Think Ahead ACCA

Guide from

HA Accountants

Tel: 01582-481381 Email: info@ha-accountants.co.uk, www.ha-accountants.com

Cloud Accounting & Business Advisory Services

GDPR – your data protection responsibilities

GDPR, the new General Data Protection Regulation, comes into effect on 25 May 2018. Although GDPR originated with the European Union, it is not affected by Brexit. GDPR builds on existing data protection law to strengthen the protection of individuals' personal data.

If your business collects or uses personal data, you must comply with GDPR. You'll need to review any existing data protection systems, policies and procedures to take account of the changes from the old Data Protection Act.

1. Does GDPR apply to you?

GDPR applies to both 'data controllers' and 'data processors'

- Most businesses are data controllers. For example, you might hold personal data on your employees and customers.
- Data processors process personal data on behalf of the data controller. For example, that includes payroll service providers, 'cloud' services that process personal data and so on.
- If your business holds or uses any personal data systematically, GDPR is likely to apply to you.

The definition of personal data is wider than it was under previous regulations

- Employee records, customer databases and so on continue to count as personal data.
- Technical data such as IP addresses, smartphone device IDs or location information can count as personal data if it can be linked to an individual.
- 'Pseudonymised' information that cannot be linked to an individual is not included.
- The rules apply to manual filing systems as well as computerised records.

There are stricter rules for sensitive personal data

- Sensitive data continues to include information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, and information on sex life or sexual orientation.
- Genetic or biometric data are also sensitive data.
- There are separate rules on handling information about an individual's criminal convictions.

Fines for non-compliance can be very substantial

- Maximum fines are up to 4% of annual turnover for the worst offenders.
- In practice, the Information Commissioner's Office (which regulates data protection) aims to work with businesses to improve compliance rather than issuing fines.
- Keeping good records and taking prompt action if there is a problem will help reduce the risk of any penalty.

Notification and fees

The existing system of 'notifying' with the Information Commissioner's Office is changing

- Under the Data Protection Act, businesses that use personal data for other than 'core business purposes' (such as staff administration and marketing your products) are required to notify and pay a fee.
- GDPR removes this requirement to notify, but data controllers will still be required to pay ICO a data protection fee.

Fees will vary for different organisations

- Small businesses that do not process large volumes of data will pay the lowest fees of up to £55.
- Small businesses that process over 10,000 records will pay up to £80.
- Larger businesses, with over 250 employees or turnover above £50 million will pay up to £1,000.
- There will be an additional direct marketing top up of £20 for businesses that use electronic marketing.

The new system comes into effect on 1 April 2018

2. When can you use personal data?

You can only collect and use personal data for a limited number of lawful reasons.

You may need to in order to carry out a contract with that individual

- For example, you might need to record a customer's name and contact details, send them updates on order progress and so on.
- This does not mean that you can keep customer data and carry on sending them marketing emails indefinitely (see the PECR point, below).

You can ask individuals for their consent

- For example, you might ask customers for permission to 'stay in touch' after you have completed an order. Your website might include a box for visitors to sign up to your mailing list.
- You must ask in clear, easily understood language. Privacy notices must give clear information about who you are, how you will use their data and details of anyone you will share it with.
- The individual must positively opt-in. Pre-ticked consent boxes are not allowed.
- Consent must be freely given.
- You must inform individuals of their rights, including the right to withdraw consent. Withdrawing consent must be as easy as giving it was.
- Special rules apply for children. Any consent request needs to be in appropriate language, and you will normally need the consent of their parent or guardian as well.
- A business can process any employee details they need to for the purposes of running the business. For example, this can include their contact details (including next-of-kin), birthday, PAYE, salary and pensions details, medical information and criminal records. You do not need the consent of the employee to process this information provided it is required to operate the business.

You may be able to process data when it is in the legitimate interests of the business

- You need to balance the interests of the business against the rights of the individuals.

- For example, you might have legitimate reasons for wanting to monitor employees' use of the internet. You would need to make sure employees know what you are doing and why. You would also need to make sure monitoring isn't excessive or abused in any way.
- Direct marketing is a legitimate use of personal information. However, the Privacy and Electronic Communication Regulations 2003 (PECR) apply.

It is PECR, rather than GDPR, regulations that restrict the circumstances in which you can send marketing to people by phone, fax, email, text, or picture or video message. For example, businesses can only email customers and former customers without their explicit consent if an email opt out option is offered.

See the ICO's handy Direct Marketing Checklist and read their 50-page Direct Marketing Guidance.

You can process personal data when this is required to comply with other legal obligations

- For examp
- le, to deal with PAYE, produce payslips for your employees and so on.

Other lawful reasons are unlikely to apply to your business

- You can process personal data when this is necessary to protect the vital interests of an individual. Typically, this would be in a life or death situation.
- You can process personal data in the public interest or where you have official authority.

