

Na Sambathchatovong
Cyber Researcher

Data Privacy: General Data Protection Regulation



Learning Objectives



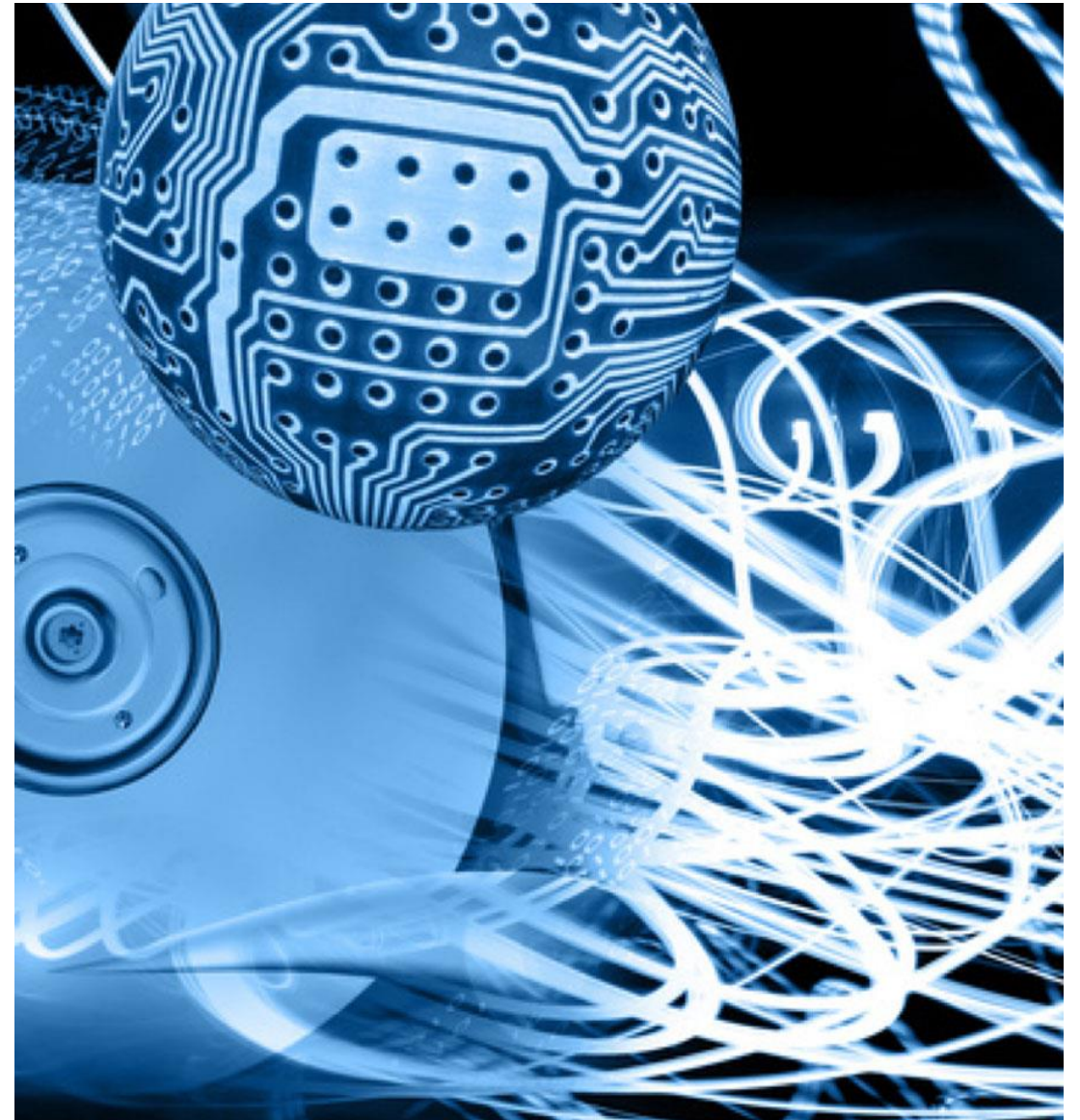
Who is who?

