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

Second edition

Louise Wiseman
Jenny Gordon

First published in the UK in 2009
by
BSI
389 Chiswick High Road
London W4 4AL

Typeset in Frutiger by Monolith – http://www.monolith.uk.com
Printed in Great Britain by Berforts Group. www.berforts.com

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978 0 580 66437 3

Contents

Contents

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[1]

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[2] 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'.[3] 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.*

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[4]

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.

---

[4] 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.

- 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[5]

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.

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

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.

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.

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,[7] 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.

---

[8] Data Protection Act 1998, Schedule 1, Part 1.

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.

Principle 2 – Processing for specified purposes

> *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.*[9]

Notification

Where system testing is deemed a purpose in itself, it must be included in the organization's notification to the ICO, but in the more usual situation where it is just one aspect of an organization's processing, the ICO generally takes the view that it is a subsidiary purpose and therefore need not be included in the notification or brought to the attention of the data subject. Indeed, to include one sub-function of processing in a notification may raise the question of why all other sub-functions have been omitted.

Even where system testing is not an organization's main purpose for processing personal data, if it is carried out regularly or on a large scale, the organization may choose to include it in notification as a matter of good practice. If it is notified to the ICO, consistency and fairness require that it must also be notified to customers which means it should then be included in the organization's privacy notice.

The notification process requires the data controller to make a brief security statement, indicating whether suitable measures have been taken to ensure the security of personal data. Compliance with Principle 7 in system testing, and the ability to provide evidence of that compliance, becomes ever more important where the testing has been included in the ICO notification. The company may be asked to produce documented evidence of compliance with its stated security measures. Any organization unable to do so instantly appears, whether correctly or incorrectly, to be in breach of Principle 7 and is also processing data contrary to its notification.

Lawfulness

Regard must also be had to the lawfulness of processing, not only of the specified purposes of processing but of the methods employed in sub-functions such as testing. In general, as long as the overall purpose is lawful so will be the subsidiary elements; however, the testing itself must still comply with all applicable legislation, regulation and codes of practice.

Data sharing

Data controllers must remember that their obligations in respect of fairness and purposes do not necessarily end when data is passed to an external body. The data controller remains responsible for any processing carried out on its behalf by a data processor and must therefore ensure that the data will only be processed in ways compatible with its own stated purposes. This should be stipulated

---

[9] Data Protection Act 1998, Schedule 1, Part 1.

in the contractual agreements governing the relationship between the data controller and data processor, and reinforced by appropriate auditing or checking throughout the business relationship.

Where the data is passed to a third party that will act as a data controller, it is still important to ensure that the first data controller's stated purposes allow it to pass data across to that party for the purposes it will undertake. If the data is to be passed over to an organization that will use it for system testing, the original data controller must notify the ICO and its customers accordingly, as this will not normally have been obvious to them when initially giving their personal data.

Principle 3 – Adequate, relevant and not excessive

> *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*[10]

As well as supporting compliance with Principle 3 by helping to ensure that the data processed in systems is adequate, relevant and not excessive, testing must in itself abide by Principle 3. This means that the data used in testing must itself be adequate, relevant and not excessive. Even where it is not a specified purpose of the processing, it is useful to treat testing in progress as a purpose in itself, against which the Principle 3 criteria can then be assessed.

All data used in testing must be strictly relevant to the purpose of testing. In deciding relevance in any context it is a good discipline to encourage the identification and justification of every individual data item to be held or used in a system; this is especially useful when carried out with test data. Although data classification can be a lengthy exercise, it yields interesting and useful results. Individual data items should be listed and identified as non-personal, personal or sensitive personal. Once the data has been classified, reasons for inclusion in the testing should be provided. Where a reason for inclusion cannot be found, the data must not be used for that function. Example classification and justification tables are included in Appendix 4 and Appendix 5 respectively and blank copies are provided in Appendix 7.

This is a measure stipulated in BS 10012, which requires an organization, as part of its overall Personal Information Management System (PIMS), to maintain an inventory of the categories of personal information it processes and the purposes for which it uses them, as well as documenting where that personal information flows through its processes.

Where sensitive personal data is used in system testing, even greater care than usual must be taken to ensure its security and consideration given to the possible need for legitimization under Schedule 3 of the DPA. The same may be true of any data classified as confidential, where a duty or expectation of confidence operates, although Schedule 3 criteria will not be relevant.

Matching and cleansing data

Principle 3 criteria are particularly important where the testing is of a system or process that performs matching or cleansing of data. Adequacy of data is important, that is it must be sufficient to avoid the risk of incorrect matching or cleansing, particularly where there is any likelihood at all that the test data may become combined with live data or where the testing is carried out in a live environment.

No additional data should be used in testing apart from that which is strictly relevant. Where extra data is needed to replicate the volumes of a live environment, dummy data should be used and should be clearly identified as such with steps taken to ensure it cannot become merged with live data.

---

[10] Data Protection Act 1998, Schedule 1, Part 1.

National identifiers

Care must be exercised in the use of general identifiers, such as National Insurance or Pupil Identification numbers. The DPA allows the Secretary of State to place restrictions on processing by means of such identifiers. Their processing is prohibited except where it is permitted by order of the Secretary of State. For example, only the Inland Revenue and the Benefits Agency are permitted to use National Insurance numbers. Permitted bodies may clearly need to include identifiers in testing, but this should occur only where it is absolutely essential, is in support of a lawful and specified purpose and is secured by all possible safeguards.

Principle 4 – Accuracy

Personal data shall be accurate and, where necessary, kept up to date.[11]

As with Principle 3, testing can be seen as supporting overall compliance with Principle 4 by helping to ensure systems process data that are accurate and up to date. This is particularly important in testing any system that matches, cleanses or in any way changes data.

On the other hand, it is essential that any system testing regime maintains an audit trail which highlights errors that occur during the testing process and allows them to be corrected promptly and fully. Checks should be carried out on the accuracy of the data being fed into a test system; and this is particularly important where there is any possibility of that data being merged with other data or fed back into source systems.

[11] Data Protection Act 1998, Schedule 1, Part 1.

Principle 5 – Retention and disposal

> *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*[12]

The key to this principle is whether testing is deemed to be a specified purpose or simply a supporting function of a specified purpose of processing. Where it is a specified purpose, it will be essential to have mechanisms in place to ensure that test data is retained for no longer than is necessary for that purpose and to fulfil any legal, regulatory or business requirements. Test data must be included in data retention policies, with clear guidance on timescales, classification, storage and retrieval methods and secure destruction. Personal data which has been scrambled or anonymized and is no longer personally identifiable may, of course, be deleted immediately after testing because it is longer 'personal data'. Personal data that is encrypted is still personal data and must continue to be handled in accordance with the DPA.

Where test data is retained after testing is complete and still constitutes personal data, it may need to be provided as part of the response to a subject access request and this needs to be considered when drawing up retention plans.

The following factors should also be considered when deciding suitable retention periods for test data.