Tighter conditions apply to the processing of sensitive personal data

- It's safest to do this only with the individual's explicit consent or when you are legally required to.
- Personal data can be used when needed for medical diagnosis or treatment, and for making or defending a legal claim.

3. Managing privacy in the business

Take data protection seriously

- Assign someone to take responsibility for GDPR. Make sure they have the resources to understand the organisational, legal and technical issues involved. If necessary, get external advice from a specialist.
- Make a top-level commitment to complying with GDPR. For example, data protection should be an item on the board's agenda. Whoever is responsible for compliance should report directly to senior management.
- Institute training for all employees to make sure they are aware of the importance of data protection and understand the procedures they must follow.
- You must appoint a data protection officer if your business carries out large scale monitoring (eg online behaviour tracking) or processing of sensitive data. This can be an employee or an external specialist.

Make sure you understand how your business is processing personal data

- What data are you processing, how? What is the legal basis for each type of processing you do?
- Keep clear records of what you are doing, and what steps you take to protect the data.

Make data protection a key part of your approach

- Minimise the personal data you collect. For example, there may be no need to know a customer's age, gender and so on. Don't collect extra information just because it might be helpful later on.
- Don't keep data longer than you need to.
- Check that you have adequate technologies and procedures to protect personal data.
- Assess and minimise the privacy impact of any new project involving personal data at the start. For example, if you decide to upgrade your IT, install CCTV or introduce a new CRM system.

Check any suppliers you share personal data with

- For example, if you are using an agency to track and analyse website visitors. Do they have adequate security and procedures for complying with GDPR?
- Only share the personal data they need to provide the service. If they don't need to know individuals' names, can data be pseudonymised?
- You must have a clear contract limiting how they can use the data. They must not share the data with anyone else (including any subcontractors they use) without your permission.
- Make sure the data will be returned to you (or erased by them) at the end of the contract.

4. Individuals' rights

You must respect individuals' rights. You may need to upgrade your systems and procedures to help you do this.

The right to be informed

- You need to let individuals know what personal data you are processing. Typically you do this with a privacy notice. Privacy notices must be clear, easy to find and easy to understand.
- The privacy notice must include your business name and contact details, why you are processing the information (eg for direct marketing or to personalise the website experience) and how long you will keep it. You also need to give details if the information will be shared with anyone else.
- You must inform the individual of their rights (such as the right to withdraw consent).
- If you are collecting information from the individual (eg asking for cookie consent on your website), the privacy notice should be provided at the time.
- If you collect data elsewhere (eg by buying a mailing list), you should provide the information when you first contact them and at the latest within a month.

Seeing and correcting data

- Individuals have the right to see a copy of the information you hold, within a month of asking. You cannot charge for providing this.
- For electronic requests, you should provide the information in a suitable electronic form. Individuals can also ask for data to be provided electronically so that they can share it with another service.
- They can ask for inaccurate information to be corrected.

Objections and data erasure

- Individuals have a right to have their data erased in most circumstances. For example, if they withdraw consent or if you no longer have a legitimate need for the data.
- You may need to stop processing (but not erase) an individual's data if they object to the processing or say the data is inaccurate.

- Individuals also have the right to object to automated decision-making. For example, if their application for credit is automatically assessed and declined, or your recruitment process automatically rejects their CV.

5. Security and data breaches

You must protect personal data with appropriate security

- This will typically include technical security
- such as firewalls and anti-virus software, passwords and so on. Make sure data is encrypted, so that it cannot be read even if your systems are hacked.
- Physical security (eg for your premises) also helps protect against theft or loss of data, either on computer systems or paper-based.
- Portable devices (eg laptops and smartphones) and data on employees' own systems (eg for homeworking) can be at greatest risk.
- The biggest weakness in most security is people. Make sure your employees understand and follow security procedures.

You must report most security incidents to the ICO

- You must report any data breach that is likely to harm individuals – for example, because personal data has been put at risk. You would not need to report the loss of a securely-encrypted USB containing personal data.
- You must report the incident within 72 hours of becoming aware of it.
- You should tell the ICO what you know about what has happened, including what data and individuals are at risk. You should also tell them what you are doing about it.

You may need to report security incidents to the individuals affected

- You must do this if they have been put at high risk. For example, if a hacker may have gained access to credit card details, or be in a position to commit identity fraud.
- They should be informed without undue delay and given clear information on what has happened.
- A breach that only disclosed the names and addresses of customers or employees would be unlikely to be high risk if these are already publicly available.

Signpost

- Find guidance for business from the Information Commissioner's Office (0303 123 1113). The helpline includes a dedicated small business advice line offering help with GDPR, data protection, electronic marketing and other legislation they regulate.
- Find a solicitor through the Law Society for advice on making sure your business is GDPR-compliant.
- Download a practical guide to IT security from the Information Commissioner's Office.
- Find guidance on the government's Cyber Essentials scheme for protecting your business against online threats.

April 2018