

Complying with the Data Protection Principles is required by law; it also makes commercial sense.

BUSINESS GUIDE

Business and Data Protection

www.business.wales.gov.uk/superfastbusinesswales | 03000 6 03000



Contents

	Page
Introduction	3
UNDERSTAND	
The eight Data Protection Principles	4
Data protection online	5
ADOPT	
Getting started	8
EXPLOIT	
What business benefits can I expect?	9
Top Tips	10
NEXT STEPS	11



“By showing that you are properly meeting legal requirements online, you reassure customers, employees and others that their personal data is safe with your business.”

..... Introduction

As digital technologies have burgeoned over the last twenty years, and Superfast Broadband has accelerated the adoption of cloud technologies, online data storage and Software as a Service, it has become more important than ever to be clear about what data you are handling, why it was collected, where it is stored, how it will be used, and when it should be deleted. It is therefore essential that companies are aware of the Data Protection Act and how to comply with it. This guide explains the key principles.

Data protection is about *personal data*, information relating to a living person: you individually, your employees, prospective and actual customers, individual business contacts, consumers, celebrities and ordinary people, who are *data subjects*. Expressions of opinion about someone may be personal data, as well as addresses, credit card numbers and dates of birth. Such information is very important in business, for marketing, sales, networking, record-keeping and analysis, and other purposes.

Organisations responsible for using and controlling personal data, including your business, are *data controllers*, with obligations at law. Conversely, note that other businesses which hold your personal data have obligations to you in your role as a *data subject*.

The eight Data Protection Principles

The eight Data Protection Principles set out in the legislation cover all aspects of obtaining, processing, using, storing and deleting personal data.

They include requirements for personal data to be processed fairly and lawfully, to be accurate, not to be kept longer than necessary, and to be kept securely, by means of appropriate technical and organisational measures.

Data protection is regulated throughout the European Economic Area, the EEA, which is the European Union together with Iceland, Liechtenstein and Norway. Many other countries also have laws on data protection.

The UK Information Commissioner's Office, the ICO, upholds information rights in the public interest, covering data protection.

The act contains eight 'Data Protection Principles'. These specify that personal data must be:

Complying with the Data Protection Principles is required by law; it also makes commercial sense.

1 Processed fairly and lawfully

2 Obtained for specified and lawful purposes

3 Adequate, relevant and not excessive

4 Accurate and up to date

5 Not kept any longer than necessary

6 Processed in accordance with the "data subject's" (the individual's) rights

7 Securely kept

8 Not transferred to any other country without adequate protection in situ

Data protection online

Businesses often obtain and use personal data online via websites, for example about individual clients or from prospective customers, or from the use of cookies or other tracking devices which they store on the user's computer. They may use social media platforms to process and share personal information.



Email correspondents and visitors to websites must be given clear information about the collection and use of their personal data. Easily accessible privacy notices available at a business's website should explain what personal data will be collected and held, the uses to which the data is put, such as for marketing the business's goods or services, and whether the data will be shared with credit reference agencies or any other third parties for any reason. The data controller's contact details must be provided.

Visitors must positively accept the terms of the privacy notice on visiting the website for the first time, and opt-in positively to give their consent before their personal data is collected and used. They must have the right to decline and click away from the web page.

There are only a few limited exceptions; thus unsolicited emails may be sent to existing customers who have previously bought similar goods or services.

“All use of personal data must be in accordance with the Data Protection Principles; as necessary and fair, accurately and so on. There are further specific obligations applying online.”

Data protection online

Cookies

Cookies may be set on users' devices to gain information commercially, for instance for user recognition, analytics and behavioural tracking. In the same way as for collecting other personal data online, their use requires clear information to be provided through notices, with explanations of the purposes for which the cookies are set, and any details on whether the data collected will be shared with third parties. Again, the data controller's contact details should be given.

In any event, acceptance must be positively signified in advance by way of ticking a box or by clicking acceptance, the first time each type of cookie is downloaded, so that the user is given the right to refuse and leave the site without any activation of the cookies.

