CYBERROADSHOW

An Overview of GDPR

QA

Why Do We Need Data Protection?

- Impact on data subjects
- Legal requirement
- Best practice
- Reputational risk
- Financial risk
- Organisational risk

CYBERROADSHOW

Current Data Protection Principles

1. Fairly & Lawfully Processed
2. Processed for Limited Purposes
3. Adequate, Relevant & Not Excessive
4. Accurate & Up To Date
5. Not Kept Longer Than Necessary
6. Processed In Line With Subject Rights
7. Kept Secure
8. Not Transferred Overseas Without Adequate Protection

QA

So Why Change?

- Inconsistent across Member States
- Rapidly changing technologies – CCTV, Big Data etc.
- Outdated legislation
- Court rulings on privacy and data protection in the US
- No mandatory requirement to report breaches
- Increased rights for data subjects to protect rights and freedoms
- Simplification of administration – Single National Authorities

BREXIT

- The ICO made a formal comment after the Brexit referendum that reform of data protection laws remain necessary
- The government confirmed on 31st October 2016 that GDPR will be implemented:

  "We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public" Karen Bradley, MP

- This position was confirmed by Digital Minister Matt Hancock in the Triennial review of the ICO

Brexit Myths?

- A survey of IT decision makers at UK companies by information management firm Crown Records Management has found 24% are no longer preparing for the regulation.
- A further 4% have not even begun to prepare.
- “Alarmingly, a massive 44% of those surveyed said they didn’t think the regulation will apply to UK business after Brexit.”

What Does The GDPR Cover?

- Extends scope
- Standardises definitions
- Extends data subjects rights
- Clarifies obligations for controllers and processors
- Strengthens enforcement regime
- Designed to address online privacy and profiling
- “Future proof” legislation for changing technology
- Introduces online personal data and privacy requirements

