Data protection: Guidelines for the use of personal data in system testing

Second edition

Louise Wiseman
Jenny Gordon
## Contents

**Foreword**

<table>
<thead>
<tr>
<th>Introduction</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data in the e-commerce environment</td>
<td>1</td>
</tr>
<tr>
<td>The Data Protection Act 1998</td>
<td>1</td>
</tr>
<tr>
<td>Processing under the DPA</td>
<td>2</td>
</tr>
<tr>
<td>The Principles: Key obligations</td>
<td>2</td>
</tr>
<tr>
<td>Personal data and sensitive personal data</td>
<td>2</td>
</tr>
<tr>
<td>Conditions for processing (Schedule 2 and Schedule 3)</td>
<td>3</td>
</tr>
<tr>
<td>The Information Commissioner</td>
<td>4</td>
</tr>
<tr>
<td>Notification</td>
<td>4</td>
</tr>
<tr>
<td>Fair collection of data: The privacy notice</td>
<td>4</td>
</tr>
<tr>
<td>Rights of individuals</td>
<td>5</td>
</tr>
<tr>
<td>The importance of system testing</td>
<td>6</td>
</tr>
<tr>
<td>Types of system testing</td>
<td>6</td>
</tr>
<tr>
<td>Reasons for undertaking live testing</td>
<td>7</td>
</tr>
<tr>
<td>The Information Commissioner's view</td>
<td>7</td>
</tr>
<tr>
<td>Key risks in system testing</td>
<td>7</td>
</tr>
<tr>
<td>A cautionary tale</td>
<td>8</td>
</tr>
</tbody>
</table>

**System testing and data protection compliance**

| Principle 1 – Fair and lawful processing | 11 |
| System testing – Purpose or subsidiary function? | 11 |
| Interpreting fairness | 11 |
| Non-obvious purposes | 12 |
| Non-obvious purposes: Data from the Electoral Register | 12 |
| Alternative test groups | 13 |
| Other privacy-related obligations | 13 |

| Principle 2 – Processing for specified purposes | 15 |
| Notification | 15 |
| Lawfulness | 15 |
| Data sharing | 15 |

| Principle 3 – Adequate, relevant and not excessive | 17 |
| Matching and cleansing data | 17 |
| National identifiers | 18 |

| Principle 4 – Accuracy | 19 |
## Contents

**Principle 5 – Retention and disposal**  
21

**Principle 6 – Rights of individuals**  
23

**Principle 7 – Security**  
25  
- Organizational measures  
- Governance  
- Accountability and ownership  
- Policy  
- Embedding data protection within the IT structure  
- User Developed Applications (UDAs)  
- Adequacy and audit  
- Privacy Impact Assessments (PIAs)  
- Physical protection of the system  
- Segregation  
- Technical measures: Test environments  
- Choosing a test environment  
- Testing by data processors  
- BS 27001  
- Remote working  
- The use of dummy or test accounts  
- Limiting the data  
- Business continuity  

**Principle 8 – International transfer**  
33  
- Outsourcing: Maintaining control  
- Offshoring: Ensuring compliance  
- Breaches of the DPA: What to do if things go wrong  
- Breach notification  
- What to report  
- Sanctions  

**Conclusion**  
37

**Appendix 1 – Factors to consider in approaching a testing strategy**  
39

**Appendix 2 – Risk analysis**  
40

**Appendix 3 – Net and gross risk**  
42

**Appendix 4 – Data classification table**  
43

**Appendix 5 – Data justification table**  
44

**Appendix 6 – Example system testing policy**  
45

**Appendix 7 – Blank form templates**  
47
Foreword

Since the publication of the first edition of these guidelines, business practice and technology have continued on a path of rapid change and expansion. Developments in IT have made complex types of data processing possible in response to changing business need. More personal data than ever is being captured and used on a daily basis across a wide range of industries, for a variety of purposes, and in geographical locations all over the world.

Increased use of data has increased the risk of that data being lost, damaged, destroyed or corrupted and the reality of this has been clearly seen in recent years. The UK alone has seen a number of very serious, large-scale and high-profile breaches of data security that have affected large numbers of individuals, as well the reputations of the organizations responsible. Although these data security breaches may not have directly resulted from data being used in system testing, they have helped to bring data security and data protection issues to the forefront of the public agenda. Heightened public awareness coupled with increased vigilance on the part of regulators now mean that organizations should take data protection seriously if they want to maintain customer confidence and competitive advantage.