There are some very limited exceptions, for example that the cookies are strictly necessary for the service the user is requesting, which could be for shopping cart activities, or where information derived from the cookies is aggregated and used only anonymously for statistical purposes.

Sanctions for breaches of data protection

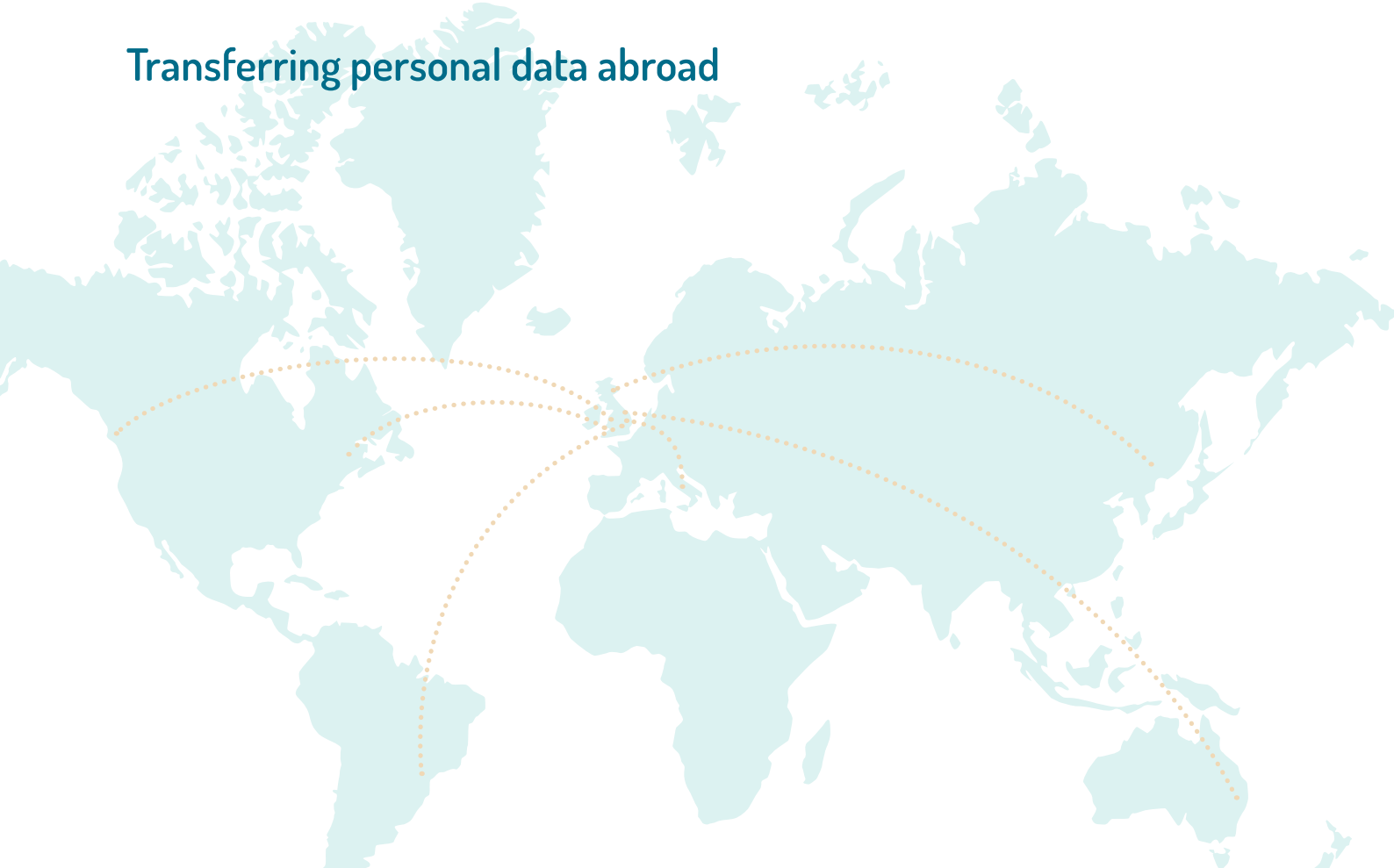
Data protection laws are enforceable by the ICO and by the courts. Criminal penalties such as fines or imprisonment may be imposed for serious data protection breaches.