- Method of storage, in terms of security, audit trail and accessibility.
- Archiving capabilities and facilities.
- Method and ease of retrieval.
- Deletion criteria and method.
- If it is possible that the data will need to be provided in response to a subject access request, it must be possible to do so in an intelligible format. This means it must be possible to reproduce it on paper, change code into language, explain terms and perhaps provide some form of data dictionary to aid interpretation.
- There may be circumstances where there is a legal or regulatory obligation to provide data to a third party, for example in response to a court order or police warrant, and specific requirements as to medium and timescale.

Retention arrangements may differ for various kinds of personal data depending on the way in which they have been classified: personal, sensitive personal, confidential, etc. and the level of security and access to be applied to each. The issue of retention can therefore usefully be addressed during the data justification exercise described earlier and carried out before the system testing takes place.

---

[12] Data Protection Act 1998, Schedule 1, Part 1.

Principle 6 – Rights of individuals

> *Personal data shall be processed in accordance with the rights of data subjects under this Act.*[13]

The DPA gives data subjects a number of rights including those listed below:

- To have access to a copy of the data.
- To request that their data is blocked from certain kinds of processing.
- To seek compensation where processing has caused or is likely to cause damage or distress.
- To receive an explanation, and a manual review, of any fully automated processing.

A request for subject access may require the organization to provide test data if it has been retained in the format of personal data and where this is the case, it must be possible to provide it in intelligible format within 40 calendar days of receipt of the request.

In some circumstances an individual may be able to exercise the right to stop personal data being used for testing purposes. The DPA's section 14 provisions can be invoked where there is inaccuracy and/or actual or likely substantial damage and distress. Although both damage and distress are usually interpreted in a very narrow sense by the courts, it is conceivable that an error in system testing could lead to both. Prevention is, of course, better than cure and any test system or testing regime must have the facility to correct errors promptly. Although not a legal requirement under the DPA, good practice requires that data controllers respect the wishes of any individual who objects to the use of their data in systems testing. It is, of course, unlikely that any objections will be received unless the data subject has been made aware of the testing and this is unlikely where it is not a specified purpose.

Similarly, the data subject's rights in relation to automated decision taking should not apply in a secure system testing regime. These rights apply only where a decision significantly affects the data subject: careful, secure and correct testing should have no direct effect on the individual whose data is being used.

Where there is any likelihood of test data entering live systems, there is the possibility of loss, damage or corruption which may lead to claims of substantial damage and distress under section 10 of the DPA. This section allows the individual to require the data controller to cease processing personal data where that processing is causing, or is likely to cause, substantial damage or distress. If there is any likelihood of this or any other aspect of testing giving rise to section 10 claims, this should be identified before testing commences and an alternative method of testing found which does not involve using live data. Potential issues of this kind will be highlighted in a thorough risk assessment of the kind illustrated at Appendix 2.

---

[13] Data Protection Act 1998, Schedule 1, Part 1.

Principle 7 – Security

> *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.*[14]

Principle 7 is pivotal to compliance with the DPA and issues relating to security underpin all the other seven principles. The organization should already have in place a robust security infrastructure that is constantly monitored for compliance with security policy,

The DPA makes the distinction between technical and organizational security measures although the two often overlap and interlink.

Organizational measures

This covers everything the organization can do to render testing safe. User accountability is vital: maintenance of secure audit trails, surveillance and tracking methods as appropriate. Hand in hand with this goes staff training: all staff should be made aware of their responsibilities as defined by the organization, which must of course include the relevant data protection measures. This is particularly important for IT professionals who, particularly in larger organizations, are all too often allowed to operate independently of the rest of the organization. It is not uncommon to find data held on databases, spreadsheets and other user-developed applications throughout an IT department. Several different software developers within the same organization may each have developed their own version of a set of data originally extracted from the organization's live database. Training, refreshed regularly, will help ensure they are aware of the implications of using, storing and manipulating personal data in this way outside of the organization's main systems.

Most importantly of all, organizations should work towards embedding data protection in their day-to-day business practice, creating a culture of compliance and making it the cornerstone of their governance processes.

Any activity carried out with personal data will then take place against a well-established background of DPA compliance.

Governance

Creating this culture of compliance is ever more vital as business practice changes. It is important for organizations to recognize that data protection is fundamental to the success of any business that processes personal data. A single major breach of the DPA may be all that is needed to bring an organization into disrepute and financial difficulty. Achieving the goal of compliance culture requires that the organization embeds data protection within its management structure in a way that guarantees ownership and accountability at a high level.

---

[14] Data Protection Act 1998, Schedule 1, Part 1.

BS 10012:2009 provides sound and comprehensive guidance that will assist any organization, large or small, in achieving this. It requires organizations to implement a PIMS that supports compliance with the DPA and takes account of the organization's needs, obligations and risk appetite.

Accountability and ownership

Effective governance depends on accountability at a suitably high level within the organization. BS 10012:2009 specifies that a member of the senior management team should be accountable for the management of personal information within the organization. Depending on the size of the organization, this individual may also be accountable for system testing. It may be more appropriate to have another senior individual with specific accountability for testing. That person must have the knowledge and awareness required to carry out the role, the seniority to work with the person responsible for the overall management of personal information and, above all, visibility at board level.

It also specifies that an organization should have a network of data protection representatives representing departments or systems defined as high risk because of the type of data they process or the activities they carry out. The role of the representative or 'champion' will be to assist the person with overall responsibility for the personal information in the organization in achieving and maintaining compliance. System testing with live data must be considered a high-risk activity and therefore one which requires a dedicated representative.

This has already been implemented in central government departments, which are now required by the Cabinet Office to have in place a Senior Information Risk Officer.

Policy

In embedding data protection within its governance framework, an organization should develop a high-level data protection policy setting out its overall approach to processing personal data. This should be supplemented by individual policies and procedures for specific and high-risk activities such as system testing. Clear, accessible documentation allows workers to understand the organization's expectations and requirements as well as providing evidence both internally to staff and externally to auditors, regulators, customers and the public that it is committed to the safe and effective management of data.

A system testing policy should be documented, with input from all key business areas and should clearly detail roles, responsibilities and requirements in respect of system testing. BS 10012:2009 specifies policy content. The policy itself must be approved at an appropriate level and made available to all those within the organization involved in system testing. The policy should include or be supplemented by a clear, straightforward and comprehensive approval process to be followed whenever testing is required. Approvals granted should be clearly logged and details retained centrally to provide a detailed audit trail. An example of a testing policy, which can easily be adapted to suit any organization, is included in Appendix 6. Blank templates of a testing approval form, system testing log and issue tracker are included in Appendix 7.

Embedding data protection within the IT structure

Testing should be an integral part of any organization's project life cycle or software development life cycle. It should appear as a routine requirement in all project plans from the outset to ensure that it is appropriately resourced in terms of time, cost and people and that it receives approvals from all stakeholders. It is vital that data protection considerations raised by system testing are integrated into the project life cycle so that they become a routine part of the whole project process.

As a vital part of any IT-related project, testing should be carefully planned and timed in such a way as to allow for initial testing, bug fixing and re-testing. All of this takes time and, especially where tester resource is limited, it should be scheduled well in advance to avoid conflicting priorities. A lack of adequate time for system testing may lead to cutting corners, which in turn could result in a serious data protection breach.

