

# GDPR is coming

## 12 Steps to take now

1

### Spreading the word

Raise awareness about the impending changes within your company. Make especially sure decision makers and any key people know, so they can prepare for the changes.

2

### Document the personal data you have

Figure out where the information you have came from, and who you share it with. Could be time for an audit.

3

### Communicating privacy information

Review your current privacy notices, and put a plan in place for any changes you need to make to adhere to the new rules.

4

### Individuals' rights

Check that your company's procedures cover all the rights people have, like how you would delete people's personal data.

5

### Subject access requests

Check if you need to update how you process subject access requests, and who will do these, within the new one-month timescale. You mostly won't be able to charge for this anymore. In very limited circumstances, you can refuse a request. You have to explain why and let the person know they can complain to the Supervisory Authority.

7

### Consent

Double-check how you record and manage consent. Consent must be informed, given freely and explicit; you cannot just assume it from inactivity or silence.

9

### Data protection by design & Data Protection Impact Assessments (DPIA)

Get reading and familiarising with the ICO's code of practice on PIA. You should also check out Article 29 Working Party's guidance document. Please note that PIA stands for Privacy Impact Assessment.

11

### Data breaches

These are about to be taken much more seriously. You'll have 72 hours to report one to your Supervisory Authority. Check you have the right procedures in place to detect and report them.

6

### Lawful basis for processing personal data

Check the lawful basis for your processing activity in the GDPR, document it, and update your privacy notice to explain it.

8

### Children

Assess whether you need to start verifying people's ages, or obtaining parental/guardian consent for any data processing activity. The GDPR brings special protection for minors' personal data, especially in the case of social media. If you now need their consent to collect data on them, in the near future you may need a parent or guardian's consent. A child can give consent at 16 (this might be lowered to 13 in the UK).

10

### Data Protection Officers

You should designate someone super reliable within your company to check that everything you do with data complies with the GDPR. Figure out where they'll sit within your company's structure and governance arrangements. Also, assess whether you need to officially designate a DPO.

12

### International

If your company operates internationally and you are cross-border processing, find out who your lead Supervisory Authority is. Again, that handy Article 29 Working Party Guideline will help you out.



## Summary

Don't worry - it's not that scary. Basically, you just need to review what you're already doing with people's data, and begin adapting your policies to adhere to the GDPR.