The ICO may investigate complaints from data subjects about breaches of data protection. Individuals may also pursue rights in respect of their personal data through the courts.



Data protection online

Transferring personal data abroad



It is an easy matter to transfer personal data abroad online. However, the eighth Data Protection Principle regulates the sending of personal data outside the EEA. There must be adequate legal protection within the receiving state, unless the data subject has given consent or unless other specific exceptions are satisfied.

The European Commission has confirmed that certain identified countries do have an acceptable level of protection, such as Switzerland and Canada. In the United States, a voluntary regime for companies, known as the 'Safe Harbor' is recognised as providing adequate protection for personal data transferred from countries in the EEA to those companies who choose to comply with its rules.

All other transfers of personal data outside the EEA must fall within one of a number of legal exemptions to be permitted, ensuring that the data remains protected. The main exceptions are where the data subject has given express informed permission for the transfer, or where there is a contract providing adequate safeguards between the data controller and the party receiving the data.

Getting Started

.....

1

Register your holding and use of personal data with the ICO.

2

Develop and publish a policy for data protection. Review what personal information your business needs to hold and use, and set out procedures for its collection, processing, use, access and disclosure. Include how it is kept secure.

Post an appropriate privacy notice at your website, and standardise any relevant footers for emails.

3

4

Establish systems online for obtaining informed consent for use of visitors' personal data and for cookies.



What business benefits can I expect?



TRUST

Your customers and employees will appreciate that your business is treating their personal data securely.



ENGAGEMENT

By giving their consent for you to use their personal data, new leads together with existing contacts and customers will be genuinely interested in an ongoing relationship with your business.



SAVE MONEY

You will be using accurate personal information, and not wasting time or money on out-of-date data.

COMPLIANCE

By proactively complying with legal requirements you will be able to respond efficiently to any queries about personal data, saving costs and avoiding any expenses of having to defend claims.



FOLLOW THESE

TOP
TIPS

1

Lead from the top

Make an appointment at Board level (it may be you) to acknowledge the importance of driving a data protection strategy in your business.

2

Note extra requirements for sensitive data

Certain sensitive data is additionally regulated, such as a person's religious beliefs or politics, health, criminal convictions and ethnicity. Check that there are no special requirements in your business sector for using personal data, for example in health, finance, marketing or politics. If there are, ensure that you conform with them.

3

Check the mechanisms for obtaining consent

From time to time and when introducing new products and services, review how you are obtaining informed consent, and that you would be able to provide evidence of acceptance if necessary.

4

Provide data protection training

Your staff should be trained in data protection, and the training updated from time to time, including temporary and part-time staff.

5

Make use of the ICO website

Refer to the helpful ICO website if you have any queries about specific aspects of data protection.

6

Design data protection into systems

Consider data protection at an early stage when designing and implementing new information systems, processes, products and services. Evaluate and manage risks associated with personal data at the planning stage.

7

Understand that data protection and privacy law evolves

Keep up-to-date, so that you stay abreast of imminent changes intended to strengthen compliance with Data Protection Principles, increasing accountability and privacy management.



NEXT STEPS

1. Register to attend a fully-funded Business Development Workshop:
www.business.wales.gov.uk/superfastbusinesswales/events
2. Make an appointment to see a Business Adviser who will help you create a personal action plan to grow your business:
www.business.wales.gov.uk/contact-us

FOR FURTHER INFORMATION

See how other businesses in Wales have exploited Superfast Broadband:
www.business.wales.gov.uk/superfastbusinesswales/superfast-success-stories

Find out how much your business could save with our savings calculator:
www.business.wales.gov.uk/superfastbusinesswales/savings-calculator

Other Business Guides that may interest you include:
www.business.wales.gov.uk/superfastbusinesswales/superfast-business-guides

For monthly updates on business development, technology news and events subscribe to the Business Wales Newsletter:
<https://public.govdelivery.com/accounts/UKWALES/subscriber/new>

For more information call 03000 6 03000 or visit:
www.business.wales.gov.uk/superfastbusinesswales

