

Data protection

Better rules for small business

Stronger rules on data protection from May 2018 mean citizens have more control over their data and business benefits from a level playing field. One set of rules for all companies operating in the EU, wherever they are based. Find out what this means for your SME.

January 2017 EN

What is personal data?



	Name
	Address
	Localisation
	Online identifier
	Health information
	Income
	Cultural profile
	and more

COLLECT
STORE
USE/RE-USE
DATA?

You have to abide by the rules

Process data for other companies?
This is for you too.

Why change the rules?

It's about trust...

A lack of trust in old data protection rules held back the digital economy and quite possibly your business.



of people feel they have complete control over the information they provide online

And helping business boom

One set of rules for all companies processing data in the EU

Doing business just got easier and fairer

The new system keeps costs down and will help business grow



€130 million

cost of informing 28 different Data Protection Authorities for business in the EU under the old system



€2.3 billion

estimated economic benefits of having one law

New rules should boost consumer confidence and in turn business.

What your company must do

Protect the rights of people giving you their data



Communication

- Use plain language.
- Tell them **who** you are when you request the data.
- Say **why** you are processing their data, **how long** it will be stored and **who** receives it.



Warnings

Inform people of data breaches if there is a serious risk to them.



Consent

Get their clear consent to process the data.

Collecting from children for social media? Check age limit for parental consent.



Access and Portability

Let people access their data and give it to another company.



Safeguarding sensitive data

Use extra safeguards for information on health, race, sexual orientation, religion and political beliefs.



Erase data

Give people the 'right to be forgotten'. Erase their personal data if they ask, but only if it doesn't compromise freedom of expression or the ability to research.



Marketing

Give people the right to opt out of direct marketing that uses their data.



Profiling

If you use profiling to process applications for legally-binding agreements like loans, you must:

- Inform your customers;
- Make sure you have a person, not a machine, checking the process if the application ends in a refusal;
- Offer the applicant the right to contest the decision.



Data transfer outside the EU

Make legal arrangements when you transfer data to countries that have not been approved by the EU authorities.

Do data protection by design

Build data protection safeguards into your products and services from the earliest stages of development.



Processing data for another company?

Make sure you have a watertight contract listing the responsibilities of each party.

Check if you need a data protection officer

This is not always obligatory. It depends on the type and amount of data you collect, whether processing is your main business and if you do it on a large scale.

You process personal data to target advertising through search engines based on people's behaviour online.	Yes 
You send your clients an advert once a year to promote your local food business.	No
You are a GP and collect data on your patients' health.	No
You process personal data on genetics and health for a hospital.	Yes 

Keep records

SMEs only have to keep records if data processing is

Regular

A threat to people's rights and freedoms

Dealing with sensitive data or criminal records

Records should contain:

- ✓ Name and contact details of business
- ✓ Reasons for data processing
- ✓ Description of categories of data subjects and personal data
- ✓ Categories of organisations receiving the data
- ✓ Transfer of data to another country or organisation
- ✓ Time limit for removal of data, if possible
- ✓ Description of security measures used when processing, if possible

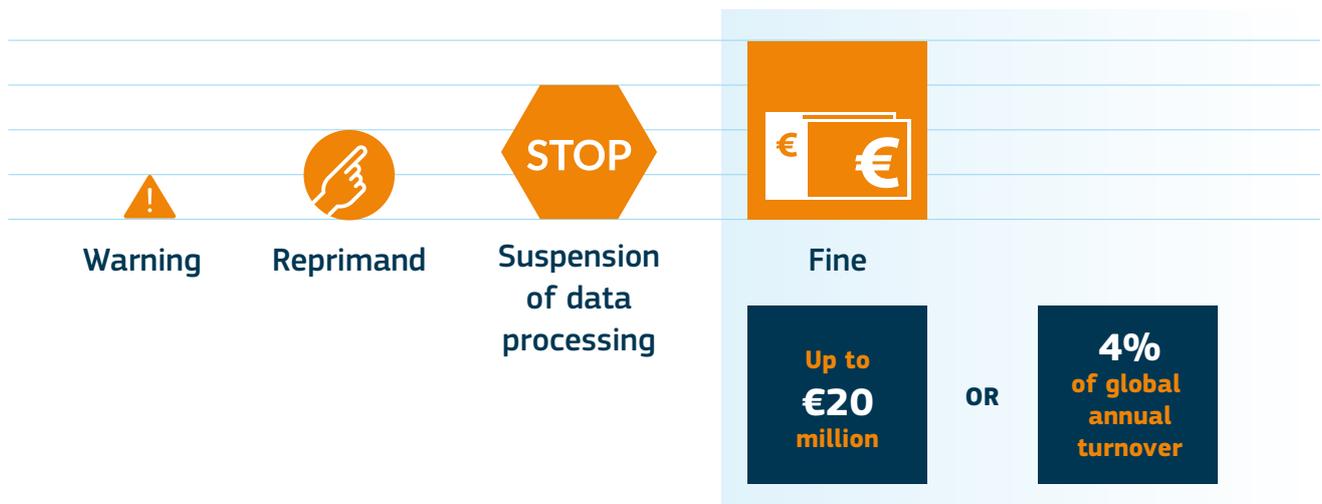
Anticipate with impact assessments

Impact assessments may be required for **HIGH-RISK** processing.



The cost of non-compliance

Your local Data Protection Authority monitors compliance; their work is coordinated at EU-level. The cost of falling foul of the rules can be high.



Protect data, protect your business

More on the EU's data protection law

<http://ec.europa.eu/justice/data-protection/>

Contact Your Data Protection Authority

http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

This document should not be considered as representative of the European Commission's official position and does not replace the legislation.