What is personal data?

What are the consequences?

Data protection principles and rights

Our company's data protection policy

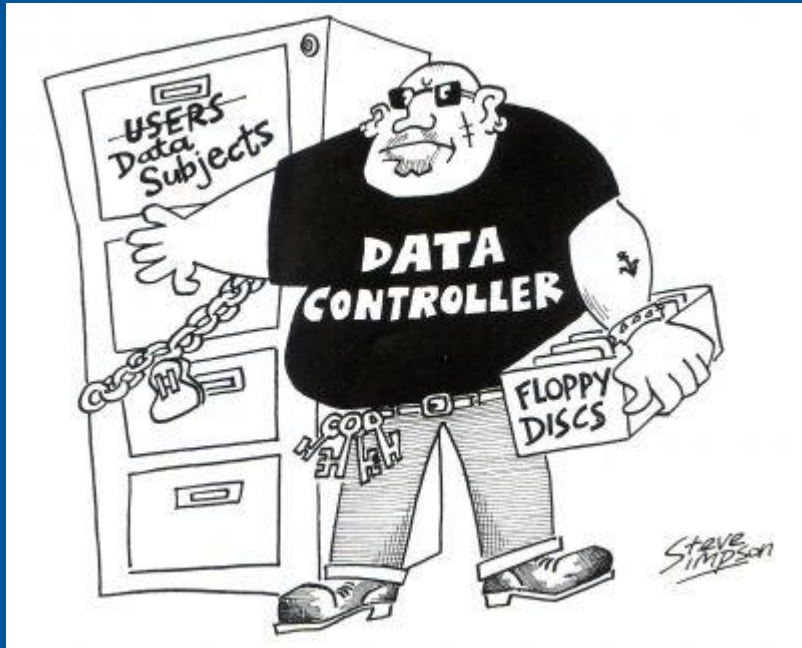


What's has changed?

Data Protection Act



**General Data Protection
Regulation (GDPR)**



If Data Protection Law applies

A **data controller** will have a certain number of obligations

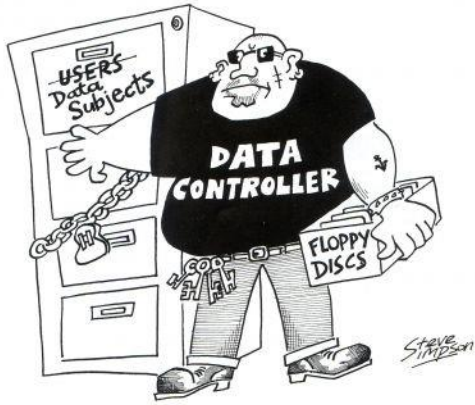


As well as his **data processor**



A **data subject** will have a certain number of rights





The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data



a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller





An identified or identifiable natural person whose personal data are being processed (by the data controller)



Who is who?






“A travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers”.

Who is the data controller?



“Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. ...The users of such networks, upload(...) personal data also of third parties”.

Who is the data controller?



“Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. **These service providers are data controllers**, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, **would qualify as controllers** provided that their activities are not subject to the so-called "household exception"”. [2010]

Article 29 WP

3. You shall only collect the data that are necessary to pursue this purpose

4. You shall keep the data for non longer than necessary

5. You shall only keep accurate data

6. You shall keep the data secure

2. You shall process the data for a specified/specific and limited purpose

7. You shall enable data subjects to exercise their rights

1. You shall have a legal basis to process the data



8. You should maintain a record of processing activities

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

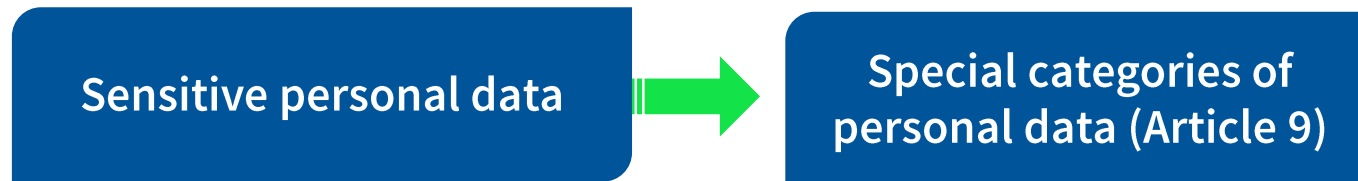
What is personal data under GDPR?