Systems that process personal data must be secure. Most organizations put a lot of resources into buying and developing their systems and databases, yet give substantially less attention to vital system testing. These guidelines aim to show the importance of planning and devoting time and resources to any testing regime to ensure it is carried out in a safe, data protection-compliant way.

By showing how to integrate testing into an organization’s governance structure, these guidelines will help ensure data protection in system testing becomes second nature and is regarded as an essential part of an organization’s activities rather than an afterthought that requires special effort. In so doing, these guidelines may help data controllers turn the need for greater control over personal data into an opportunity to drive improvements in the quality of testing and the strength of governance within their organization.
Introduction

Personal data in the e-commerce environment

The growth of e-commerce has seen a rise in the use of personal data across an increasingly aggressive and geographically expanding marketplace. Personal data is easier to obtain than ever before and rapid developments in business technology constantly open up new, exciting and complex possibilities for the gathering and processing of that data.

With increased use, comes increased potential for misuse and thus the need for stronger controls and greater responsibility on the part of the data controller. Legislation and regulation have developed in tandem with e-commerce to increase the safeguards afforded to the privacy and freedoms of the individual and to control the use of personal data. The attendant increase in public awareness of data protection, in particular the rights it affords to the individual, means that data protection compliance is ever more vital to the continued success of business today.

Most companies across all business sectors, regardless of their size or turnover, have systems that process some personal data; this raises many issues around security and data protection. Even in the more traditional business environment it is increasingly hard to avoid the use of automated processing, and the simplest of small-scale computer systems must operate in line with the DPA in just the same way as larger, more sophisticated operations.

The Data Protection Act 1998

The Data Protection Act 1998 (DPA) gives effect in the UK to EC Directive 95/46/EC which came into being with the aim of harmonizing data protection legislation throughout the European Community. The DPA applies to ‘personal data’, which is data about identified or identifiable living individuals. A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed is known as a ‘data controller’.

The identified or identifiable individual who is the subject of the personal data is the ‘data subject’. They need not be a UK resident or a UK citizen. They could be anyone who is anywhere in the world. Any person other than an employee of the data controller who processes data on behalf of the data controller is a ‘data processor’.

The strength of the DPA lies in placing contractual obligations on data controllers, giving rights to data subjects and empowering an independent commissioner, the Information Commissioner, to oversee compliance with the law.

---

1 The full text is available online at http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm
2 For a full definition of ‘data’ and guidance as to whether any particular item falls within that category, refer to BS 10012:2009, Data protection: Specification for a personal information management system.
3 Definitions taken from BS 10012:2009, Data protection: Specification for a personal information management system.
Introduction

Processing under the DPA

The DPA refers to the ‘processing’ of personal data. ‘Processing’ includes almost anything that can be done with data, from obtaining it through to destroying it and includes everything that comes in between. This includes activities such as recording, storing, retrieving, consulting or using, disclosing, sharing, blocking, erasing and transporting the data as well as altering it in any way.

The Principles: Key obligations

Under the DPA, data controllers must:

• abide by the eight data protection principles; and
• unless exempt, notify the Information Commissioner of their data processing.

The eight data protection principles that lie at the heart of the DPA say that data must be:

• fairly and lawfully processed;
• processed for limited purposes;
• adequate, relevant and not excessive;
• accurate;
• not kept longer than necessary;
• processed in accordance with the individual’s rights;
• secure;
• not transferred to countries without adequate protection.

Personal data and sensitive personal data

Personal data is defined by the DPA as data that relates to a living individual who is identified or identifiable from that data or from that data and other information that is in the possession of, or likely to come into the possession of, the data controller. In addition to personal data, the DPA creates a category of ‘sensitive personal data’, which requires additional protection and may only be processed in very limited circumstances. Sensitive personal data is defined in section 2 of the DPA as:

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

Definitions taken from BS 10012:2009, Data protection: Specification for a personal information management system.
Schedule 2 of the DPA sets out six conditions for processing personal data, and all processing must satisfy at least one of these criteria. In addition to one of the conditions in Schedule 2, any processing of sensitive personal data must meet one of several specific conditions set out in Schedule 3 of the DPA.

