DATA PROTECTION AND THE LAW

qLegal

The small print for BIG IDEAS

A LITTLE BIT ABOUT US

qLegal

The small print for BIG IDEAS

- Public Legal Education Programme
- Legal Advisory Programme
- Legal Projects Programme

Contact us - qLegal (qmul.ac.uk)

Amina Kabiru Turaki: LLM in Comparative and International Dispute Resolution

Rajat Datta: LLM in International Corporate and Commercial Laws

Anjali Karunakaran: LLM in Comparative and International Dispute Resolution

qLegal
The small print for BIG IDEAS

OUR OBJECTIVE TODAY

- Analysis of the GDPR and why it is relevant
- The Marriot case study
- Q&A at the end of the session

qLegal

The small print for BIG IDEAS

WHAT COMES TO YOUR MIND WHEN YOU HEAR DATA PROTECTION?

qLegal
The small print for BIG IDEAS

WHAT IS DATA PROTECTION?

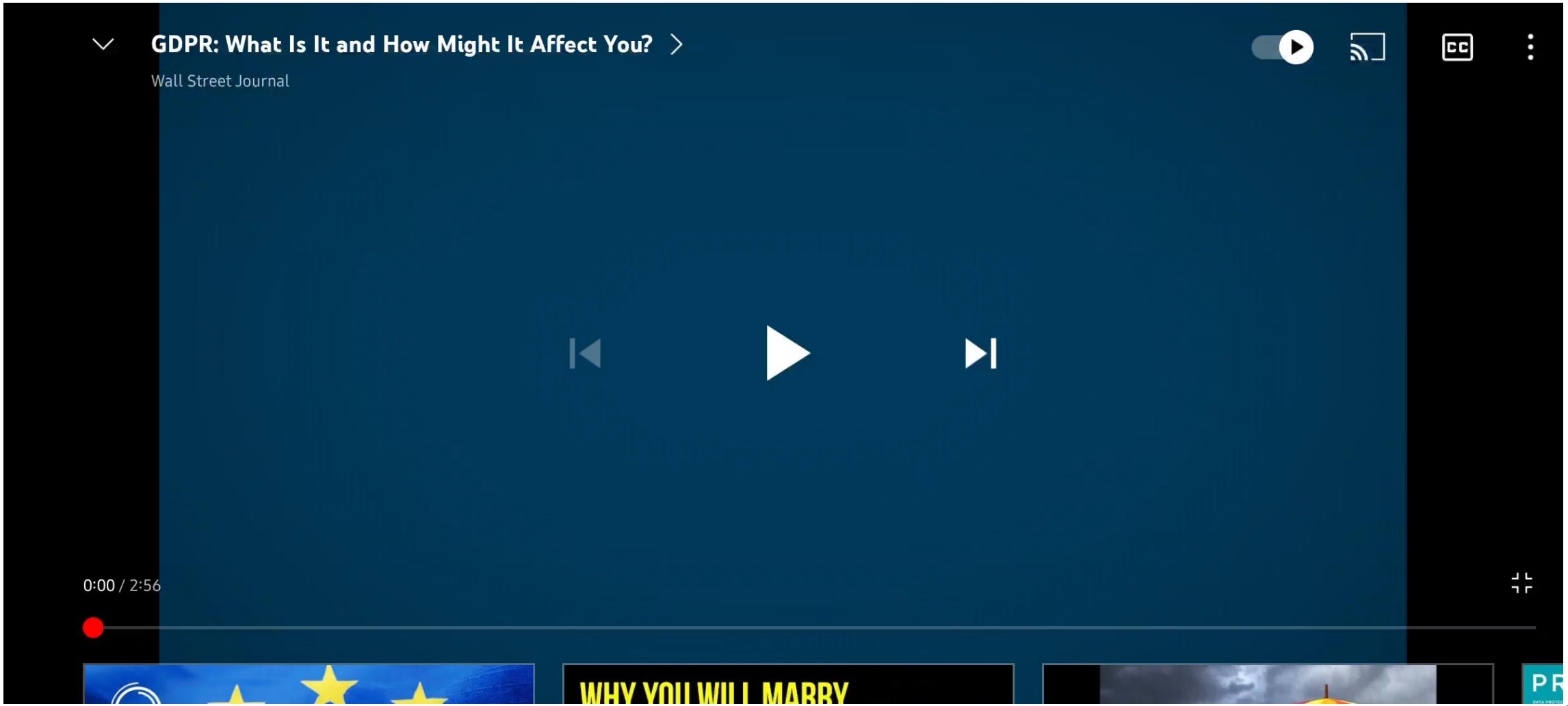
- The relationship between collection and dissemination of personal data and technology
- The legal and political issues surrounding the public expectation of privacy

WHY DOES IT NEED REGULATION?

