The NIS Regulations for RDSPs And other indecipherable acronyms

Jon Langley
Senior Technology Officer (Technology Policy)

ico.
Information Commissioner's Office

What we’ll be covering

- What is NIS, and what is it for
- The ICO’s regulatory function under NIS
- Who’s covered – and who isn’t
- How NIS is being regulated – enforcement, penalties, etc.
- Digital services and security requirements
- How NIS and the GDPR overlap – and inter-relate
- Available guidance
- Resources

CA

SaaS ICO

NCSC OES

RDSP **NIS** SPOC

IaaS CSIRT GCHQ PaaS

Each one is in this presentation somewhere!

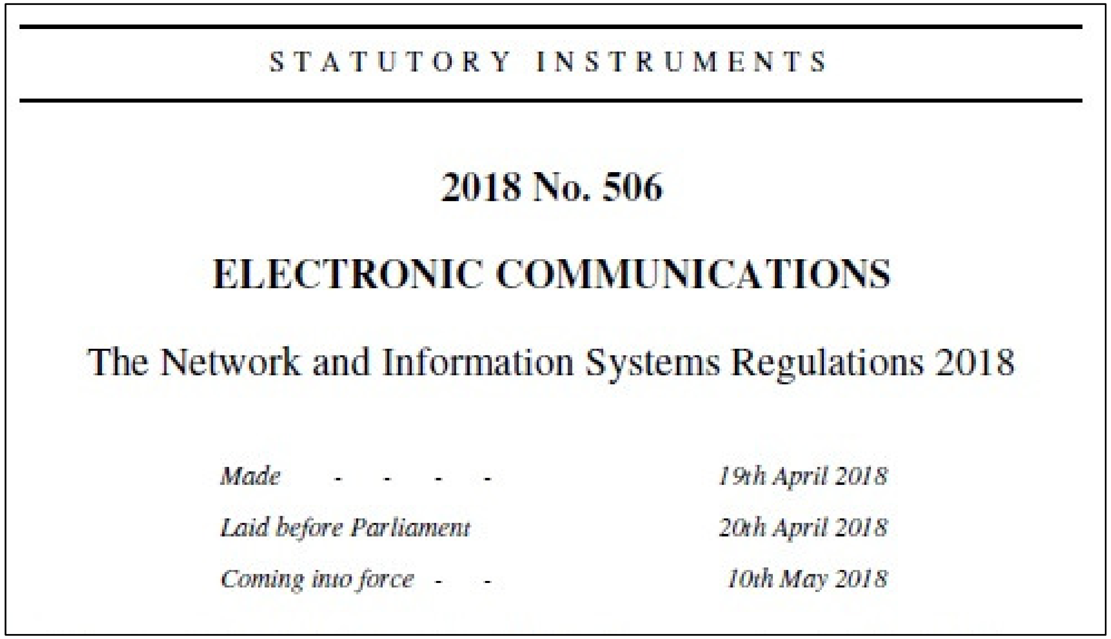
What is NIS?

NIS Directive – originating EU law

Network and Information Systems (NIS) Directive
EU 2016/1148

- Key dates:
  - Finalised: 6 July 2016
  - Implementation: 10 May 2018
- Brexit?
  - Required to transpose
  - UK Government: NIS will continue to apply post-Brexit

NIS Regulations - UK implementing law



STATUTORY INSTRUMENTS

2018 No. 506

ELECTRONIC COMMUNICATIONS

The Network and Information Systems Regulations 2018

Made - - - -	*19th April 2018*
Laid before Parliament	*20th April 2018*
Coming into force - -	*10th May 2018*

- Key date:
  - In force: 10 May 2018
- Part of the delivery of the UK’s National Cybersecurity Strategy 2016-2021
  - A requirement of the NIS Directive

What’s it for?

- Three goals:
  - Address threats posed to essential services
  - Ensure smooth running of the EU’s internal market
  - Protect customers and businesses

- Is it a cybersecurity law?
  - Not entirely, but most of it concerns cybersecurity
  - However it concerns *physical* and *environmental* factors too
    - Including the weather!

Purposes of NIS

What are “network and information systems”?

- Three definitions:

  a) “Electronic communications networks”

  b) Devices, or groups of connected devices, which perform “automatic processing of digital data”

  c) “Digital data” stored, processed, retrieved or transmitted by either of the above “for the purposes of their operation, use, protection and maintenance”

- BUT: Only in the sectors specified in the Directive!