**Conditions for processing (Schedule 2 and Schedule 3)**

As well as being fair and lawful, when processing any personal data the data controller must be able to satisfy at least one of the following six conditions as set out in Schedule 2 of the DPA:

- The processing takes place with the consent of the data subject.
- The processing is in the context of a contract or pre-contractual negotiations with the data subject.
- The processing is necessary for the data controller to comply with a legal obligation.
- The processing is necessary to protect the vital interests of the data subject.
- The processing is necessary for the administration of justice, the exercise of a function under an enactment, the exercise of a function of the Crown, a minister of the Crown or a government department or the exercise of a public function in the public interest.
- The processing is necessary for the purpose of legitimate interests pursued by the data controller or a third party to whom the data is disclosed, except where the processing is unwarranted because it would prejudice the rights and freedoms of the data subject.

Where the data to be processed falls into the category of ‘sensitive personal data’, the data controller must also fulfil one of the following criteria as laid out in Schedule 3:

- The processing takes place with the explicit consent of the data subject.
- The processing is necessary for performing any right or obligation imposed by employment law.
- The processing is necessary to protect the vital interests of the data subject or another person and consent cannot be given or cannot reasonably be sought.
- The processing is carried out in the course of the legitimate activities of a non-profit making organization which:
  - exists for political, philosophical, religious or trade union purposes;
  - processes personal data in a way that safeguards the rights and freedoms of data subjects;
  - does not disclose personal data to third parties without the data subject’s consent.
- The information has deliberately been made public by the data subject.
- Subject to any additional conditions set by the Secretary of State (none at the present), the processing is necessary:
  - for the purpose of, or in connection with, legal proceedings;
  - for the purpose of obtaining legal advice; or
  - for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary for:
  - the administration of justice;
  - the exercise of a function under enactment;
  - the exercise of a function of the Crown, a minister of the Crown or a government department.
Introduction

- The processing is necessary for medical purposes, processed by a health professional or someone who, in the circumstances, owes a duty of confidence equivalent to that which would be owed if they were a health professional.
- Subject to any additional conditions set by the Secretary of State, the processing relates to racial or ethnic origin and is to identify or review equal opportunities policies in order to promote or maintain such opportunities and the processing is carried out with appropriate safeguards for the rights and freedoms of data subjects.

The Information Commissioner

The DPA created a public official known as the Information Commissioner. The Information Commissioner’s duties are to:

- interpret and enforce the data protection principles;
- maintain a register of data controllers;
- prosecute offenders;
- promote good practice on matters of data protection.

The Information Commissioner’s Office (ICO) offers a telephone helpline for queries from data controllers and the public. The UK Information Commissioner also enforces the Freedom of Information Act although there is a separate Information Commissioner for Scotland who is responsible for the Freedom of Information Act (Scotland) but not for data protection legislation.

Notification

In order to process personal data, all data controllers must be properly registered with the Information Commissioner, except where they are able to claim a valid exemption. The process of registering with the Information Commissioner is known as ‘notification’ and requires the data controller to provide certain details about the processing they intend to undertake. The Information Commissioner maintains a public register of these details.

Notification must be renewed each year and updated with any change in processing. The DPA introduces a number of specific criminal offences related to notification including failure to notify, failure to keep a notification up to date and processing contrary to notification.

Fair collection of data: The privacy notice

Fairness to data subjects lies at the heart of the DPA. In order for processing to be fair, the data controller must, subject to limited exemptions, provide the individual with certain information when collecting personal data. This should be provided by means of a privacy notice (commonly known as a ‘fair processing notice’ or ‘fair collection notice’) detailing the intended uses of the data. This notice must be very carefully drafted as future processing will be limited by its content.

5 See the Information Commissioner’s website http://www.ico.gov.uk, for guidance on implementation of the DPA.
Introduction

As a minimum, the privacy notice must state the identity of the data controller, the purposes for which the data controller will process data and any other information necessary in the circumstances to make the processing fair. This means any unexpected or unusual uses of the data must be clearly stated. In deciding what to include in the notice, the data controller should consider the possible consequences of the processing for the data subject. The notice should be expressed in terms that data subjects are likely to understand and it should be displayed with sufficient prominence: it must not be hidden away in ‘the small print’.

The ICO’s Privacy Notices Code of Practice,6 emphasizes the importance of clarity and simplicity in the drafting of privacy notices and stresses that they should be used to inform individuals and not simply as a means of protecting the organization from liability. Technical jargon should be avoided and the notice should be worded in clear, simple language that people can easily understand.

The Privacy Notices Code of Practice stresses that organizations must not mislead the public or offer choices they cannot understand or that will not be honoured, and that any unusual or unexpected uses of data should be clearly explained. On the other hand, it states that there is no need for an organization to go to great lengths to explain a purpose that is obvious to everyone.