“...IP addresses...”

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

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



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

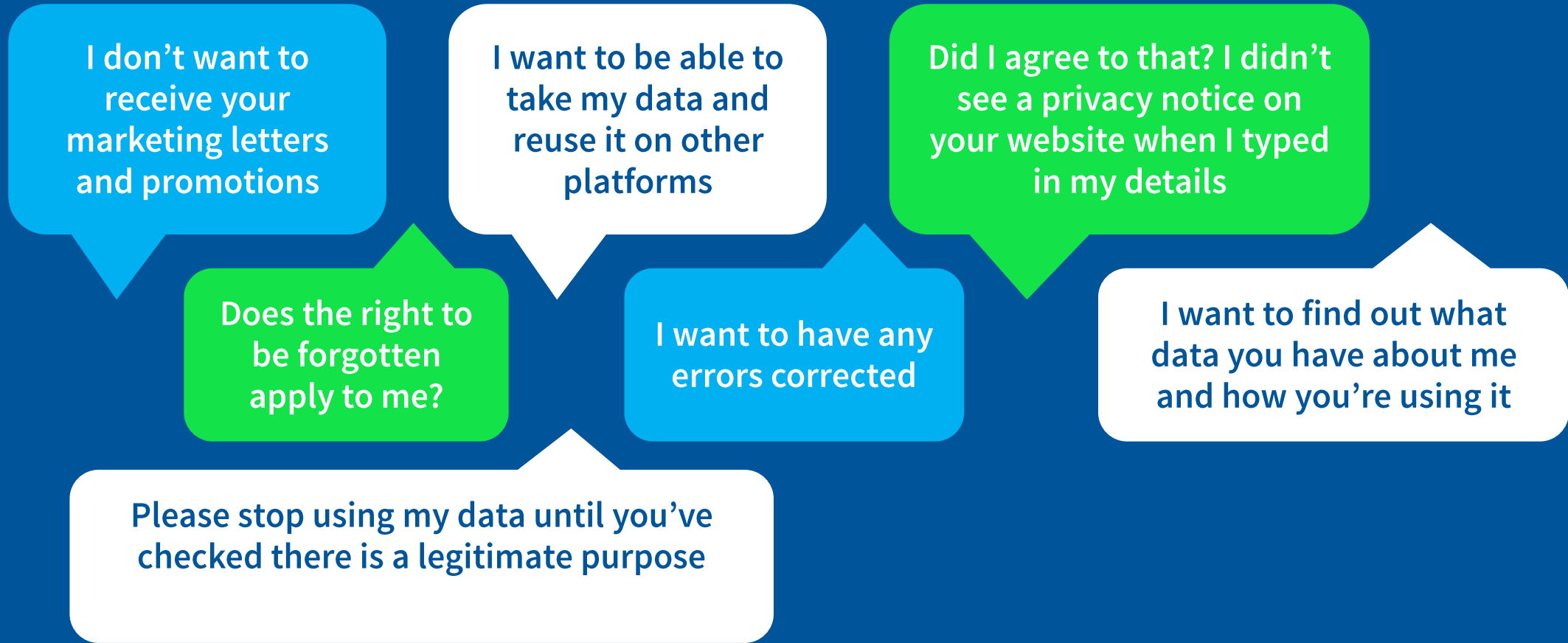
YES

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?



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**

When it goes wrong



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



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

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

To Do



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



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

Privacy and Data Protection in the age of COVID-19:

Does Data Protection hinder the measures that need to be taken for public health?



Privacy and Data Protection in the age of COVID-19:



Does the processing of health data by public authorities open the door to surveillance?



Any Questions?