- To prevent misuse by third parties for fraud, identity theft
- To protect how people's personal data is used by corporations and businesses

qLegal
The small print for BIG IDEAS

GENERAL DATA PROTECTION REGULATION (GDPR)



qLegal
The small print for BIG IDEAS

KEY TERMINOLOGY

Personal Data

Any information relating to identification of a person (for example- name, IP address, home address, biometric data, cultural, social identity markers etc.

Data Subject

An identifiable person who can be identified by reference to their personal data.

Controller

A person or agency which alone or jointly determines the purpose and means of processing personal data.

Processor

A person or agency which processes personal data on behalf of the controller.

Data Protection Officer

Appointed by the controller or processor where processing occurs, operations require monitoring of data on a large scale.

qLegal
The small print for BIG IDEAS

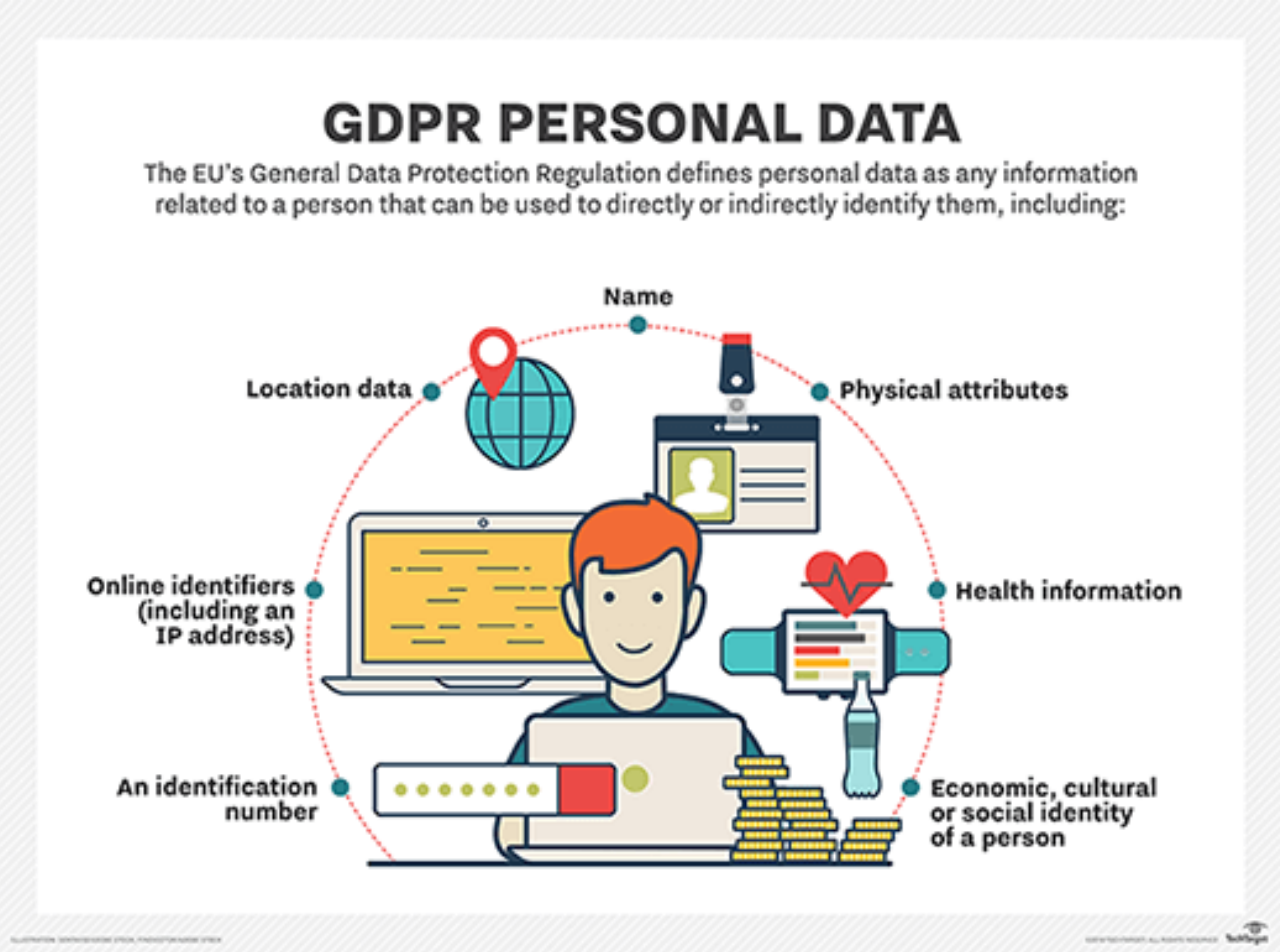
SCENARIOS

1. Meta

2. Law firm

qLegal

The small print for BIG IDEAS



qLegal
The small print for BIG IDEAS

LAWS GOVERNING DATA PROTECTION

Data Protection Act, 2018 (DPA)

- Information that is in use to identify an individual or their personal details
- Data collection doesn't require an opt-in, explicit consent is not needed
- Businesses are under no obligation to report when data breaches occur, even though it is advisable
- Does not stipulate how the governance of data security functions should be allocated, requiring only a basic commitment to the concept from management.
- Current claims only cover material damages

UK General Data Protection Regulation (GDPR)

- Broadens that scope to include online identification markers, location data, genetic information etc.
- Clear privacy notices must be given to consumers – there must be an explicit opt-in option
- Any future breaches have to be reported within 72 hours of the incident