The Privacy Notices Code of Practice recommends a ‘layered’ approach to the drafting of privacy notices, whereby the vital ‘headlines’ are positioned up front where they are obvious to the data subject, while other less important detail is placed elsewhere. Data subjects can then easily pick out the information they need to understand how their personal data is to be used, without being distracted by excessive detail.

Although it does not mandate any particular wording, the guidance in the Privacy Notices Code of Practice is clear and easy to apply. The ICO will use it to inform their approach to enforcement where they receive a complaint that personal information has been collected unfairly.

Rights of individuals

Just as the data controller has responsibilities under the DPA, so the data subject has rights. These are summarized below:

- Subject access: the right to have a copy of any data being processed that relates to the data subject.
- The right to prevent processing of the data subject’s personal data in circumstances where it is likely to cause unwarranted substantial damage or distress.
- The right to prevent processing of the data subject’s personal data for the purpose of direct marketing.
- The right, in certain circumstances, to require that no decision that significantly affects the data subject is solely based on automated processing.
- The right to compensation: in some circumstances the data subject may be entitled to redress from the data controller for damage or distress caused by a contravention of the DPA.
- Rights to rectification, blocking, erasure or destruction of personal data under certain circumstances.

6 Available from the ICO website: www.ico.gov.uk
Introduction

The importance of system testing

All automated systems and processes require thorough testing to maximize their benefits while minimizing the potential for damage to, or loss or destruction of, personal data. It is vital to ensure that all systems are robust and secure. From the point of view of the data subject, security of personal data is paramount and many would expect, and indeed assume, that every possible means of protection for that data is employed – including full system testing. From the organization’s point of view, any failure to protect personal data carries a potential financial cost by way of compensation and fines and a less tangible but often more serious cost in terms of lost consumer confidence and bad press.

System testing is the most reliable way of assessing the true security and robustness of a system and the data it processes, and it should therefore be a matter that affects any organization that processes personal data electronically. It is a key factor in achieving compliance with Principle 7 of the DPA as well as supporting compliance with the other seven principles of the DPA by helping to identify any areas of concern at an early stage in development.

This presents organizations with a dilemma. On the one hand, the quality of test data used will directly affect the reliability of the system testing carried out and therefore the effectiveness of the system or process being tested. On the other hand, the use of live personal data raises issues of security and data protection compliance. Squaring these two seemingly opposed issues can often seem an insurmountable problem.

Types of system testing

System testing may take one of the following forms:

- ‘Dummy’ data in a test environment;
- ‘Dummy’ data in a live environment;
- Scrambled or anonymized data in a test environment;
- Scrambled or anonymized data in a live environment;
- Live data in a test environment;
- Live data in a live environment.

The type of system testing that is performed will depend on the function of the system or process being tested. Where it is possible to carry out system testing using fictitious information or real data that has been scrambled or anonymized, this will always be the safest course of action. Either of these options poses little threat to the integrity of live personal data provided precautions are taken to ensure the test data remains separate from any live data so the two cannot accidentally become merged. Wherever possible, then, the use of fictitious, scrambled or anonymized information should be the first preference in any system testing regime.

This type of testing, however, is not always sufficient for effective and thorough system testing. There will be situations in which it is essential to use live personal data either in a test environment or a live environment (both situations are covered by the term ‘live testing’ throughout this document.) These guidelines seek to examine the issues around live testing, rather than testing which uses fictitious, scrambled or anonymized data.
Introduction

The flow chart in Appendix 1 gives a very high-level view of the process of determining which testing strategy is applicable in a particular situation, and the key factors to consider.

Reasons for undertaking live testing

These include the reasons given below:

• The particular type of data to be processed or the function of the system may require the use of live data in order to adequately test out its capabilities.
• Test environments may not be as fully built as live environments so certain components of a system may only be adequately tested in a live environment.
• It may not be possible to replicate a particularly specialized process within the test environment due to limitations on the process itself or the data it requires.
• Test environments may not be sized in proportion to the size of live databases, therefore live testing may be necessary to assess the scalability of a system.
• There may be configuration changes to the live environment that cannot be tested in any other way due to the limitations of the test environment.
• Project conflicts may mean that a test environment is only able to support accurate load testing for one project at a time, thus it may become essential to use a live environment. Planning a testing schedule well ahead and ensuring it is part of the organization’s software development life cycle or project life cycle will avoid such conflicts and help to make live testing less of a necessity.
• Practical reasons: time, tester resource and cost.