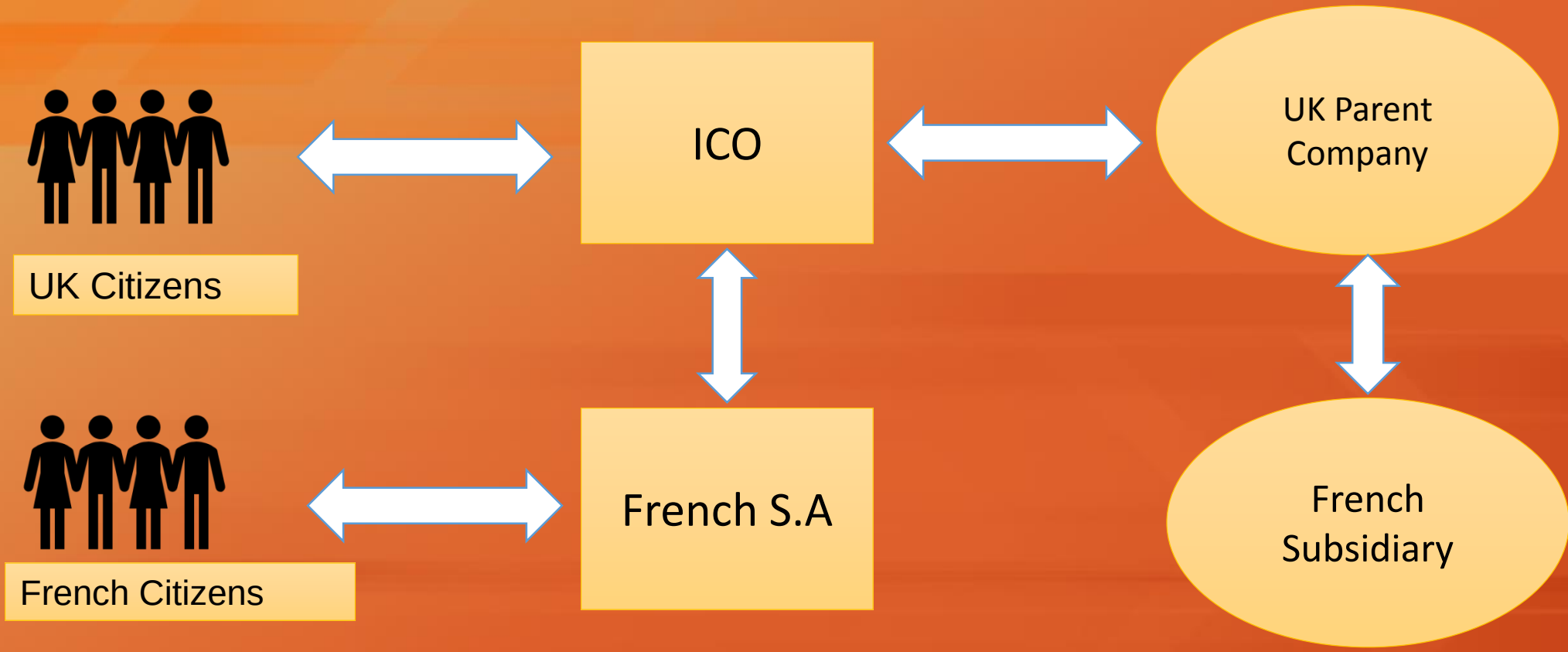
CYBERROADSHOW

Summary Of Changes

Standardised definitions	Right to data portability	Privacy by design & default
Explicit consent required	Risk based security implemented	Liability of controller and processor clearer
Data retention period required	Mandated reporting within 72 hours	Must respond to SARs within a month
Right to be forgotten	Main establishment	Mandated records required
Right to restricted processing	Enforcement regime	Appointment of a DPO
Right to object enhanced	Extended territorial scope	Obligation to notify when buying data in
Right to withdraw consent	Impacts consent and online profiling	Defines safeguards for 3rd countries