User Developed Applications (UDAs)

It is important to know what data is held and processed in different business areas. Good practice dictates that personal data should be processed only on an organization's official live or test systems whose purpose, use and security are known and monitored. There may be cases, however, where data is processed in tailored database systems or spreadsheets. System testing should always take place in properly maintained environments and while it will not normally be appropriate for it to take place on a UDA, this practice is not unknown, particularly within larger organizations. It is wise to develop a policy specifically covering the use of UDAs and clearly outlining what is and is not acceptable and against which the organization's activities can be monitored for compliance.

Adequacy and audit

Under BS 10012:2009, the issues above will be picked up naturally as part of an organization's PIMS, which will assist in embedding a culture of data protection and privacy compliance within an organization's overall structure. To be effective, the PIMS must be checked regularly against the DPA to assess whether it continues to provide an adequate infrastructure for compliance. It is also essential to audit the organization's processing activities for compliance with the PIMS and therefore with the DPA. Depending on the organization's size and resources, this audit may be undertaken as one large exercise in itself, perhaps annually, or broken down into a series of smaller audits. System testing may be one discrete area that lends itself well to a smaller and specific audit that will then feed into the organization's ongoing programme of auditing PIMS compliance.

To be effective, audit findings must be reported, escalated and acted upon. The audit report must be seen by senior management. This is an important element of their oversight of the PIMS within the organization.

Privacy Impact Assessments (PIAs)

Depending on the nature of the testing, or indeed overall processing, carried out by a data controller, it may be useful to conduct a Privacy Impact Assessment (PIA). This is a management tool which enables organizations to look at in detail, and address the likely impact of, new projects or specific activities and to build up a good picture of the real level of risk involved which can then be effectively managed. The output from a PIA is usually a documented report which should be shared with senior management and business stakeholders. If system testing involves a large volume of personal data or any new or potentially intrusive technologies, a PIA will certainly be appropriate. A very detailed PIA handbook giving guidance on this matter is available on the ICO[15] website. PIAs are commonplace in Canada, the USA and Australia, particularly in the public sector and in some jurisdictions are legally required. Within the UK they are not a legal requirement but may be a useful tool in the management of data protection and wider privacy risk and are now a mandatory process for central government departments embarking on any processing of personal data.

Physical protection of the system

This aspect of security fits under both the technical and organizational headings. Test data should be physically protected from unauthorized access. This ties in with the use of access controls, audit trails and surveillance measures. Data should not be viewable by, or accessible to, any individuals other than those who require access to carry out the testing. Access levels should be authorized according to the individual's need for the data according to role, function, individual task or department and it should be possible to trace an action back to one identifiable user or small, finite group of users.

The physical location of the test system is important. It should be placed where passers-by cannot see the data or access the system. It is also important to identify whether it is possible for any member of staff to take test data off the premises. Printing and copying facilities should be restricted and controlled especially where the testing is carried out off-site or by a data processor.

Databases holding test data should not be held on shared drives and should be password-protected and access-controlled as appropriate.

Segregation

Wherever possible, segregation should be employed as a safety measure. This covers the segregation of powers which at a very simple level would mean that those who authorize a task should not also undertake or check it. It also includes segregation of duties, whereby those who carry out the task should not also check it and segregation of location – simply, different functions should not be carried out in the same place at the same time.

[15] http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/pia_final.pdf

Technical measures: Test environments

Where data cannot be scrambled or anonymized, it should be tested on a totally separate, secure and isolated test system wherever possible. This system must be prevented from feeding data back into the live systems. Encryption should be used where appropriate, as should measures such as firewalls and walled gardens. Filters should be applied to prevent the use of data that is not relevant, such as that which has been designated 'sensitive personal data'. Free text fields on source systems can allow the inclusion of sensitive personal or confidential data and it is advisable to filter these fields out where they are not specifically being tested.

There must be procedures in place for bug fixing and to enable any errors to be corrected in the test system without any impact on live data. It must be possible to identify any 'leaks' in the test environment so they can be closed off and to this end a leak reporting process should be documented.

Back-up facilities may be necessary where data from two or more systems is being compared or where testing takes place continuously on the test system.

Choosing a test environment

There are different solutions available for system testing, depending on the size of the organization concerned, the resources available to it and the regularity with which it undertakes testing activities. An organization may design and build its own test environment suited to its particular needs or it may use the hardware and/or software from an external supplier. If designing a testing program or system in-house, the organization should build in data protection compliance from the outset. This should be backed up by audit capabilities to enable compliance to be monitored. Such a program or system should be developed after consultation with specialist data protection professionals, whether in-house or external.

If purchasing a product 'off the shelf', or using a testing environment that is part of a suite of products already in use by the data controller, that environment should be subject to the same scrutiny and monitoring as a tailor-made solution. It should not be assumed to be DPA compliant simply because it is provided by a reputable vendor. The data controller – not the vendor – is responsible for compliant processing, and this includes ensuring that it takes place on secure, compliant systems. Any test system should be fully assessed for security and data protection compliance and any gaps addressed with the vendor. The importance of this is illustrated by the following example, based on a true situation, which also emphasizes the need for system testers themselves to be made aware of how the DPA applies to their role.

> *An organization used the testing environment that formed part of a suite of products from vendor A. The system took a regular feed of customer data from its live sister system and 'anonymized' it for use in testing processes. It was only after some years of operating the system that the anonymization process was found to be very simple indeed: the system simply took each letter of the customer's name and replaced it with the next letter of the alphabet. Hence Smith became Tnjui, Jones became Kpoft, and so on. This 'encryption method' was not sufficiently robust to satisfy the requirements of Principle 7 as it was clearly not strong enough in relation to the type of data, the potential harm, the risk involved and the 'state of the art' encryption technology*

freely available. The data controller had no alternative but to negotiate with vendor A and bear the substantial cost required for it to introduce alternative and more robust encryption methods at such a late stage in their relationship.

Testing by data processors

Where a data processor undertakes testing, contracts must ensure that they process data only as per the instructions of the data controller. They should be contractually prohibited from making independent use of the data and have documented arrangements to destroy, delete or otherwise dispose of the test data at the end of the testing or of the contract. Contracts should also cover reporting obligations in the event of a problem or of a data protection breach and audit or inspection rights on the part of the data controller. The data controller must also ensure its own privacy notices and notification with ICO cover the processing to ensure compliance with Principle 1 and Principle 2.

Full due diligence should be carried out on any such organization, and this must include data protection issues. Although largely an information security exercise, the due diligence process must have input from the person responsible for data protection within an organization. The exercise must look at not only the technical but also the organizational security measures in place in order to allow confidence in Principle 7 compliance. It may not be sufficient to simply look at the third party's testing department or test environment. Taking account of the bigger picture – the culture within the organization, the level of staff awareness, general security around its premises, etc. – will give a more realistic and reliable picture of the true level of security and care likely to be applied to processing personal data.