The Information Commissioner’s view

The ICO advises that the use of personal data for system testing should be avoided. Where there is no practical alternative to using live data for this purpose, systems administrators should develop alternative methods of system testing. Should the Information Commissioner receive a complaint about the use of personal data for system testing, their first question to the data controller would be to ask why no alternative to the use of live data had been found.

Key risks in system testing

There are a number of general risks that exist whenever system testing is undertaken using live data and/or a live environment. These are:

• unauthorized access to data;
• unauthorized disclosure of data;
• intentional corruption of data;
• unintentional corruption of data;
• compromise of source system data;
• loss of data;
• inadequacy of data;
• objections from customers.
Introduction

Any of the above risks can also lead to financial loss to the data controller and/or the data subject, and to reputational damage to the organization concerned. There will of course also be sector-specific risks faced by each individual business, each type of business and each system.

Before commencing any system testing, it is advisable for the data controller to undertake a Privacy Impact Assessment (PIA). This process, which is strongly endorsed by the ICO, helps an organization assess privacy risks in order to bring about potential solutions. It can be a very useful management tool if carried out at an early stage in a project. Although designed to aid compliance with the whole range of privacy legislation, including the DPA, the PIA is not specifically focused on the DPA itself. Depending on the scale of the testing, or of the overall project (where the testing is undertaken as part of a wider project), an organization may find it useful to supplement its PIA with a risk assessment specific to data protection risk and limited to the data that is to be used in testing. Examples of how this might be done in a way that enables identification of data protection risks, their possible impact and planned handling strategies, is given in Appendix 2 (Risk Analysis Table) and Appendix 3 (Net and Gross Risk). Blank versions of both forms are given in Appendix 7.

There is no statutory requirement to undertake a PIA, but central government departments are now required by the Cabinet Office to do so.

A cautionary tale

The view is sometimes expressed that system testing poses no real data protection problem as it takes place all the time with little apparent detriment to individuals. The following case study, which is based on a true complaint received by the ICO shows that the use of live data to test systems can indeed cause very real problems for individuals.

A pupil was away from home at boarding school. The pupil’s parents received a letter from the local hospital informing them that their daughter had been involved in a road accident. In fact, there had been no accident, but the hospital had been using live patient data to test a system for sending out letters to patients.

It is sometimes hard to see in practical terms that system testing can have effects that are detrimental to an organization. A further example, again based on a true situation, illustrates the potential for real financial damage to an organization.

A credit card provider carried out testing of a new process within its customer application procedure using a small amount of live customer data. Several days later, a customer notified the organization that they had received 17 credit cards in their name, each with a substantial credit limit, even though they had not applied for a card.

7 Refer to the ICO website, www.ico.gov.uk, for further guidance and the PIA handbook.
System testing and data protection compliance
Principle 1 – Fair and lawful processing

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.8

System testing – Purpose or subsidiary function?

System testing clearly falls within the DPA definition of ‘processing’. In order to assess compliance with the requirements of the DPA, the data controller must first decide whether system testing is the actual objective of the processing or simply one function of a wider objective. On the whole, system testing will not itself be a ‘specified purpose’ in terms of the DPA but will rather support the purposes of processing. For example, where the specified purpose is administration of customer accounts, it will be supported by a number of subsidiary functions, one of which will be system testing.

Where this is the case, it is the larger, overall purpose itself that must satisfy the fairness and lawfulness criteria demanded by Principle 1. It is not necessary to justify individually each subsidiary element of that purpose by reference to those criteria or to Schedule 2 and Schedule 3. If the necessary Schedule 2 and/or Schedule 3 conditions are met for the larger purpose, they will usually cover all the constituent elements of that purpose.

There will be situations where system testing is the purpose of processing. For example an organization that designs and develops IT systems is likely to undertake a significant amount of system testing on a sufficiently regular basis to render system testing one of its primary purposes. Assuming personal data is used for the testing, the organization’s notification to the ICO would need to state system testing as one of its purposes. That system testing would then need to meet the criteria for processing laid down in Principle 1.

Data controllers should bear in mind that the totality of their processing must satisfy Principle 1. Any unfair element in the system testing process, or indeed in any other process, will mean that Principle 1 is breached regardless of whether the overall purpose is essentially fair.

Interpreting fairness

Schedule 1, Part 2 of the DPA provides guidance on interpreting Principle 1 and states the need to consider the way in which personal data is obtained. In particular there is a need to consider whether the person from whom it is obtained has been deceived or misled about the reasons for processing the data.

