you see something by chance on CCTV – you were not looking for anything specific, but in the course of looking you saw a member of staff doing something wrong – then you can use that as the basis to investigate. For people working with staff and HR, the Code provides some useful information about using employees' personal data. It touches on recruitment and selection for HR and in keeping employment records, but what can we do in relation to monitoring? Can we look at employees'

e-mails and check when they come in and out of the building? Can we use CCTV to ascertain what they are doing after work when everyone else has left?

Issues to consider in relation to employee monitoring – Case studies

Scenario one

"I tried to do a disciplinary to show that somebody was using work time to do their outside work. She was doing 'English as a second language' classes for a local college, and the staff around her in the open plan area could see what she was doing on the computer. They saw that she was constantly doing work, printing things out and stealing stationery; it was non-stop but we could not quite get the evidence. Her supervisor at the time had access to her e-mails for a week when she was off sick and went through her e-mails without any permission from anybody. The unions immediately said, 'You cannot do that'."

Unless you follow the proper procedures through audit, you cannot go in and read someone's e-mails – even if your policy states that you should not use your work e-mail for personal use. If you see a title on an e-mail that makes you suspicious, you *must* go through the proper process to investigate. You cannot open the e-mail. There have been instances where individuals have won cases because their organisation has gone into their account and opened an e-mail. This is a tricky area, and you need to have clear internal policies and guidance to let employees know what is expected of them.

Scenario two

"We have been monitoring with covert surveillance after work. The owners believe that one of the premises officers is stealing. We cannot catch him at it but, wherever he works, things go missing so they have moved him around to different buildings. The pattern is there, but we cannot quite get him."

The issue here is what you can do within this remit, and what you need RIPA for. The employer is probably not going to prosecute the individual, and RIPA probably does not come into play, so what are they allowed to do using the Code without breaching his privacy rights and human rights when there is no other way to catch him? Look at collateral intrusion into other people, and whether or not you will not be filming other people; has everybody else has gone home by the time the employee is on his own? Even if there are CCTV signs stating that you are being filmed at work, this is a grey area.

Public registers

Is it not just councils that hold public registers. Some organisations hold them on behalf of councils; for example, the Royal Society for the Prevention of Cruelty to Animals (RSPCA) might hold the stray dogs register. If something is on a public register, then people cannot object to its publication. The law says that your name will be published, whether it is because you have handed in or collected a stray dog, or you have put in or objected to a planning application. There are some public registers on which your data appears whether you like it or not; it is important to make people aware of this because they can get very upset about planning, regarding objections in particular. If you object to a planning application anonymously it may not be taken into account but, if you put your name to it, it will remain on file for all to see. Obviously this can result in animosity if the objection is to a neighbour's property, for example.

With the ever-increasing improvement of technology, and fast searching tools such as Google, it is easy to see people online. The stray dogs register was, in the past, a

large handwritten book kept out of town; few people would choose to go and inspect the register. The minute the information is online, it is easily searchable. Modern online tools and technology can 'spider' information from here, there and everywhere, and it is an automated process. People can become upset about their data being online because it is so easily accessible and, once it is online, is almost impossible to remove.

However, remember that registers containing personal information do not necessarily have to be published online. If the legal requirement is to make them available for inspection, they can still be contained in an accessible book. The stray dogs register is a classic example: why would putting this online be a problem? But for owners of a stolen pedigree dog, if the register displays the address to which it was returned, it could be stolen again. In addition, anonymised and aggregated data could become identifiable if mapped against other publicly available registers. These types of issues must be considered when dealing with personal information on public registers.

Individuals can take the initiative to opt out of lists, or include the minimum amount of data necessary. In some instances it is necessary to seek out the check box that prevents information from being shared; in the case of sensitive personal information such options should automatically default to private, requiring the user to opt in if desired. This issue is discussed further in Chapter 5.

References

1. The full text of the Human Rights Act 1998 is available at http://www.legislation.gov.uk/ukpga/1998/42/contents.
2. The full text of the Regulation of Investigatory Powers Act 2000 is available at http://www.legislation.gov.uk/ukpga/2000/23/contents.
3. *Campbell v MGN Limited* [2005] UKHL 61.
4. The full text of the Freedom of Information Act 2000 is available at http://www.legislation.gov.uk/ukpga/2000/36/contents.
5. See www.irms.org.uk.
6. 'The code of recommended practice for local authorities on data transparency', Department for Communities and Local Government, published 29 September 2011.
7. The Employment Practices Code is available from the ICO website; see http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/employment.aspx.