A full due diligence exercise may not always be possible but as a minimum, the following good-practice recommendations should be applied when choosing a data processor to carry out system testing.

- Select a reputable organization offering guarantees about its ability to ensure data security.
- Make sure the contract with the organization is adequate and enforceable.
- Ensure the security of data in transit to and from the data processor.
- Check that the processor has appropriate security measures in place.
- Make sure it carries out appropriate checks on its staff and their activities.
- Carry out regular audit of its processing against the data controller's requirements and standards.
- Require it to report any security breaches or problems to the data controller.
- Ensure procedures are in place to enable fast action in the event of such a report.

Note that if the testing is carried out outside the European Economic Area (EEA),[16] Principle 8 will also apply.

---

[16] At the time of publication, the European Economic Area (EEA) comprises the EU member states plus Iceland, Liechtenstein and Norway. The following countries have been approved as 'adequate' by the European Commissioner and therefore acceptable for the transfer of personal data: Argentina, Canada, Switzerland, Guernsey, Jersey, the Isle of Man and companies in the US that are members of the 'Safe Harbour' scheme. For an up-to-date list of countries, refer to http://Europa.eu.int

BS 27001

BS 27001[17] is the security standard adopted by the BSI and the International Organization for Standardization (ISO). Although not compulsory for data protection compliance, compliance with this standard provides a solid framework for compliance with Principle 7 of the DPA.

BS 27001 relates not just to personal data, but to all data and is therefore applied across the board in any organization that adopts it. Adherence to BS 27001 will enable an organization to build a robust security management infrastructure, identify key security objectives, identify the highest-risk areas of processing and to assess its processing against best practice. There are a number of areas covered in BS 27001 that may be of particular use to organizations looking to carry out system testing, such as data security, data storage protection, data processing, computer networks, computer hardware and software, access, data transmission and information exchange.

Reading the relevant sections of BS 27001 in conjunction with a PIA and/or full risk analysis will provide a good foundation for any data protection-compliant testing strategy.

Remote working

More and more companies now encourage their workers to work from home some or all of the time. This raises risks from a data protection point of view if personal data is to be taken or transferred off the premises and underlines the need for an embedded data protection culture across the organization.

Workers in remote locations must be aware of the implications of taking personal data off the premises and be given clear guidelines about what they are and are not allowed to do it with this data in addition to requirements about its transport, storage and disposal.

There are some situations in which remote testing has to be carried out, for example where testing internet or extranet applications, and this must be allowed only after a full assessment of the additional risks that result from transferring test data to and from an external location. It should rightly be regarded as a very high-risk activity and assessed, managed and monitored accordingly, although an organizational culture of DPA compliance and security, preferably embedded within a PIMS, will lay firm foundations for it to be carried out safely.

The use of dummy or test accounts

The use of dummy or test accounts is preferable to using real accounts, particularly in financial environments. Dummy accounts usually exist for ongoing test purposes to support the live environment, whilst test accounts exist for a short period of time only to support a specific testing project after which the accounts are closed and reconciled.

---

[17] ISO/IEC 27001: 2005, Information technology – Security techniques – Information security management systems – Requirements.

Where either of these options is used, there should be tight controls on the creation, activity and closure of such accounts and the number of these accounts that exist at any time. The organization should have and implement a dummy account policy and process. Such accounts should of course be fictitious and clearly distinguishable from live accounts. Wherever possible they should use one central address or e-mail address to avoid the possibility of any correspondence to customers being triggered accidentally. If this is not possible for any reason, it is wise to put in place a manual check that will physically prevent it.

Limiting the data

Wherever possible, a limited and finite list of data items should be used in testing. A comprehensive record should be maintained to show which data items have been used and why. Staff should also be trained to avoid the use of offensive or contentious language in test cases. The strategy should always be to limit the potential damage caused in the event of test data becoming mixed or merged with live data.

Business continuity

System testing should be included in continuity of business or disaster recovery plans for two reasons. First, following a major incident, testing of existing systems or data may be required prior to commencing usage once more. Second, depending on the IT structure of the organization concerned, test systems and data may need to be periodically recovered and reloaded.

Principle 8 – International transfer

> *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.*[18]

This principle will come into play where the testing is to be carried out in a country outside the European Economic Area (EEA).[19] Data which has been subject to a request from the data subject to be blocked from processing outside the EEA must not be involved in any testing outside the EEA. Safeguards should also be in place to ensure that data on test systems is not inadvertently sent abroad in the course of testing or as a result of testing.

However, where the object is to test the functionality to block data from being sent outside the EEA, the system must test this capability adequately and this may of course involve data being sent outside the EEA, either deliberately or inadvertently. This will require careful consideration of the issues discussed in Principle 1 and Principle 2 regarding fairness and consent.

Outsourcing: Maintaining control

Companies now routinely outsource work to companies both within and outside the EEA. Geographical remoteness must never be allowed to compromise the degree of oversight and monitoring applied over the outsource organization. There may be industry-specific rules or guidelines about the oversight of outsourced activities such as those of the Financial Services Authority. Where such rules exist, they will provide the required framework for compliance. In the absence of any specific rules or guidelines a due diligence exercise should be carried out, including all data protection elements, before entering into any outsource agreement, and appropriate mitigating measures put in place.

Clearly drafted, legally enforceable contracts are vital to any outsourcing agreement. In the event of a breach or a dispute, a written contract is often the only real way in which a data controller can prove it took steps to ensure the processor's DPA compliance. However, contracts cannot be considered simply as a way of an organization 'covering its back' in case of a breach but rather as a means of initiating and enforcing good practice and compliance. Contracts themselves should be reviewed regularly to ensure they still cover the processing activities in question and take account of any changes. Adherence to contracts should be monitored and audited regularly. In the event of a problem, a contract may resolve legal liabilities and may give rise to financial redress, but it cannot repair customer confidence once a breach has occurred. The emphasis in outsourcing, as in all activities involving personal data, should be on prevention rather than cure.

---

[18] Data Protection Act 1998, Schedule 1, Part 1.

[19] At the time of publication, the European Economic Area (EEA) comprises the EU member states plus Iceland, Liechtenstein and Norway. The following countries have been approved as 'adequate' by the European Commissioner and therefore acceptable for the transfer of personal data: Argentina, Canada, Switzerland, Guernsey, Jersey, the Isle of Man and companies in the US that are members of the 'Safe Harbour' scheme. For an up-to-date list of countries, refer to http://Europa.eu.int

Offshoring: Ensuring compliance

More companies than ever choose to send work outside the EEA. This is an area that is constantly developing as more countries become eager to secure business from partners within the EEA and therefore work to achieve a suitable standard of data protection.

