



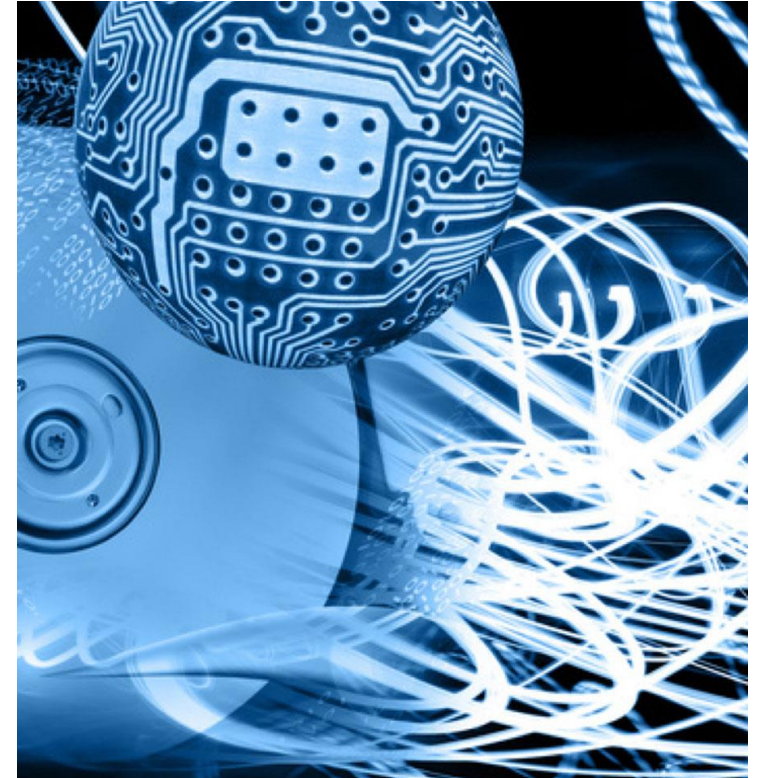
General Data Protection Regulation (GDPR)

[name] [date]



Learning objectives

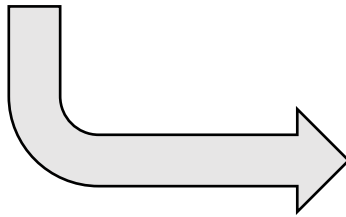
- What is personal data?
- What are the consequences?
- Data protection principles and rights
- Our company's data protection policy





What has changed

Data Protection Act



General Data Protection
Regulation (GDPR)



What is personal data?



- “... information relating to a living individual who can be identified from that data...”
- “...it may include expressions of opinion...”
- “...held in manual or electronic systems...”
- ICO guidance



What constitutes personal data?

Our company's
annual report

NO

Your salary details

YES

Your medical
information

YES

Your name and date
of birth

YES

Your anonymous
response to a survey
question

NO

Your photo or
image on a CCTV
camera

YES



What is personal data under GDPR?

“...IP addresses...”

“...automated personal data and data held in manual systems...”

“...key-coded (pseudonymised) personal data...”

Sensitive personal data



Special categories of
personal data (Article 9)



Special categories of personal data

Your name and date
of birth

NO

Racial or ethnic
origin

YES

Genetic data

YES

Religious or political
beliefs

YES

Data concerning sex
life or sexual
orientation

YES

Biometric data

YES



Lawful processing

1. Explicit consent of the data subject
2. Necessary for the performance of a contract
3. Necessary for legal or judicial reasons
4. Necessary to protect the data subject's best interests
5. Necessary to perform a task carried out in the public interest
6. Necessary for legitimate interests





What rights do data subjects have?

I don't want to receive your marketing letters and promotions

I want to be able to take my data and reuse it on other platforms

Did I agree to that? I didn't see a privacy notice on your website when I typed in my details

Does the right to be forgotten apply to me?

