



what you need to know to start and grow your business

data protection

What is data protection?

Data protection, or data privacy, is concerned with the protection of individuals' personal data - how it is shared with and used by others. Statutory regulation is not restricted to the internet, but the ease with which large amounts of data can be stored, shared and processed on the internet means data protection is a key issue for any business with an online presence. The 2018 EU General Data Protection Regulation (GDPR) boosted awareness, and set a high (but manageable) bar for compliance. The UK has equivalent legislation. First, terminology:

PERSONAL DATA	DATA PROCESSING	DATA PROCESSOR	DATA CONTROLLER
any information that can, on its own or in combination with other information, be used to identify an individual, even if this information is already in the public domain. This includes someone's name, phone number, email or postal address, computer IP address, bank details, photos, etc.	handling data in pretty much any way - collecting, storing, analysing, deleting, combining with other data or sharing with someone else	any person or organisation that processes the data on behalf of the data controller, in accordance with the controller's instructions	organisation calling the shots on 'what, how and why' for collecting and using the personal data. It is the data controller who must make sure any processing of personal data complies with the law - and who will be liable for any data breaches or other non-compliance. The controller will usually be the business rather than any individual, although if you set up as sole trader it will be you. (An employee making these decisions on behalf of his/her employer is not the data controller - the employer will be.)
'SPECIAL CATEGORIES' of personal data sensitive personal data such as information concerning someone's age, race, gender, religion, sexuality, political views or trade union memberships, or biometric, genetic or health data.	DATA SUBJECT		
	any individual resident in the EU (or in the UK for UK Law) - customers, website subscribers, employees, patients, etc.		

Why is it important?

As an individual, an extraordinary amount can be done with your personal data without you even being aware: important to retain control. As a business, whatever your size, there are potentially very serious consequences:

- data breach or other act that affects an individual's rights: fine up to higher of £20M or 4% of your global annual turnover
- administrative non-compliance: fine up to higher of €10M or 2% of global annual turnover
- reputational damage and loss of consumer trust

What are the basic principles?

- lawfulness, fairness and transparency (in how you use personal data)
- purpose limitation (only collect and use for valid, explained purposes)
- data minimisation (only keep data you need for explained purposes)
- accuracy (keep the data accurate and up to date)
- storage limitation (store only for time needed for explained purposes)
- integrity and confidentiality (store the data securely)
- accountability (take responsibility, appropriate measures in place)

What do I need to do to comply?

Create a policy	Comply with your policy	Register at Information Commissioner's Office?
<ul style="list-style-type: none">• Even if not online• Keep it simple• Address all the points in the circles below	<ul style="list-style-type: none">• Carry out an internal check before launching: can you give necessary explanation and confirmation for each of the policy promises?• Calendarise and carry out regular reviews: delete data no longer needed.	<ul style="list-style-type: none">• Check whether you need to register as a data controller with relevant data authority (example: if using data for non-core business activities such as advertising/marketing for others).• If in doubt, register anyway: only a small annual fee for micro/small/medium businesses.
Impact assessment	Appoint Data Protection Officer?	
<ul style="list-style-type: none">• Unlikely to be needed for a small business.• This is an assessment upfront of risk to individuals if you will be obtaining, using or storing on a large scale 'special categories' of personal data; systematically monitoring areas open to the public (eg car park CCTV); or systematically profiling or other processing eg an employer monitoring employees' internet usage.	<ul style="list-style-type: none">• Unlikely to apply to a small business.• Only needed in similar situations as for impact assessments.• Still good practice to nominate one of your team to be responsible for data protection.	

How do I create a data protection policy?

Your data protection policy needs to clearly address all of the issues described below. You should ask a lawyer to assist if you are not comfortable doing this. If you run a shop on an online marketplace, you may have the option of using their suggested standard privacy terms with minimal adaptation. However, you still need to develop your own policy for the business you run offline or via your own website.



What about cookies?

What are cookies?	How do I comply with GDPR?
Small text files with a website name and unique user ID that users download when accessing a website. On return to the site, the cookie makes the device message the website, so it 'remembers' user details, preferences and settings. This can be very useful for users, but can also be used by websites to help tailor advertising to meet a user's preferences.	There is additional legislation as well as GDPR. In short, make sure you obtain express consent from your website users to the use of the cookies for any particular purposes that you specify.
	Usually done by including a tick-box for first time visitors to click on.

How do I handle subject access requests?

- Any data subject can ask to access, edit or object to particular use of any of their personal data being held or handled by your business, or even to have particular personal data records deleted.
- There is no prescribed form for the request: does not need to be in writing, can be made orally
 - Note that your employees and other staff can make a subject access request
 - You must respond within one month (not much scope to extend).
- Make sure your business has the necessary processes and technology in place to respond

What to do if there's a data breach

A data breach is a breach of security, however caused, leading to accidental/unlawful destruction, loss, alteration, unauthorised disclosure of/access to personal data.

- Put in place reliable breach detection, investigation and internal reporting process.
- If likely to result in risk of affecting individual's rights and freedoms, report to relevant authority (UK: Information Commissioner's Office) within 72 hours.
- If likely to result in high risk of affecting individual's rights and freedoms, inform individual without undue delay.
- Always keep record, even if no need to report.

Also think about

- Cybersecurity: how robust are your security measures?
- Confidentiality • Selling Online • Disputes • Contracts

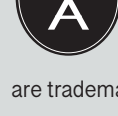
This content is for general information purposes only and does not constitute legal, financial or tax advice.

To address any specific concern, you should not rely on this content and should seek appropriate advice for the relevant jurisdiction.

To find more information or request help or advice:



© 2019 Venture Adventures Limited



VENTURE ADVENTURES



are trademarks of Venture Adventures Limited. All rights reserved.