- Designated data protection officer must be appointed if there are more than a stipulated number of employees/profiles processed
- Individuals can claim compensation for material and non-material damage resulting from data security lapses

qLegal
The small print for BIG IDEAS

7 PRINCIPLES UNDER GDPR

Article 5 of the UK GDPR

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimalization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

qLegal

The small print for BIG IDEAS

- [x] Yes
- [ ] No
- [ ] Maybe

HOW DO YOU PREFER TO GIVE CONSENT?

qLegal
The small print for BIG IDEAS

INFORMATION COMMISSIONER'S OFFICE (ICO)

What we've done

Action we've taken to ensure organisations meet their information rights obligations.

Enforcement

See the latest monetary penalties, enforcement notices, undertakings and prosecutions we have issued.

Decision notices

Since 2005 we've ruled on more than 13,500 freedom of information and environmental information cases.

Audits and overview reports

What we've found when visiting and working with organisations.

Monitoring reports

Our monitoring of how long organisations are taking to respond to freedom of information requests.

FOI information notices and practice recommendations →

What's happening now

Find out about our work regarding charity fundraising practices, data security incidents, nuisance messages and cookies.

- Investigation into data analytics for political purposes
- Investigation into data protection compliance in the direct marketing data broking sector
- Timeliness of responses to information access requests by police forces
- Update February 2022: Timeliness of responses to information access requests by police forces in England, Wales and Northern Ireland
- Data security incident trends
- Nuisance calls and messages trends
- Cookie trends
- The ICO's work to recover fines
- Data protection fee non-payment trends report
- Sign up for our action we've taken e-newsletter