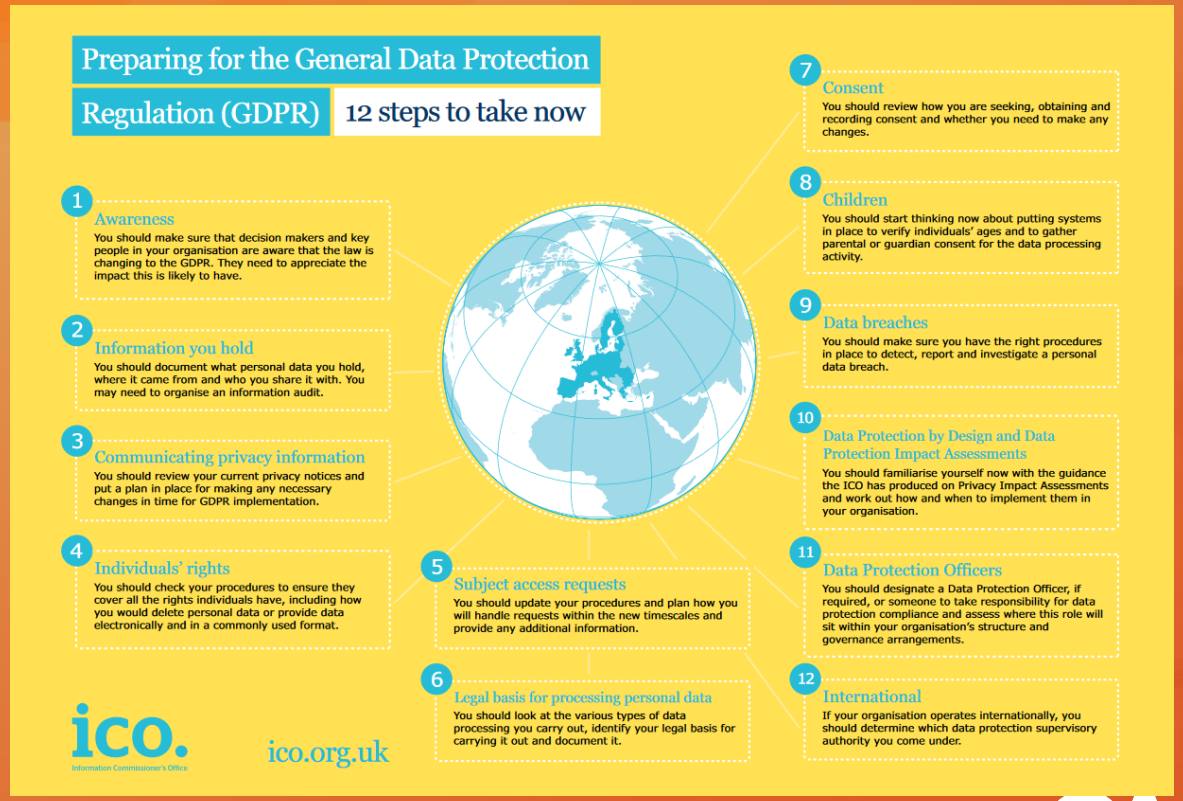
QA

Cooperation & One Stop Shop



CYBERROADSHOW

Preparing For The Changes



QA

Governance Frameworks

- ISO 27000 series – Information security standards
- ISO38500 – Corporate Governance of IT
- NIST SP 800 series – US government information security requirements
- BS10012 – Data protection: specification for a personal information management system
- COBIT – Control objectives for information and related technologies
- Privacy Management framework – implemented by the Australian Information Commissioner

Information Assurance & Accreditation

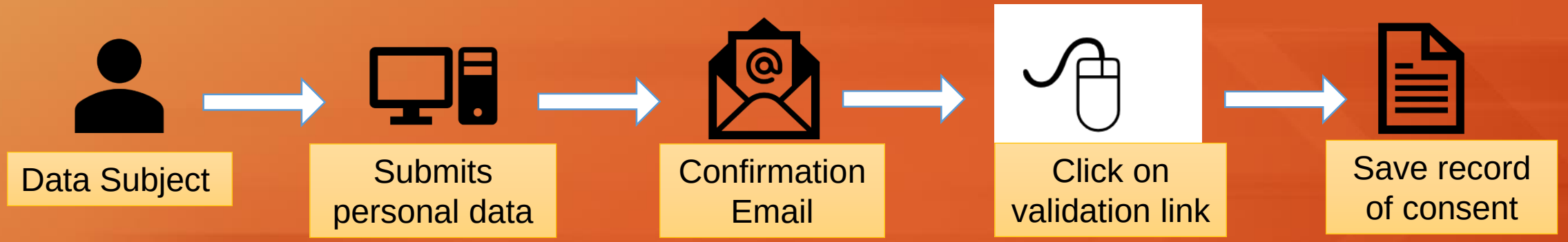
- Organisations will implement security controls based on a risk managed approach
- Based on an assumption of mitigation of risk & effectiveness of controls
- Assurance process provides confidence that risk is managed and controls are effective
- Accreditation is an independent function which provides the organisation with the necessary assurance

Be Careful With Consent!

- An organisation **MUST** be extremely careful when & how they clarify the consent they hold
- Fines will be imposed if there is a breach of the PECR
- In March 2017 the ICO issued the following fines:
  - Flybe - £70,000
  - Honda - £13,000
- ICO position: "Businesses must understand they can't break one law to get ready for another"

Double Opt-In

- It is not a double negative!
- Ensures consent is explicit & an unequivocable affirmative act
- Ensures a clear record of what was consented to & when
- Single opt in may not be sufficient proof of consent



Getting It Wrong...

Under GDPR:

- 2016 total fines of £880,500 would increase to £69 million
- Talk Talks fine would be £59 million instead of £400,000
- Pharmacy2U would be fined £4.4 million instead of £130,000