I want to have any errors corrected

I want to find out what data you have about me and how you're using it

Please stop using my data until you've checked there is a legitimate purpose



Rights of individuals under GDPR

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure (“right to be forgotten”)
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights on automated decision making & profiling





When it goes wrong

TalkTalk fined £400k
by ICO for cyber
attack

1b customer
accounts hacked,
admits Yahoo

Shop owner fined
for using instore
CCTV without
registering

Social worker drives
off with family court
data on roof

Loan company fined
£70k for spam texts

Insurance firm
fined £150k for
losing 60,000
customers' data



You make the call: Is it a breach?



“She asked me to remove her information from our systems – but it’s required for regulatory reasons, so I refused”

Breach

No Breach ✓



You make the call: Is it a breach?



“At first, he gave us his consent to use his data but then he changed his mind – I told him that it wasn’t allowed”

Breach ✓

No Breach



You make the call: Is it a breach?



“We assumed she gave us her consent because she placed an order with us and friended us on social media”

Breach ✓

No Breach



Data breach notifications

A data breach only occurs when data is lost

No. It can occur if data is accessed inappropriately due to a lack of internal controls

Breaches are only serious if data is actually taken

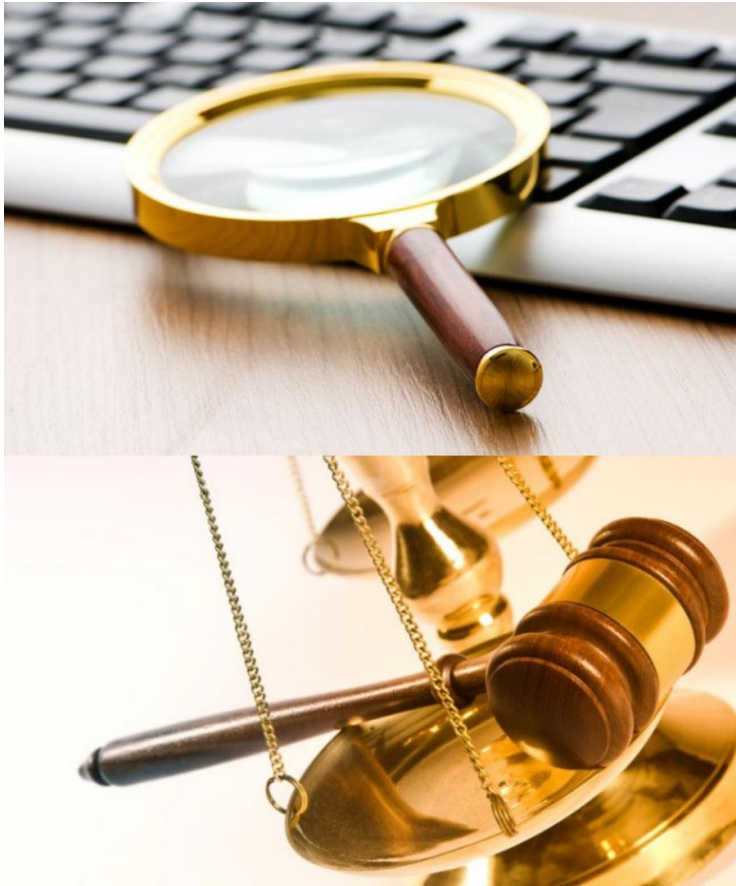
No. Unauthorised access, disclosures, loss, destruction, and alteration are also serious

Look at Yahoo – isn't it best to keep quiet?