qLegal
The small print for BIG IDEAS

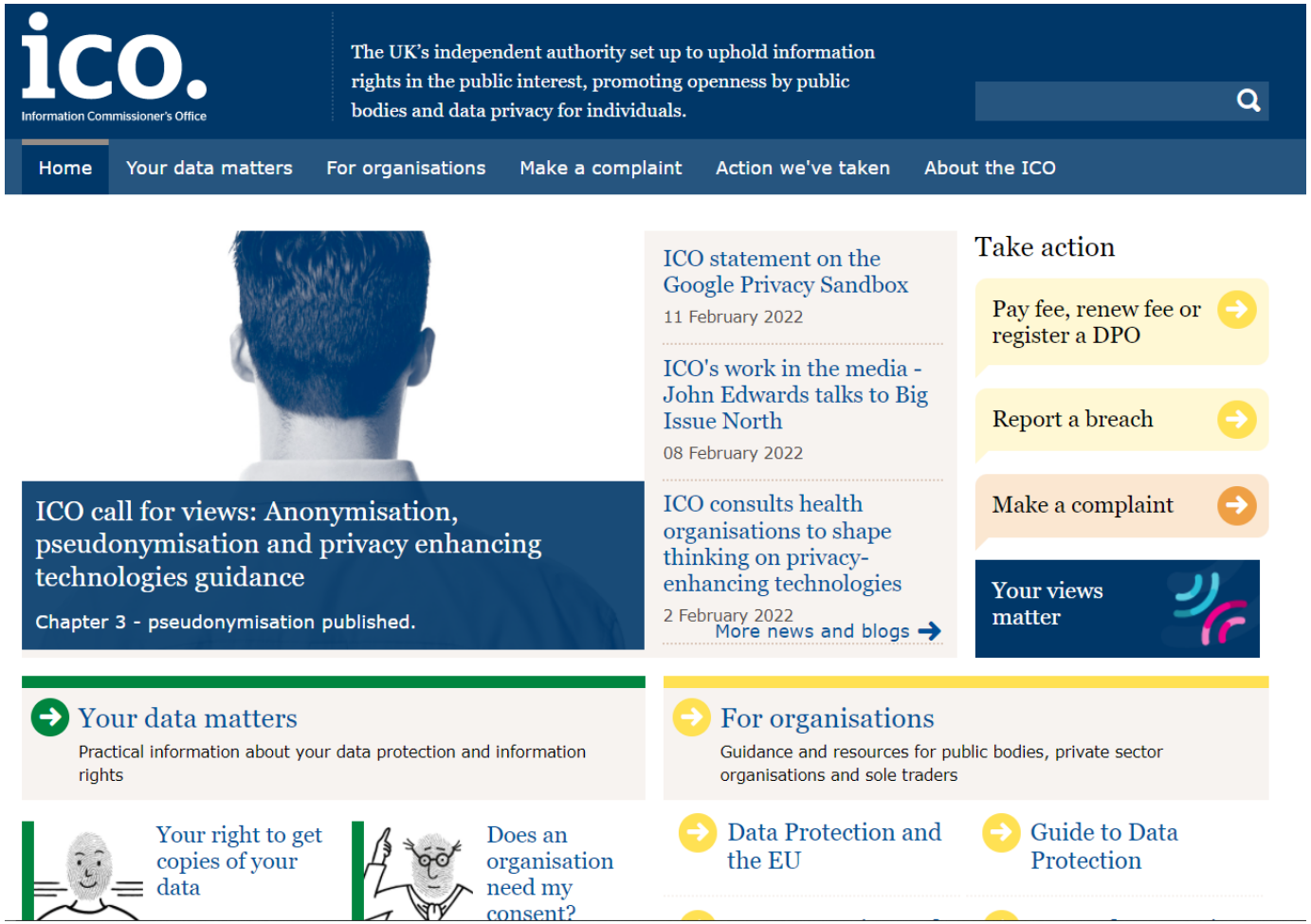
SEQUENCE OF EVENTS

Company notifies ICO of a breach

ICO launches an investigation

ICO issues notice of intent to fine

ICO issues monetary penalty notice



qLegal
The small print for BIG IDEAS

THE MARRIOTT CASE STUDY

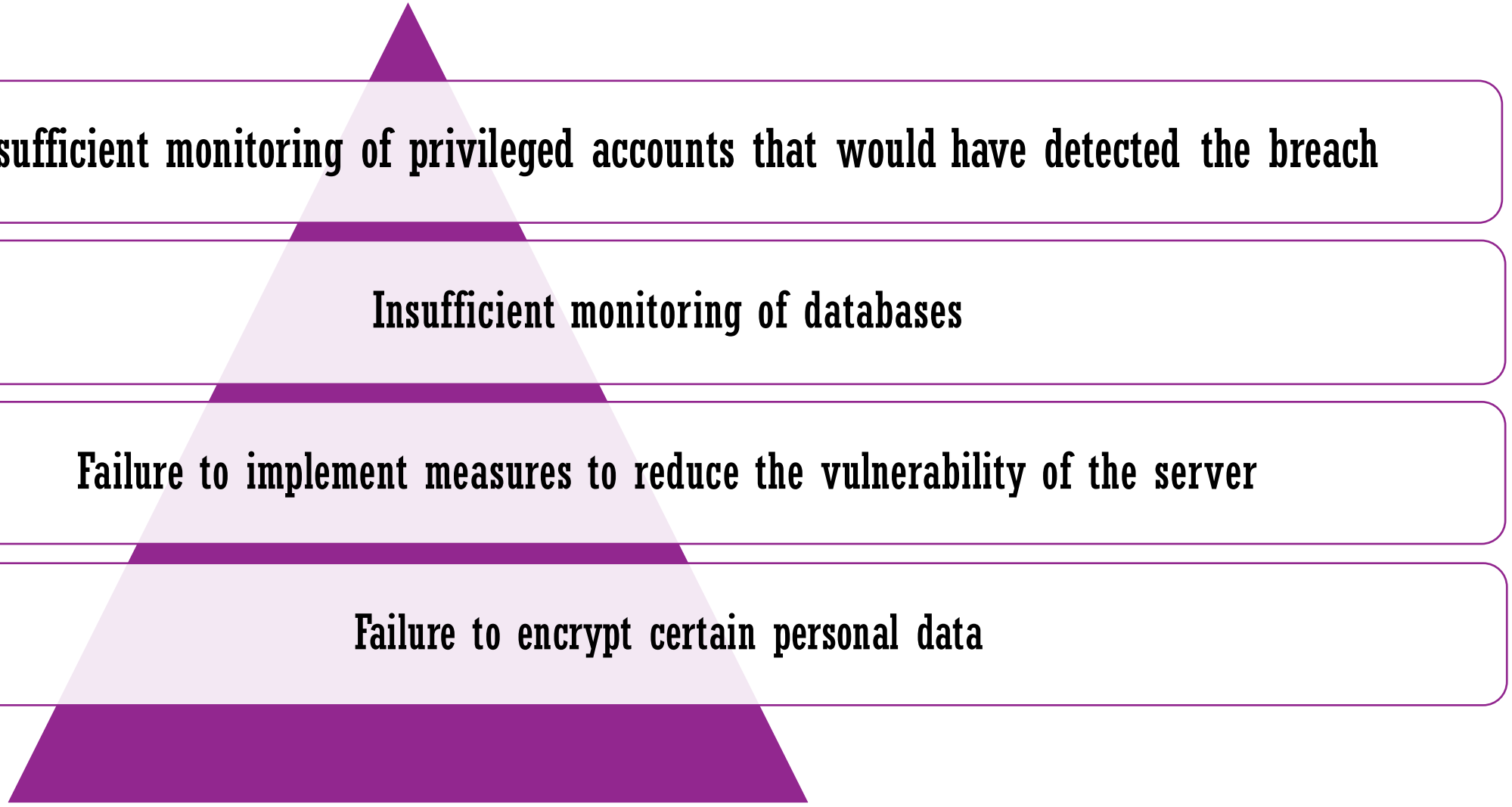
(2014-2020)

FACTS

- An unknown attacker installed code in the Starwood system, giving them remote access to the network
- Personal data of 300+ million in 2018 and ~500 million in 2020 Starwood customers was compromised as a result of this breach
- Information Commissioner's Officer's (ICO) investigation found that Marriott failed to put appropriate technical measures in place as per the GDPR
- ICO issued Marriott with an intent to fine. Total fine amount paid - GBP 18.4 million.

qLegal
The small print for BIG IDEAS

ICO'S FINDINGS ON FAILURES OF MARRIOTT



qLegal
The small print for BIG IDEAS

ICO'S ASSESSMENT OF MITIGATING FACTORS MARRIOTT COULD HAVE TAKEN

- Marriott did not derive any financial benefit from the breach
- The breach was negligent but not intentional
- There was no infringement on Marriott's part, so this was a first offence
- Marriott extended full coorperation to the ICO w.r.t the investigation

qLegal
The small print for BIG IDEAS

THE MARRIOTT CASE STUDY

KEY TAKEAWAYS

- The need for cybersecurity due diligence
- Reminder to review vendor, license, software agreements to ensure that obligations and liabilities of contracting parties is made clear
- Individuals impacted by the breach had locus standi to bring claims – which was typically only the responsibility of the IT vendor who was contracted by Marriott

qLegal

The small print for BIG IDEAS

WHAT CAN YOU DO TO AVOID A DATA BREACH?

