Protecting personal information

A consumer's guide to the British Standard BS 10012:2009 Data Protection – specification for a personal information management system

bsi.

...making excellence a habit.™

Every time you use a supermarket reward card, contact your bank, use NHS services or shop online, organizations collect and store information about you. This might be your address, date of birth, medical history, credit card number or even your shopping habits.

Used correctly, this information can make your life easier. But if it falls into the wrong hands you could become a victim of identity theft or fraud. Criminals could use your personal details to apply for credit cards, open bank accounts, claim benefits, and even get passports in your name. Identity theft is reckoned to cost UK consumers over £1 billion each year.

You can protect your data by keeping information in a safe place and being careful who you give details to. But how can you be sure that the organizations you deal with – from your local council and hospital, to banks, online stores and supermarkets – are using your information legally and keeping it safe?

The law

The Data Protection Act (DPA) 1998 is there to make sure that organizations collect only relevant and accurate information, store it safely and use it correctly. It also gives you the right to find out what information an organization holds about you.

However, although the DPA sets out principles, it doesn't specify how personal data should be managed. As a result, organizations can find their responsibilities confusing and difficult. British Standard BS 10012 helps to address this confusion. It is specifically written to help organizations meet the requirements of the DPA, giving step-by-step guidance about how to manage customer information.

BS 10012 – the basics

- The standard for data protection can be used by organizations of any size in any sector
- It provides a clear framework to help organizations create a tailored system for managing personal information
- It includes detailed guidance that covers training, risk assessment, disposal of data, and disclosure to third parties

BS 10012 – the details

The standard is voluntary but from an organization that chooses to use it you should expect:

A clear data protection policy

- A senior management team should be responsible for creating and maintaining a data protection policy that complies with the law
- The policy should follow the commitments set out in the standard

Use of personal information

Organizations should:

- Put in place procedures to ensure that personal information is used fairly and lawfully
- Collect information that is relevant, accurate, up to date, and not excessive
- Not keep data longer than necessary and dispose of it safely
- Ensure that personal information is protected against loss, damage or theft
- Make an inventory of the types of data they collect and how it's used
- Provide customers with a privacy notice or statement, clearly explaining how their personal details will be used
- Use personal information only for the purposes stated and pass the data to third parties only if customers agree (third parties can also use personal information only for the reasons specified)
- Restrict access to personal information to members of staff who need it
- Ensure that all staff who handle data know what to do if there is a breach of security
- On request, provide customers with copies of any personal data held about them

You can protect your data by keeping information in a safe place and being careful who you give details to.

Clear responsibility

- A senior manager should be accountable for the management of personal information
- At least one person should be responsible for ensuring the organization complies with the data protection policy on a day-to-day basis and that the organization's Personal Information Management System (PIMS) is kept up to date
- Adequate resources should be allocated to the PIMS

Education and training

- The details and importance of the data protection policy should be clearly communicated to all members of staff who handle data
- Relevant staff should be made aware of the PIMS and receive ongoing training

Regular checks

- Regular audits of the PIMS should be carried out and any problems resolved as quickly as possible
- There should also be regular management reviews to make sure that the system remains effective and up-to-date

Complaints

- The organization should create a complaints and appeals procedure for customers

Checklist

- Keep your personal information safe
- Think carefully before supplying information to any organization
- Does the organization you're dealing with use BS 10012? If you're not sure, ask
- When asked for personal information you should receive a clear statement of what the organization is collecting it for
- If you have concerns, ask for a copy of the personal information that the organization holds about you

Frequently asked questions

Q. What is BSI?

A. BSI is the UK National Standards Body which has been developing standards for more than 100 years to make products and services safer for consumers. Standards set out good practice and guidelines for organizations to follow.

Q. Do all organizations have to comply with the standard?

A. No, the standard is voluntary. Organizations that choose to sign up to BS 10012 should follow its requirements. In the event of a major data breach, the Information Commissioner's Office will look for evidence that data protection compliance is being taken seriously, and application of BS 10012 could be considered evidence of this.

Q. How do I know if an organization is signed up to the standard?

A. Organizations using the standard are likely to communicate this to the public in literature such as annual reports and social responsibility policies. You could check their website or contact them directly to make enquiries.

Q. Who do I complain to if I think that my personal information has not been handled legally?

A. Contact the Information Commissioner's Office for help. Complaints are usually dealt with informally but, if this isn't possible, enforcement action can be taken.

Q. Where can I get a copy of BS 10012?

A. Your local public library may be able to help you access a reference copy, or you can buy a copy from BSI at shop.bsigroup.com

Useful information

British Standards (BSI)

020 8996 9001

bsigroup.com

Action Fraud

(Fraud and identity theft reporting centre)

0300 123 2040 (to report Fraud and internet crime)

actionfraud.police.uk

CIFAS

(UK Fraud Prevention Service)

cifas.org.uk

Information Commissioner's Office (ICO)

(Fraud and identity theft reporting centre)

0303 123 1113 (helpline)

ico.gov.uk

BSI/UK/99/ST/1212/en/DD

BSI Group
389 Chiswick High Road
London W4 4AL
United Kingdom

T: +44 20 8996 9001
E: consumer@bsigroup.com
bsigroup.com