No. Under GDPR, you just have 72 hours to notify of data breaches



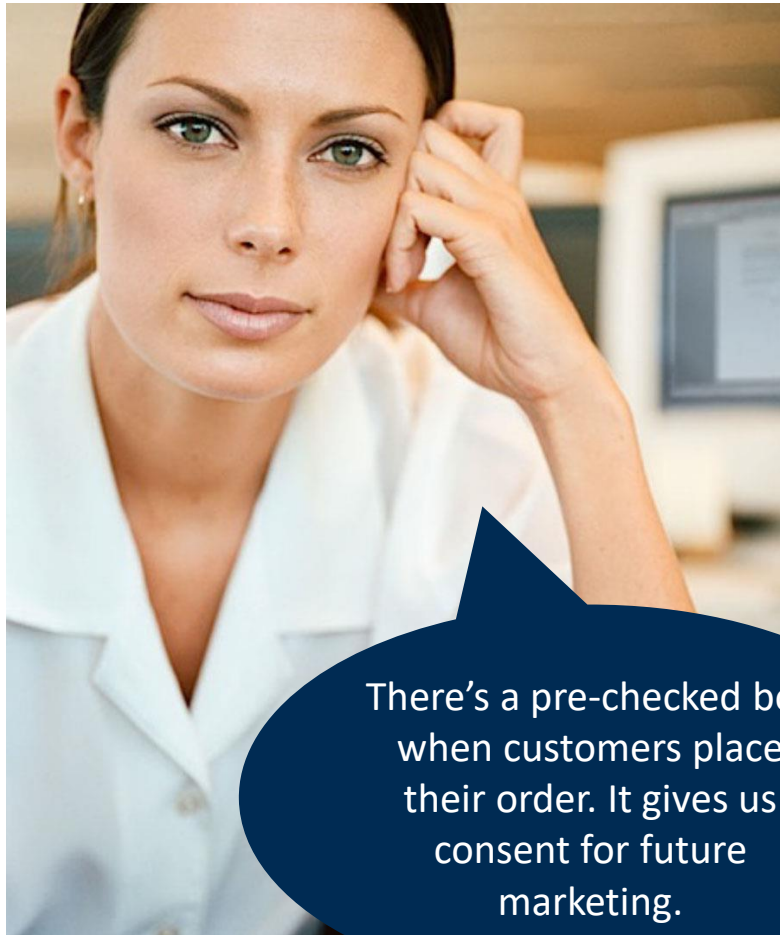
Fines under GDPR



- Infringements of rights, basic principles and rules on international transfers:
 - 4% of worldwide turnover or €20 million
- Failure to notify of data breaches:
 - 2% of worldwide turnover or €10 million



Scenario 1



There's a pre-checked box when customers place their order. It gives us consent for future marketing.

What do you think?

- a) Great – it looks like Jayne is on top of GDPR already
- b) Not bad – but Jayne can get consent verbally from customers too
- c) Poor – Jayne must ensure that consent is active ✓
- d) Poor – consent is only required for children under 13 years



Scenario 2



We've got a US firm helping us process customer data. It's all big-data analytics wizardry.

What do you think?

- a) Excellent – it looks like Peter really knows his stuff
- b) Great – there are no restrictions on transfers outside the EU
- c) Not bad – but Peter must ensure there are adequate safeguards for EU data ✓
- d) Poor – Peter must get consent from the supervisory authority first



Our Data Protection Policy

1. What personal data we use and how
2. Our rules and procedures – creating, storing, sharing and disposing of personal data safely
3. Identifying our Data Protection Officer and how to contact them
4. Requiring everyone to read and implement our Data Protection Policy



Do

- ✓ Read our Company's Data Protection Policy – make sure you understand the rules and why they're important
- ✓ Follow our policies and rules whenever you use personal data – taking particular care to prevent unauthorised access, loss, theft or alteration
- ✓ Speak out promptly if you accidentally lose, delete or transfer personal data to someone else – our firm has just 72 hours to report it
- ✓ Talk to your manager or our Data Protection Officer if you have any questions or concerns



Don't

- ✗ Keep using customers' personal data for marketing if they ask you to stop
- ✗ Transfer personal data outside the EU without ensuring there are adequate protections in place
- ✗ Leave personal data lying around on a desk or unattended onscreen
- ✗ Collect or use children's personal data without getting parental consent first



Questions, comments
or concerns?



Next steps

- Call _____ on _____ if you need information or guidance
- Call _____ on _____ if you need to raise concerns
- Access self-study courses on our e-learning portal for further training [or optionally – Complete your mandatory training on our corporate e-learning portal]



About Skillcast

- Skillcast provides digital learning content, technology and services to help you train your staff, automate your compliance processes and generate management reports to help you keep track of it all.
- Our best-selling Compliance Essentials Library provides a complete and comprehensive off-the-shelf compliance solution for UK businesses.

Register for a free trial at <https://www.skillcast.com/free-trial>

Copyright © 2022 Skillcast. All Rights Reserved