qLegal
The small print for BIG IDEAS

BRITISH AIRWAYS CASE STUDY

(2018-2020)

FACTS

- User traffic to BA website was diverted to a fraudulent website where personal data of 400k users was harvested by hackers
- ICO's investigation found that BA had inadequate security measures to prevent such cyber attack
- ICO issued BA with an intent to fine. Total fine amount paid – GBP 20 million.

qLegal
The small print for BIG IDEAS

ICO'S ANALYSIS OF POTENTIAL MEASURES BA COULD HAVE TAKEN

1. Limiting access to applications, data and tools to those required to fulfil a user's role

2. Undertaking rigorous testing, in the form of simulating a cyber attack on the business' systems

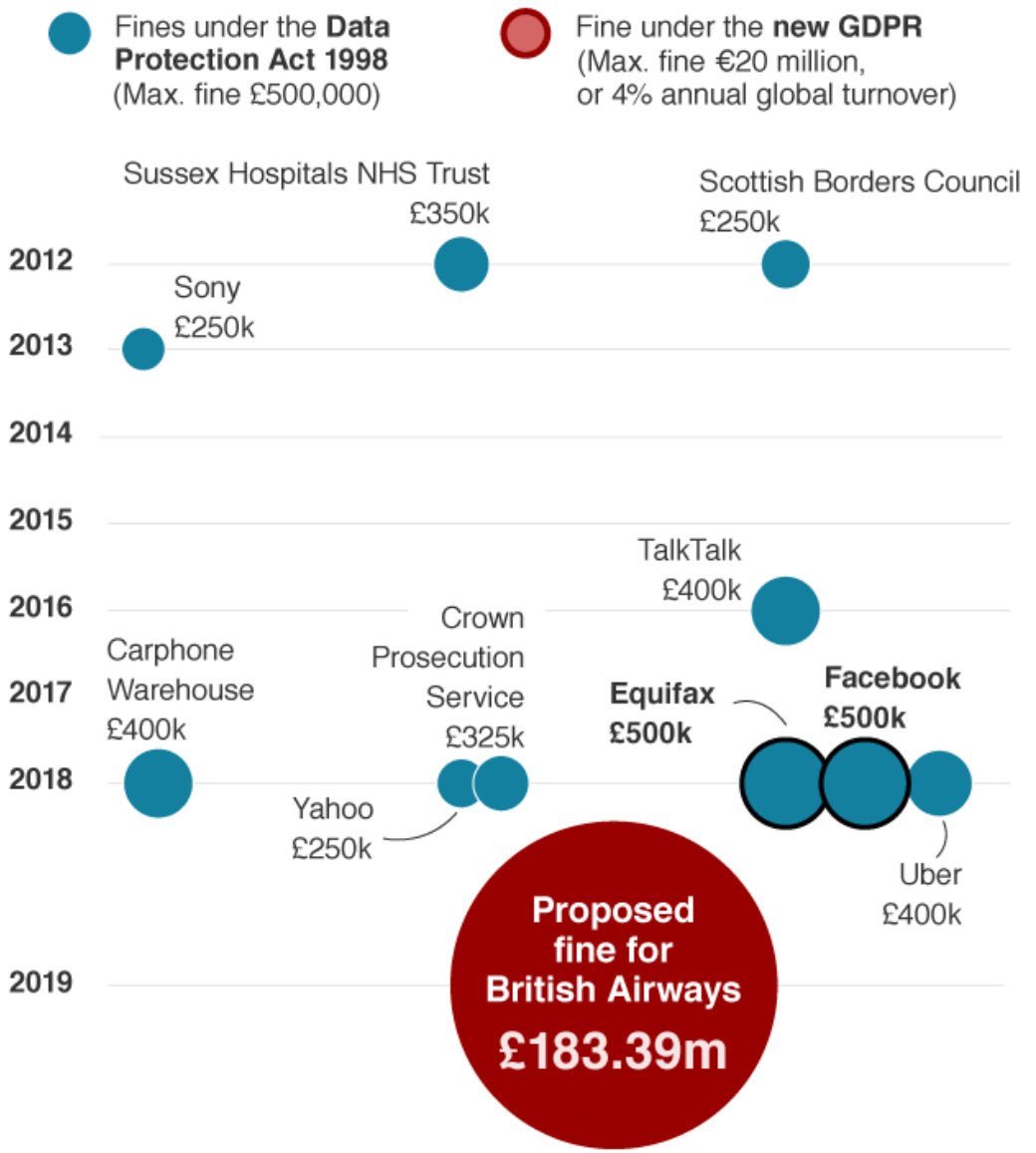
3. Protecting employee and third-party accounts with multi-factor authentication