A set of approved standard contracts has been developed and approved by the European Commission and the UK Information Commissioner for use by companies entering into arrangements with so-called 'third countries' outside the EEA. Use of these contracts allows overseas transfer of personal data under the DPA, making that particular transfer acceptable, or 'adequate' under the DPA even where it is to a country that has a much lower standard of data protection than that of the EEA countries. Although the contracts are standard templates, it is permissible to add to them to ensure all relevant activities are covered. The contracts have two versions depending on whether data is being transferred between a data controller and a data processor (known as a 'C2P') or between two data controllers (a 'C2C') and both can be downloaded from the ICO website or the European Union website.[20]

An alternative approach suitable for large multinational companies wishing to transfer personal data within their own 'group' companies is to use Binding Corporate Rules (BCRs). The organization draws up a set of BCRs to which it agrees to adhere when transferring data to its group members outside the EEA. It then obtains approval for these rules from data protection authorities in one or more European countries thereby achieving 'adequacy' for the data transfer. Again, it must be said that although such contracts and rules will satisfy legal responsibilities and the 'adequacy' requirements of Principle 8 of the DPA, they must be monitored effectively and applied in such a way as to ensure compliance happens in practice.

Breaches of the DPA: What to do if things go wrong

In the event of a breach of data protection occurring during system testing, it is important to act quickly and calmly. The first priority must be to establish the facts – to find out exactly what has or has not happened and the likely effect on individuals. In terms of data protection, a breach that actually affects individuals is far more serious than one that does not.

Once the facts are established, the next step must be rectification. This means correcting the breach itself and limiting the impact it has on the individual. Depending on the scale of the breach, its nature, and the likelihood of adverse publicity, it may be appropriate for the organization to contact data subjects. The data subject may need to know of the circumstances of the breach if there are consequences that may affect them, or if they are likely to read about it in the press. In addition to being an exercise in good customer relations and an opportunity to pre-empt customer complaints, contacting the customer may be a practical necessity. For example, following a breach in a banking environment, the customer's online security access details, and possibly even their account number will need to be changed.

[20] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF

An investigation should then be launched to find out exactly why the problem occurred. Depending of course on the size and structure of the organization it will usually be necessary to call upon the expertise of key internal contacts such as the Information Security department for assistance. It is advisable to have a data security breach-handling procedure prepared and documented for use in this situation. This should detail the departments or individuals to be involved, their responsibilities and the actions to be taken. As part of the testing governance process, any breaches or issues that occur during system testing should be logged in the system testing log (see Appendix 7) and tracked through to completion. An issue tracker form such as the example given in Appendix 6 will prove useful in doing this.

Having rectified the immediate breach and its consequences, the organization must then look to the long term to ensure that it does not recur. This could involve a reassessment of the organization's system testing procedures and in doing this it may be useful to revisit the PIA, risk assessment and data classification/justification exercises that were undertaken before testing began.

BS 10012:2009 advocates that the PIMS should incorporate procedures for assessing and managing security incidents involving personal data and for assessing whether to notify ICO or data subjects. Advance preparation will avoid undue delay in investigating and rectifying any incident and is therefore to be recommended. Staff should be trained to recognize a data protection breach and be confident in its handling and a formal, documented, breach-handling process available to all workers will prove valuable in the event of a breach happening, ensuring consistent and effective action.

Breach notification

There is no obligation for data controllers to notify the Information Commissioner of a breach of data protection. However, if it is likely that the breach will generate a significant volume of complaints and requests for assessment, it is advisable to notify ICO of the circumstances. Informing the ICO of a breach will not prevent it from taking enforcement action if necessary but ICO is keen to encourage openness from data controllers in such circumstances and may be able to offer advice that will help to limit the damage caused or lessen the risk of the breach recurring. A full investigation must take place before ICO is notified so that full details can be provided about what has happened and why, how it has been rectified and what measures have been put in place to mitigate the risk of recurrence.

The Information Commissioner believes serious breaches should always be brought to the attention of their office and although they do not define 'serious', they have published guidance to help data controllers make an assessment of the severity of a breach and the need to notify. The following factors should always be considered:

- Potential harm to the data subject.
- The extent of the harm, considering the volume and sensitivity of the data.
- The volume of personal data affected. ICO considers that where more than 1000 data subjects are affected and there is a real risk of harm, the breach should be reported.
- The sensitivity of the data affected.

What to report

If a breach is being reported, the Information Commissioner will need to know:

- the type of data and number of records affected;
- the circumstances of the breach;
- the actions taken to minimize or mitigate the effect on individuals;
- whether the individuals affected have been informed;
- how the breach is being investigated;
- whether any other regulatory body has been informed and its response;
- what remedial action has been taken to prevent recurrence;
- any other information that could be relevant.

Sanctions

The Information Commissioner's powers have until now been somewhat limited. In 2009, its powers to investigate public bodies were increased and this may eventually be extended to cover non-public sector organizations. The action taken by the ICO in response to a breach will depend on individual circumstances. It may simply record the breach and take no action, it may investigate and impose a requirement on the data controller to undertake a particular course of action. It may take formal enforcement action which will turn such a requirement into a legal obligation although it will not normally do this unless the data controller fails to take any recommended actions or there is reason to doubt future compliance. The Information Commissioner may recommend making a breach public if they feel there is a strong public interest argument for doing so. Where enforcement action is taken it is always publicized as a matter of policy. Until 2008, the ICO had no power to impose a fine or other penalty directly but could and did prosecute in appropriate cases. Although the fines that result from such prosecutions may not in themselves be too punitive, the resultant publicity, reputational damage and loss of consumer confidence can be immensely harmful to an organization and its future business activity. The Criminal Justice and Immigration Act 2008[21] gave the ICO powers to impose substantial fines on any data controller that knowingly or recklessly breaches the DPA. In addition to this, the Coroner's and Justice Bill[22] will give the ICO powers to carry out spot checks on government departments, local authorities and certain police and NHS bodies to ensure DPA compliance and there are calls for these powers to be extended to cover private sector and third sector bodies.