---

Principle 1 – Fair and lawful processing

The data controller must consider whether sufficiently detailed information about those reasons has been provided to the data subject. If system testing constitutes a major use of the data subject’s data and they have been told little or nothing of this, the processing cannot be considered to be fair. Where the data subject has given consent to processing, it is unlikely that their consent is fully informed (and freely given) unless system testing has been specified as a purpose and explained to them or unless the data subject can be reasonably expected to anticipate that system testing will be carried out. In making this assessment of fairness, the data controller needs to consider the likely perception of the data subject, particularly where processing is legitimized by consent. This may depend on the cross-section of data subjects whose data is being used. A customer base made up of IT professionals is likely to be more aware of the routine nature of system testing than an average cross-section of the general public. Society is changing, however. Children grow up using IT in the classroom and at home and the majority of people are accustomed to using computers at work, at home and even on the move. Arguably, then, the average adult today is reasonably aware of computer technology and the ways in which it is used.

Non-obvious purposes

Where data subjects are unlikely to anticipate that their data may be used in system testing, it may be necessary – or at least prudent – to inform them. Although data subjects do not need to be notified of each and every element of the processing performed on their personal data, they must be notified of any unusual purposes. The ICO's guidance is that in assessing fairness the paramount consideration must be the consequences of the processing to the interests of the data subject.

It is certainly in the interests of data subjects that their data should be processed on systems that are robust and secure. Since system testing is an inevitable prerequisite for this, it is unlikely to be contrary to the interests of the data subject.

Earlier guidance provided under the previous Data Protection Act of 1984, as applied in the Innovations Mail Order case of September 1993, also states that ‘personal information will not be fairly obtained unless the individual has been informed of the non-obvious purpose or purposes of the processing’.

In deciding whether system testing is a ‘non-obvious’ use of data, it is important to look at the context in which it takes place and the purposes which have been notified by the organization. Again, it may also depend on the likely perception of the data subject. There is nothing to be gained by informing the data subject of a purpose that should be obvious to him in the context in which he provides his personal data. For example, an online retailer need not inform customers that their name and address will be used for the purpose of processing and despatching their order, since that is clearly an obvious purpose.

Non-obvious purposes: Data from the Electoral Register

In certain sectors, companies may draw data from the electoral register for use in testing. Although the data contained in the electoral register is published information in the public domain, this may count as a non-obvious use of data if the data subject would not be likely to expect it.
Since the introduction of the Representation of the People (Amendment) Regulations 2002, there have been two versions of the electoral register, a full version and an edited version. Everyone who provides their details in the electoral canvass is included in the full register, which is available only for certain statutory purposes and to credit reference agencies. The electoral canvass offers individuals the choice of opting out of appearing on the edited register, which is available for general sale and is often supplied to marketing organizations. System testing using data from the full electoral register will be acceptable only in extreme and very limited circumstances and when it occurs it must be in support of a purpose that is ‘legitimate’ under the Representation of the People (Amendment) Regulations 2002, such as credit referencing or the prevention of money laundering. If testing is in support of a marketing-related purpose, it must use only data obtained from the ‘edited’ register list. Even then, the data controller must give careful consideration to whether that testing is likely to be ‘obvious’ or ‘non-obvious’ to the data subject.

**Alternative test groups**

One possible way around the issues of awareness, consent and fairness in testing is to consider using the data of a finite group of customers, with their consent. While this may be practical where testing is occasional or for a special one-off set of tests, it may not be a suitable approach for ongoing, regular testing. Note that if these individuals are to be asked to consent they must still be provided with sufficient information to enable their consent to be fully informed and freely given. They must also be able to withdraw their consent at any time.

Another alternative is to use data relating to members of the organization’s own staff, with their fully informed consent. Staff must not be pressurized, either explicitly or implicitly, into giving consent. The idea of consent in the employer–worker relationship is a difficult one with duress considered by many to be unavoidable. Any organization planning to use data relating to its workers should therefore take extra care to ensure fairness at every step in the process.

Workers, and carefully selected groups of consenting customers, are data subjects like any other and retain the same rights and protections under the DPA. Any processing using their data must still adhere to all the principles and provisions of the DPA.

**Other privacy-related obligations**

In addition to the DPA, there may be other guidelines or codes of practice specific to particular sectors or industries, such as the NHS Code of Practice on Confidentiality. It is important that any use of personal data in system testing takes account of all appropriate rules and guidance to ensure fairness and lawfulness in the context in which it takes place.