qLegal

The small print for BIG IDEAS

Biggest fines for data breaches

Fines over £250,000



Source: ICO - Information Commisioner's Office

BBC

qLegal
The small print for BIG IDEAS

COMMONALITY BETWEEN BA AND MARRIOTT CASES

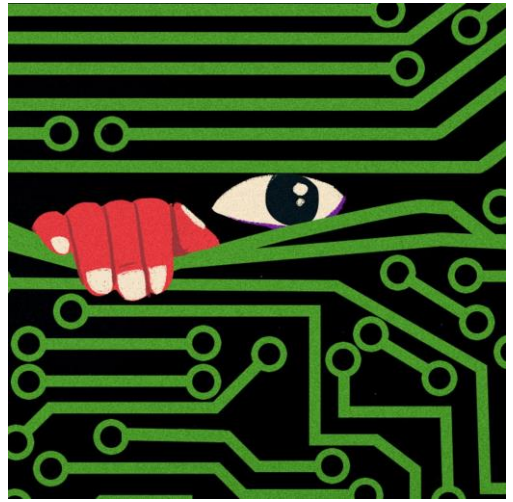
- Breach of security of data was undetected for a prolonged period of time
- Mitigating factors reduced the final fine amounts
  - both companies implemented immediate measures to minimise and mitigate the effects of the attacks
  - both companies cooperated fully with the ICO investigations
  - the broad press coverage of the cyber attacks resulted in both companies suffering significant reputational loss

qLegal

The small print for BIG IDEAS

WHAT CAN WE DO?

(AS DATA PROCESSORS AND CONTROLLERS)



Compliance

- Continuous server and data checks
- Test network security at regular intervals
- Data Protection Impact Assessment (DPIA)
  - Helps organizations identify and minimize risk

qLegal
The small print for BIG IDEAS

WHAT CAN WE DO?

(AS PER THE LAW)

Penalties

- Levy fines as per statutory catalogue of criteria that are proportionate and effective on a case to case basis
- Impose a temporary or definitive limitation such as a ban on data processing

qLegal
The small print for BIG IDEAS

WHAT CAN WE DO?

(AS DATA SUBJECTS)

Know your Rights as data subjects

Articles 15-22 of the UK GDPR

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Notification obligation regarding rectification/erasure of personal data or restriction of processing
- Right to data portability
- Right to object
- Automated individual decision making