---

[21] http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

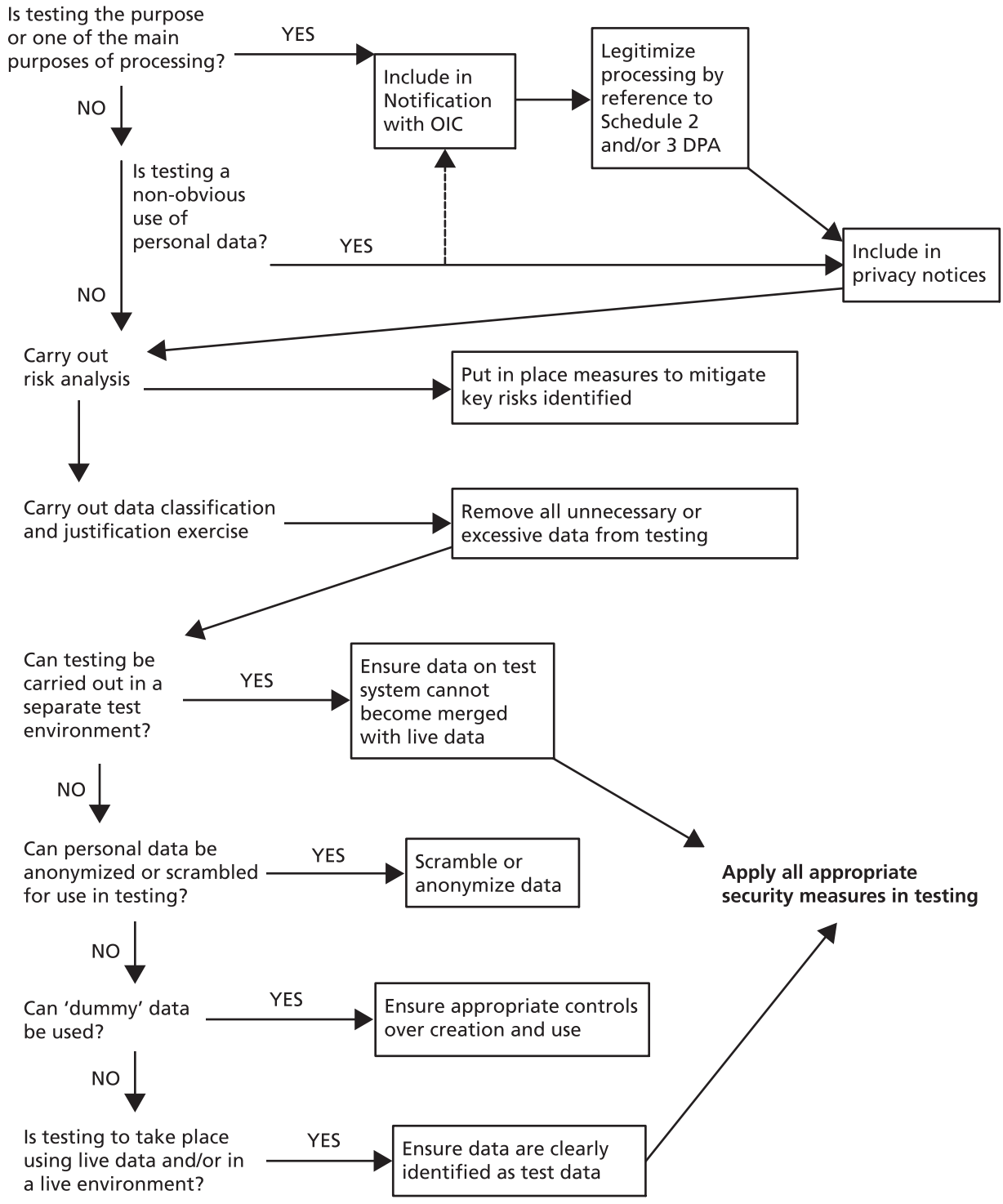
[22] http://www.justice.gov.uk/publications/coroners-justice-bill.htm – this was passing through Parliament at the time of publication.

Conclusion

The importance of system testing, including governance around the process, record keeping and audit trails, cannot be overemphasized in today's business environment. Yet in a climate of growing awareness and risk it is essential that it is carried out securely. Any organization embarking on a testing regime should begin by assessing the risks involved and deciding how to mitigate them effectively. It is also important to be clear as to how the activity of testing fits into the range of the organization's activities and whether notification is required. It is then possible to move onto a full consideration of the eight principles of the DPA and the impact of each on the system testing regime that is planned.

Essentially, testing should be viewed in the same way as any other form of processing – there are no special risks or conditions that apply over and above normal data processing concerns. In following the above guidelines, it is hoped that companies will be able to maximize the benefit they obtain from thorough testing while minimizing and mitigating the potential for harm. Incorporating testing and DPA considerations into the governance fabric of an organization will embed good practice and compliance into the overall structure in such a way that it becomes second nature.

Appendix 1 – Factors to consider in approaching a testing strategy



Appendix 2 – Risk analysis

Table 1 shows the way in which the key risks involved in testing and suitable handling strategies may be identified.

Table 1 – Risk analysis

Risk	Level of impact	Likelihood	Potential impact/Consequences	Accept/ Mitigate	Handling strategy
Intentional corruption of data	High	Medium	Major impact on customers leading to complaints, compensation claims, loss of consumer confidence and bad publicity.	Mitigate	Appropriate security measures to be in place, particularly access controls and audit trails.
Unintentional corruption of data	High	High	Major impact on customers leading to complaints, compensation claims, loss of consumer confidence and bad publicity.	Mitigate	Appropriate security measures to be in place. Monitoring and checking processes required.
Use of inadequate data	Medium	Medium	Data may be incorrectly identified, matched or merged due to use of insufficient data. Also, system capabilities may be insufficiently tested.	Mitigate	Need to ensure that sufficient data are used to fully test out the system and to prevent incorrect matching of data in the test system.
Compromise of source system data	High	Medium	Live customer data may become corrupted if accidentally merged with test data, leading to complaints, compensation claims, loss of consumer confidence and bad publicity.	Mitigate	Separate test environment to be used with appropriate security measures.
Hacking	High	Medium	Financial loss to customers, financial and reputational damage to organization as above.	Mitigate	Appropriate security measures to be used, particularly access controls, audit trails and monitoring.
Unauthorized access to data	High	Medium	Breach of DPA; potential for fraud both leading to financial and reputational damage.	Mitigate	Staff training and monitoring required. Access controls, audit trails and segregation of powers and duties to be maintained.

Risk	Level of impact	Likelihood	Potential impact/Consequences	Accept/ Mitigate	Handling strategy
Unauthorized disclosure of data	High	Medium	Complaints from customers, compensation claims; loss of confidence; breach of DPA.	Mitigate	Staff training and all appropriate security measures.
Objections from customers	Low	Low	Customers may wish to opt out of testing. Their data must be blocked from use in testing regime.	Mitigate	Customers who wish to opt out must be flagged on the system and their data filtered out before testing begins.
Substantial damage and distress claims from customers	High	Low	Would indicate underlying weakness in the security measures used in the testing regime. May result in compensation claims, possible court action, loss of consumer confidence and bad publicity.	Mitigate	Security measures must be robust. If there is found to be any likelihood of such claims arising, an alternative method of testing will be found avoiding the use of live data.
Reputational damage	High	Medium	Loss of consumer confidence and financial loss.	Mitigate	A 'compliance culture' should be maintained. A communications plan should be in place for customers, staff, regulators and the press.

Appendix 3 – Net and gross risk

Figure 1 shows an alternative way of representing the key risks involved in a testing strategy, using the same sample information as in Appendix 2.

The position of items shown in bold type and in boxes with solid lines shows gross risk (risk before any mitigating strategies are put in place) and the position of items in standard type and in boxes with dashed lines shows net risk (risk once mitigating strategies are in place).

