

Website laws and compliance

Did you know your website must adhere to some legal requirements? If not, I have written this blog to summarise them. If you collect user data on your website, then the **Data Protection Act** must be adhered to, and a website **Privacy Policy statement** would allow you to inform visitors of this. Other information such as **Company Information** needs to be displayed, and it is also important your site conforms to the **Web Accessibility Guidelines**. For e-commerce sites, **Consumer Protection** statements need to be displayed (Terms & Conditions, Delivery, Pricing and Returns Information etc.), and if you collect credit card information, the **PCI DSS** guidelines must also be met. Electronic Communication (i.e. Newsletters) also must confirm to the **Anti-Spam Laws**. This page provides summary with links to further information to ensure your website is legal.

Company information

As from 1st January 2007 the following applies to **Business Stationery (which includes Websites)**:

Whether in hard copy, electronic or any other form:

- A company must state its name, in legible lettering, on the following -
- all the company's business letters, order forms;
- all its notices and other official publications;
- all bills of exchange, promissory notes, endorsements, cheques and orders for money or goods purporting to be signed by, or on behalf of, the company;
- all its bills of parcels, invoices, receipts and letters of credit
- on all its websites

On all of its business letters, order forms or any of the company's web sites, the company must show in legible lettering –

- its place of registration
- registered number
- its registered office address
- and if it is being wound up, that fact
- Whenever an email is used where its paper equivalent would be caught by the stationery requirements then that email is also subject to the requirements. The above also applies to Limited Liability Partnerships.

How Does This Affect My Website?

For a registered business, the website needs to display the business name, place of registration, registered number, its registered office address and if it is being wound up.

Sources & More Info:

<http://www.companieshouse.gov.uk/promotional/busStationery.shtml>

Disability Discrimination Act (DDA) and Accessibility

The World Wide Web Consortium (W3C) is an international consortium where member organizations, full-time staff, and the public work together to develop Web standards. They have developed a set of standards to ensure websites are built to best and common practices which also ensure people with disabilities can use and operate websites.

They have split the Web Accessibility Guidelines into three "checkpoints".

Priority 1: A Web content developer must satisfy this checkpoint. Otherwise, one or more groups will find it impossible to access information in the document. Satisfying this checkpoint is a basic requirement for some groups to be able to use Web documents.

Priority 2: A Web content developer should satisfy this checkpoint. Otherwise, one or more groups will find it difficult to access information in the document. Satisfying this checkpoint will remove significant barriers to accessing Web documents.

Priority 3: A Web content developer may address this checkpoint. Otherwise, one or more groups will find it somewhat difficult to access information in the document. Satisfying this checkpoint will improve access to Web documents.

The UK Government and the RNIB both advise that your website must satisfy **Priority 1** of guidelines and should satisfy **Priority 2** guidelines. If the website is built to these guidelines then it allows people with disabilities to be able to use and operate your website. For example, a Screen Reader could be used to read out website content to a visually impaired user if the guidelines are followed.

The guidelines are not only for the web developer to take into account when building the site, but also need to be considered if content is added by other users using a content manager. For example, images added to the site should have the ALT attribute added to provide alternate text that a screen reader can read out. This is an example of one of the guidelines and with a content manager can easily be overlooked by the website administrator.

If you want to ensure your website conforms then contact your web developer for more information.

How Does This Affect My Website?

Your website should conform to at least **Priority 1** of the W3C Guidelines (or at least show that you have done all you can to adhere to it).

Sources & More Info:

<http://www.w3.org/>

http://en.wikipedia.org/wiki/Web_accessibility

Data Protection Act

The Data Protection Act defines UK law on the processing of people's data and is the main piece of legislation that governs the protection of personal data in the UK. It gives people the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.

The Act states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection
- It also provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

How Does This Affect My Website?

If your website collects users data, even a simple enquiry form asking for Name, Email and Phone Number, you should include a Privacy Policy that informs website visitors how you retain, process, disclose and purge their data in line with the requirements above.

Sources & More Info:

<http://www.ico.gov.uk>

http://en.wikipedia.org/wiki/Data_Protection_Act_1998

http://en.wikipedia.org/wiki/Privacy_policy

E-commerce Sites

If your site is an e-commerce website, then the further requirements must be met.

Consumer Protection (Distance Selling) Regulations

Distance Selling Regulations give protection to consumers who shop by phone, mail order, via the Internet or digital TV. The protection includes:

- The right to receive clear information about goods and services before deciding to buy;
- Confirmation of this information in writing;
- A cooling off period of seven working days in which the consumer can withdraw from the contract;
- Protection from credit card fraud.

How Does This Affect My Website?