qLegal
The small print for BIG IDEAS

Bigger Responsibility, Bigger Repercussions

Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

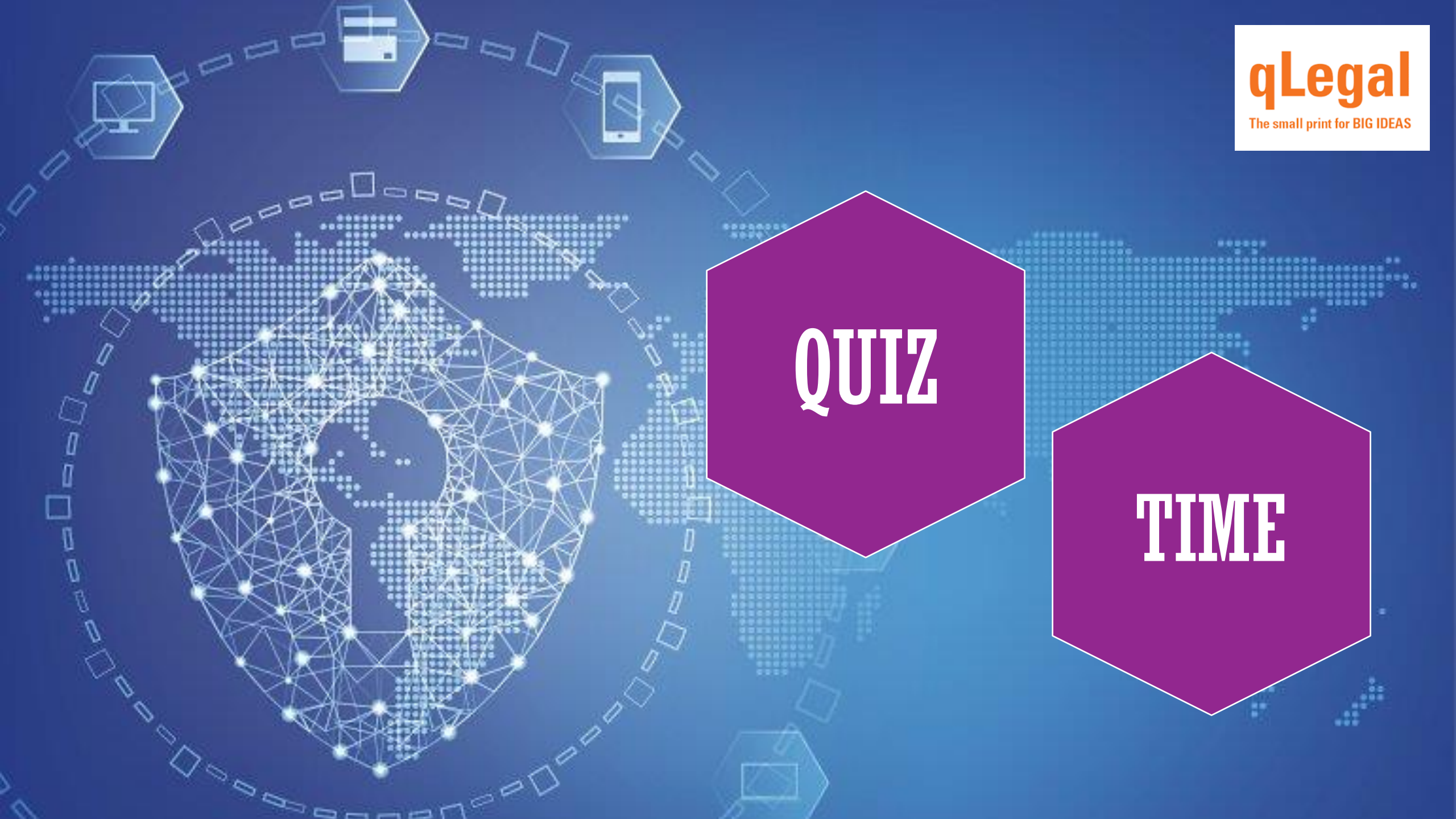
Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to be forgotten
Entitles the data subject to have the data controller erase his/ her personal data (and potentially third parties, too).

Right to access and portability
Users can inquire whether and how their personal data is being processed.

Mandatory data protection officers
Appointed in certain cases, to facilitate the company's need to demonstrate GDPR compliance.


qLegal
The small print for BIG IDEAS
QUIZ
TIME

qLegal

The small print for BIG IDEAS

- Scenario 1: An employee of a company loses their company laptop while commuting from their workplace back home. Should the ICO be notified of such a breach?
- Scenario 2: A courier delivering medication to patients accidentally dropped the medication of patient A to patient B. The personal data of the patients including the name and contact address was on the medication pack. Should the ICO be notified of such a breach?
- Scenario 3: A finance department employee in a Company A sent the file of a new client to a colleague in a different department. There was a hack in the system and only the details of the new client were released. Should the ICO be notified of such a breach?

qLegal
The small print for BIG IDEAS

CONCLUSION

- With the advent of technology and the internet, transfer of data has become very efficient. Therefore, data protection laws must keep pace.
- The internet is not only used to disseminate information, but it is also a source for its collection.
- Organizations must pay attention to how they collect, store and process the personal data from data subjects. There is a need to constantly update marketing practices and internal training mechanisms.

CONTACT US

http://www.qlegal.qmul.ac.uk/contact

@qLegal_

@QMqLegal

https://www.linkedin.com/company/qlegal

qLegal@qmul.ac.uk