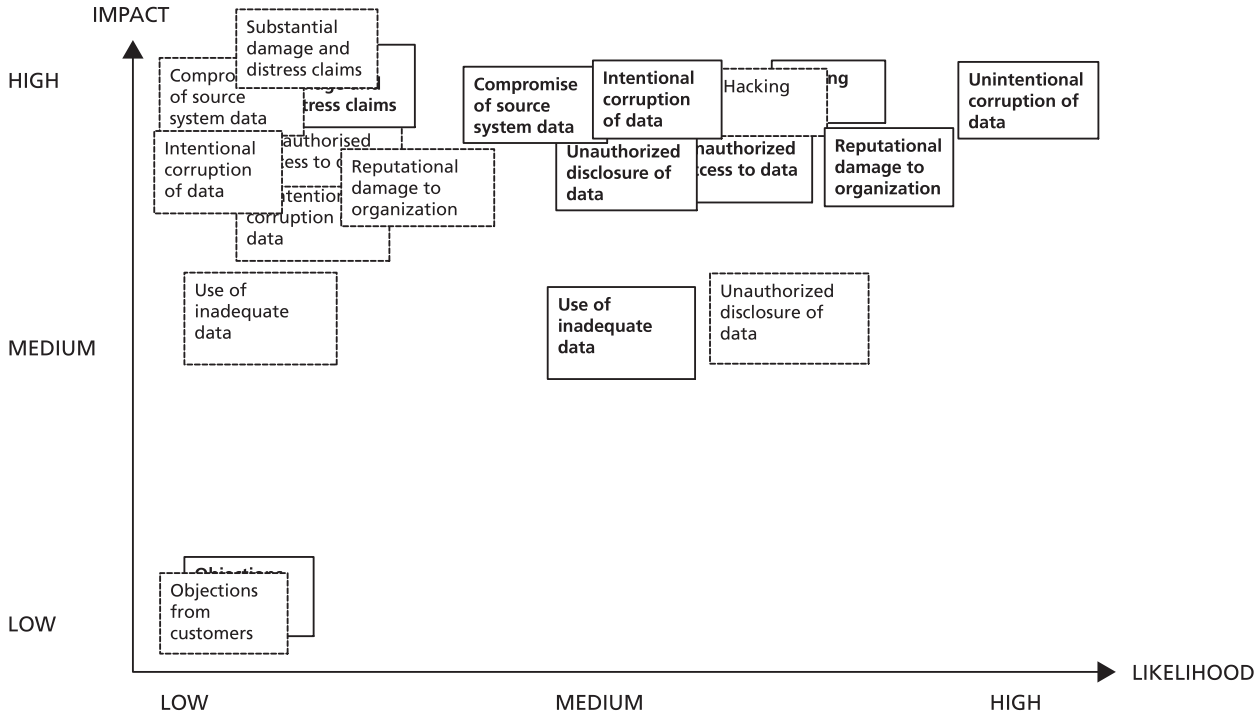


Figure 1 – Net and gross risk

Appendix 4 – Data classification table

DATA ITEM	CLASSIFICATION OF DATA ITEM*															
	Non-personal		Personal			Sensitive Personal										
	Non-personal	Personal factual, not identifying data subject	Directly identifies the individual	Identifies the individual only when taken with other data	Opinion	Intent	Racial or ethnic origin	Political affiliation or beliefs	Religious beliefs	Trade union membership	Physical or mental condition	Sexual life	Offences	Offence proceedings
Surname	✓			✓										
Date of birth	✓			✓										
National Insurance number			✓											
Preferred salutation		✓												
Income		✓		✓										
Number of driving convictions													✓	
Loan application date	✓			✓										
Final lending decision					✓	✓								

* Data could also usefully be categorized as ‘non-personal and confidential’ and/or ‘personal and confidential’.

Table 2 – Data classification

Table 2 shows sample data items that could be held on a banking system and the way they could be classified. Note that in deciding whether data are personal, much depends on context. Data that is on its own non-personal, such as application date, will be personal where it indicates an identifiable customer’s application, while data such as name will be non-personal if it does not indicate a particular individual with that name. Some items are given both classifications in the above table to illustrate this point, but these should be classified as appropriate in the context in which they occur.

Appendix 5 – Data justification table

Where data items are required for use in system testing, they should first be classified as shown in Appendix 4. Their use in testing should then be justified. Table 3 is an example of how this could be approached, using the data classified as personal and sensitive personal in Appendix 4. As in Appendix 4, note that in deciding whether data are personal or non-personal, much depends on context. Data that would alone be considered non-personal, such as loan application date, may be personal if they identify a customer. Data normally considered personal, such as name, will be non-personal if they do not indicate a particular individual with that name. The classification given in a particular context will therefore affect the justification and approval of that data.

Data Item	Classification*	Justification for use in testing	Approved for use in testing?**	Notes
Surname	Non-personal	To identify correct customer record	Yes	Aids compliance with Principle 3 DPA by ensuring adequate data used to identify correct customer record
Date of birth	Personal	To identify correct customer record	Yes	As above
Number of driving convictions	Sensitive Personal	To test the ability of the system to sort records by selected criteria	No	This functionality can be adequately tested using items of data that are not sensitive personal data
Final lending decision	Personal	To provide sufficient data to be matched with customer record	No	This functionality can be adequately tested using other data. Principle 3 DPA states that data must not be excessive
Loan application date	Non-personal	To test whether data in field maps over from one system to another	Yes	Required to enable functionality to be adequately tested

* As per data classification table in Appendix 4 above.

** Please note that this table relates to a fictitious, generic testing regime therefore the justifications, approval and notes are intended to be general. These factors will vary depending on the testing being carried out, the data used and the type of business.

Table 3 – Data justification

Appendix 6 – Example system testing policy[23]

In order to comply with the DPA and with internal policy, live personal data must not normally be used in system testing. In exceptional cases where there is no alternative, it may become necessary to use live personal data in this way. Live data may be used for system testing only in the following circumstances:

- Where all alternatives have been explored and there is a solid justification for using live data;
- Where a full risk assessment and data classification/justification have been completed and documented;
- Where there are adequate controls in place to mitigate any risks identified;
- Where an approval form has been completed in full and signed by *[the relevant data owner, the Information Security Officer and the Data Protection Officer]*

This policy and procedure apply in all instances where live data is to be used in system testing, including where the data is to be scrambled or anonymized.

It is the responsibility of *[The Project Manager]* to ensure adherence to this policy and the process detailed below. Failure to follow the approval process may constitute misconduct and could result in disciplinary action.

Approval process[24]

The process for requesting approval for the use of live data in system testing is as follows:

1. *[The Project Manager]* must ensure that a full risk assessment and data classification/justification exercise are carried out and documented.
2. An approval form must be completed in full and supporting documentation attached.
3. The completed approval form must be submitted for approval by *[the Data Owner, The Data Protection Officer and the Information Security Officer]*. It is not valid until such approvals have been provided.
4. Approval via e-mail is acceptable, subject to evidence being retained.
5. The form must be submitted for approval not less than *[five working days]* before any scheduled testing date
6. Once approval is obtained, *[the Information Security Officer]* will complete the system testing log and allocate a unique reference number.
7. If any security issues or data protection breaches occur during testing, *[the Project Manager]* must complete an issue tracker giving full details and stating the remedial actions being taken.
8. The issue tracker must be circulated to *[the data owner, the data protection officer and the Information Security Officer]*.

---

[23] Wording in italics should be customized to suit each individual organization.

[24] The approval process should reflect the roles and structure of an individual organization. In small firms, the specific roles mentioned in this example may not exist, or may be carried out by the same person.