The following information must be shown on your website, and this is commonly done via pages such as **Terms & Conditions, Delivery Details, Returns Policy etc.**

1. Identity of the supplier and address whereby payment is upfront.
2. A description of the service
3. The contract price inclusive of taxes
4. Delivery Cost (if applicable)
5. Payment and delivery arrangement
6. Notification of the right of cancellation (reg 13 of these Regulations)
7. The cost of the means of communication by which the contract is to be concluded (e.g. premium rate phone numbers)
8. The period for which the terms are available
9. Minimum duration of the contract, where it is not of one-off performance

Sources & More Info:

<http://www.berr.gov.uk/whatwedo/consumers/buying-selling/distance-selling/index.html>

http://en.wikipedia.org/wiki/Consumer_Protection_%28Distance_Selling%29_Regulations

Electronic Commerce Regulations (EC Directive)

The EU Ecommerce Directive is a policy for online service providers to ensure that customers can easily and quickly contact the service provider

How Does This Affect My Website?

The following information must be shown on your website:

- You should display the name of your business.
- We recommend you display your company registration number or proprietor's name (as you would in a letter).
- You should show your geographic address (street number etc, not just a PO box).
- You should show your contact information such as phone number and email address.
- You should show your VAT number if you are VAT registered.
- Refer to trade or professional recognition schemes, with registration number, if applicable.
- Provide clear information on price, tax and delivery.
- Show clear Terms and Conditions and acknowledge orders.

Sources & More Info:

<http://www.opsi.gov.uk/si/si2002/20022013.htm>

http://en.wikipedia.org/wiki/Electronic_Commerce_Regulations_2002

The EU Anti Spam Laws

If you send newsletters or marketing emails to email addresses, you must ensure that these people have opted in to receive your communications otherwise you could be breaking the law and be fined.

How Does This Affect My Website?

Firstly, if you use your website forms to collect users email addresses which you then use to send marketing emails to, you must ensure the user is offered an opt-in option to receive your emails. Customers are exempt from this but need to be offered an opt-out option.

Secondly, if you have a database of emails you must ensure these people have opted in to receive your marketing emails. So for example, if you purchased a database of emails, you must ensure these people have initially given consent to pass their emails on to third parties.

Thirdly, if you use an email marketing or newsletter system, such as our Email Marketer, you must make sure opt-out instructions have been provided.

Sources & More Info:

http://en.wikipedia.org/wiki/Directive_on_Privacy_and_Electronic_Communications

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was created to help prevent credit card fraud with organisations that process credit or debit card payments. It ensures controls around data are increased and reduces exposure to compromise. The standard applies to all organisations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

The industry standard PCI DSS, includes 12 key requirements for organisations that accept or processes card payments:

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for passwords or other security parameters
- Protect stored data
- Encrypt the transmission of cardholder data and sensitive information
- Use and regularly update anti-virus software
- Develop and maintain securer systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

How Does This Affect My Website?

It is not only your website that are affected, but the server your website is hosted on also. You should check with your web hosting developer and e-commerce system provider that:

- you have a suitable **firewall** on the server
- system passwords are **secure**
- if you save credit/debit card that it is protected, the website have a suitable **SSL certificate** to **encrypt** transmitted data
- the server uses **anti virus** software
- the systems are **secure and access** is only granted to those who need it.

Sources & More Info:

<https://www.pcisecuritystandards.org/>

<http://www.visaeurope.com/aboutvisa/security/ais/requirements.jsp>

http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

So What Does My Website Need to Confirm?

To summarise all the above and ensure your website is legal you must:

All Websites

- Adhere to Priority 1 of the Web Accessibility Guidelines set out at W3C For a registered business, the website needs to display the following Company Information: the Business Name, place of registration, registered number, its registered office address and if it is being wound up.
- If the website collects user data (i.e. via simple enquiry form, or shopping cart), display a Privacy Policy informing the user what the business does with the data and that it conforms to the Data Protection Act

E-commerce Sites

- Have Terms & Conditions, Delivery and Returns Policy pages to display information as part of the Consumer Regulations Directive and the Electronic Commerce Regulations.
- To conform to Anti Spam laws, ensure your email database is of opt-in email addresses, and include an opt-out instruction on all marketing emails sent
- Perform a PCI DSS Self Assessment check to ensure your e-commerce website conforms to the PCI DSS.
- Hope this helps. If you think I have missed anything or have anything wrong, please feel free to post a comment below or email me.

Part III of the DDA refers to the provision of goods, facilities and services. The Code of Practice which specifically mentions websites, can be downloaded in its entirety from the Equality and Human Rights Commission website.