9. The issue must be recorded in the system testing log, which must be updated once the issue is closed.
10. Approval forms and issue trackers must be retained by *[the Information Security Officer]* for *[2 years from the end of the testing or resolution of any issues]*.
11. The system testing log and supporting evidence will be regularly reviewed by *[the Compliance team]* to ensure adherence to this policy.

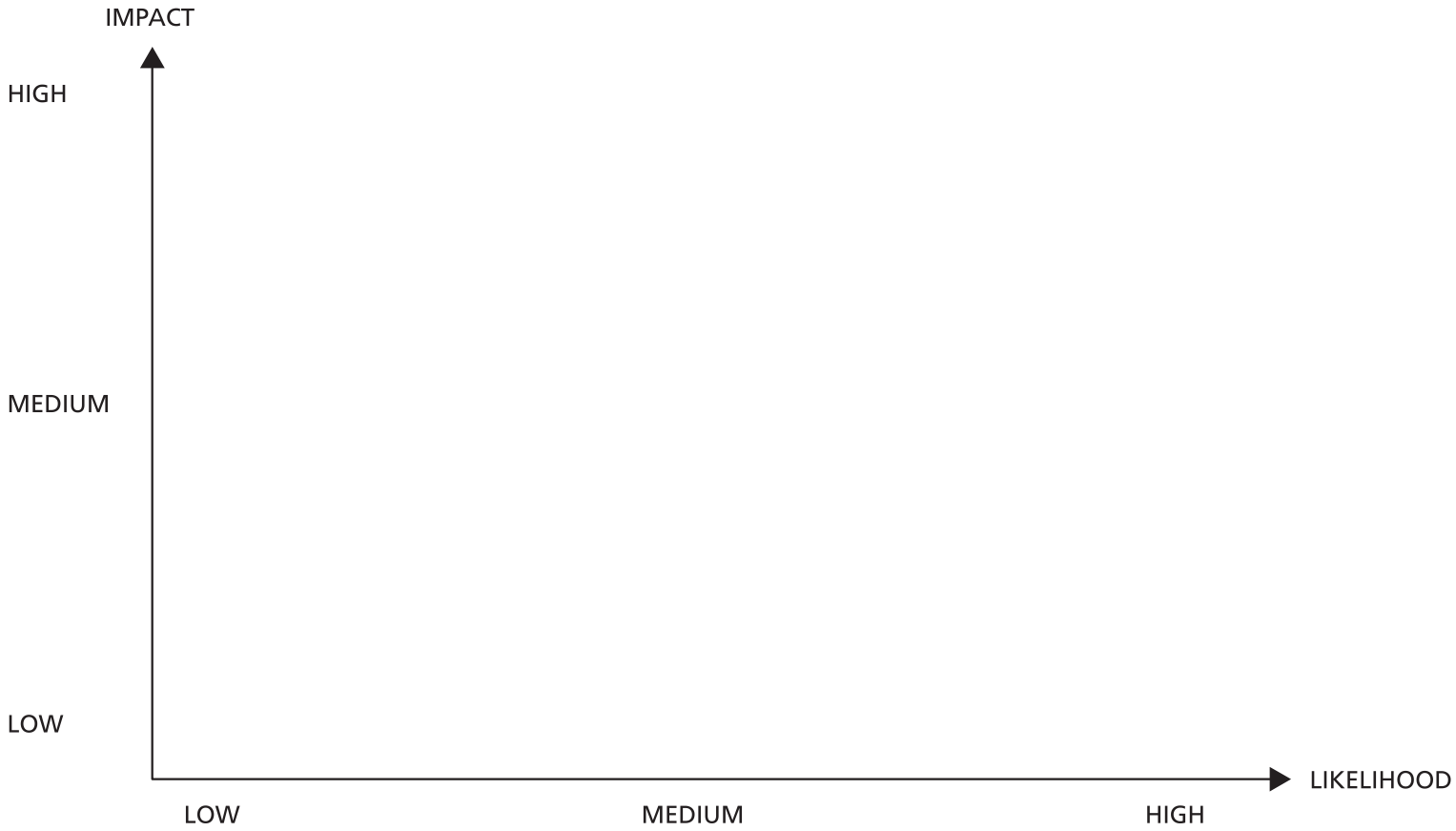
Appendix 7 – Blank form templates

Risk analysis table

Risk	**Level of Impact** (High, medium, low)	**Likelihood** (High, medium, low)	**Potential impact/ Consequences**	**Accept/Mitigate**	**Handling strategy**

Net and gross risk

[Gross = risk before any mitigating strategies are put in place. Net = risk once mitigating strategies are in place]



Data classification table

DATA ITEM	CLASSIFICATION OF DATA ITEM
Non-personal	Non-personal
Personal factual, not identifying data subject	Non-personal
Directly identifies the individual	Personal
Identifies the individual only when taken with other data	Personal
Opinion	Personal
Intent	Personal
Racial or ethnic origin	Sensitive Personal
Political affiliation or beliefs	Sensitive Personal
Religious beliefs	Sensitive Personal
Trade union membership	Sensitive Personal
Physical or mental condition	Sensitive Personal
Sexual life	Sensitive Personal
Offences	Sensitive Personal
Offence proceedings	Sensitive Personal

Data justification table

Data Item	Classification	Justification for use in testing	Approved for use in testing?	Notes

System testing log

Project	Approved date	Unique reference number	Date testing completed	Breaches or issues identified during testing?		Data owner signature
				Issue tracker number	Date resolved	

System testing approval form

1. Testing requirements
Requestor's name
Role
Project name
Project Manager name
Date of request
Date of planned testing
Have you read and understood the testing policy?
Why is this testing required?
Justification for using live data
2. Source data
Highest level of classification of source data
Describe in detail the data items that will be used. (Attach documentation if appropriate)
Volume of data to be used
Data owner
3. Systems
Source System Name
Source System Location
System Owner
Test system name
Test system location
System owner
Is target a production system or a test system?
Describe risk mitigation measures in target system
How will data be transferred to the target system?

4. Risk mitigation
Has a PIA and/or full risk assessment been carried out? (Attach report/sheet if applicable)
Has a data classification and justification been carried out? (Attach sheet if applicable)
Describe controls in place to prevent contamination of live data
Is data being scrambled?
If yes, describe the approach and tools used
If no, provide a justification
If not scrambled, how will the data be destroyed when testing is completed?
5. Risk Acceptance: Approvals
System Owner
Date of approval
Contact details
Data Owner
Date of approval
Contact details
Information Security Officer
Date of approval
Contact details
Data Protection Officer
Date of approval
Contact details
Unique reference number

Issue tracker form

1. The Testing
Name
Role
Project
Project Manager name
Date of testing
Unique Reference number
2. Issue identified
Details of the issue that has occurred
Date issue occurred
Data affected
Number of individuals affected
Cause
Potential risks
3. Corrective action
Details of corrective actions being taken
Action owner
Measures to be taken to prevent recurrence
Action owner
Data owner notified?
Data Protection Officer notified?
Security Officer notified?
Senior management notified?
Issue Tracker number
Date closed
Closed by

ISBN 978-0-580-66437-3