Network and information systems

Who’s covered?

Services that are essential for the functioning of the economy and wider society

Operators of essential services (OES)

Relevant digital service providers (RDSPs)

Online search engines…

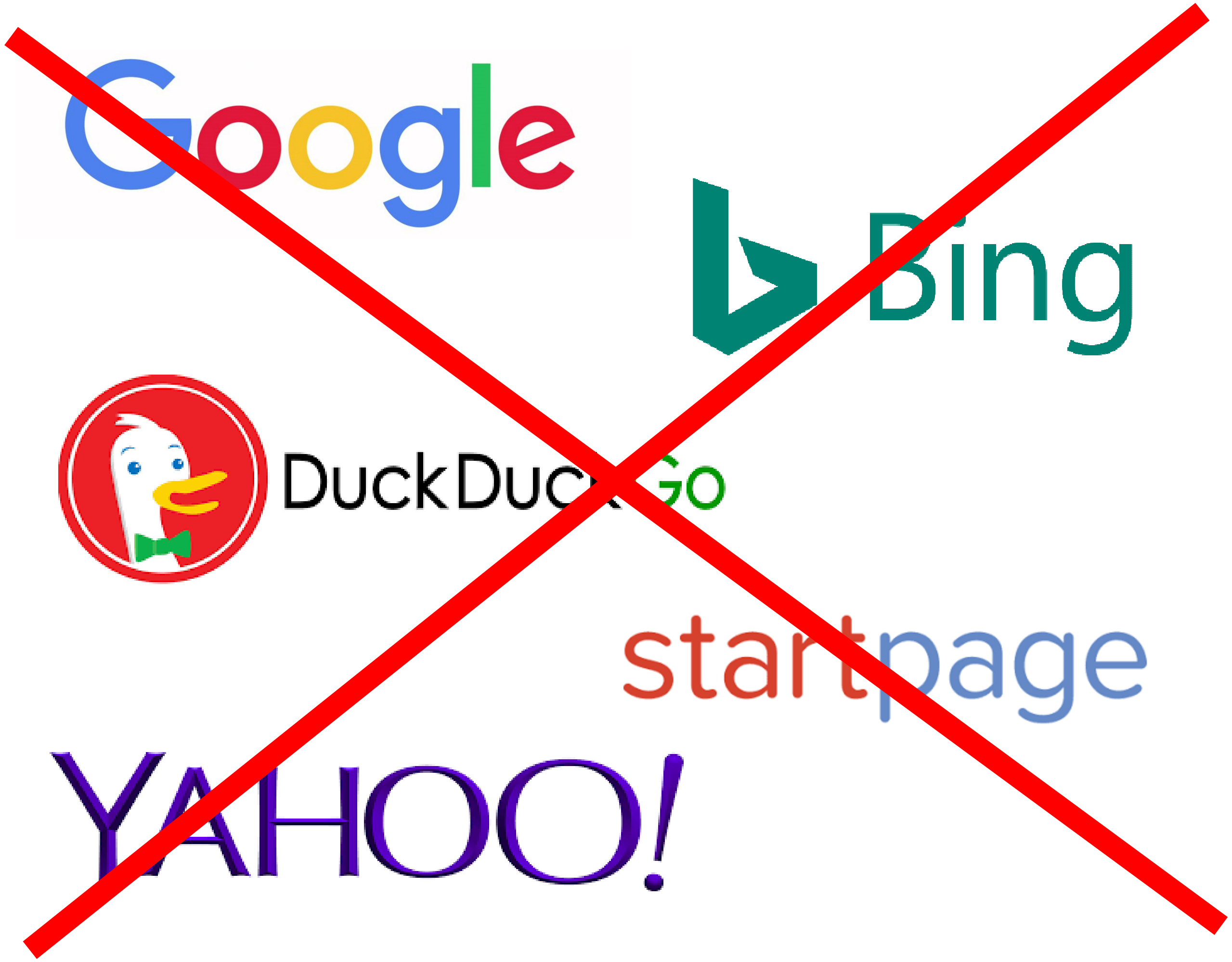
Online marketplaces…

Cloud computing services…

…with a UK head office or nominated representative

- “a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found”

Online search engines – Regulation 1(2)



- Number of UK-based online search engines?

0

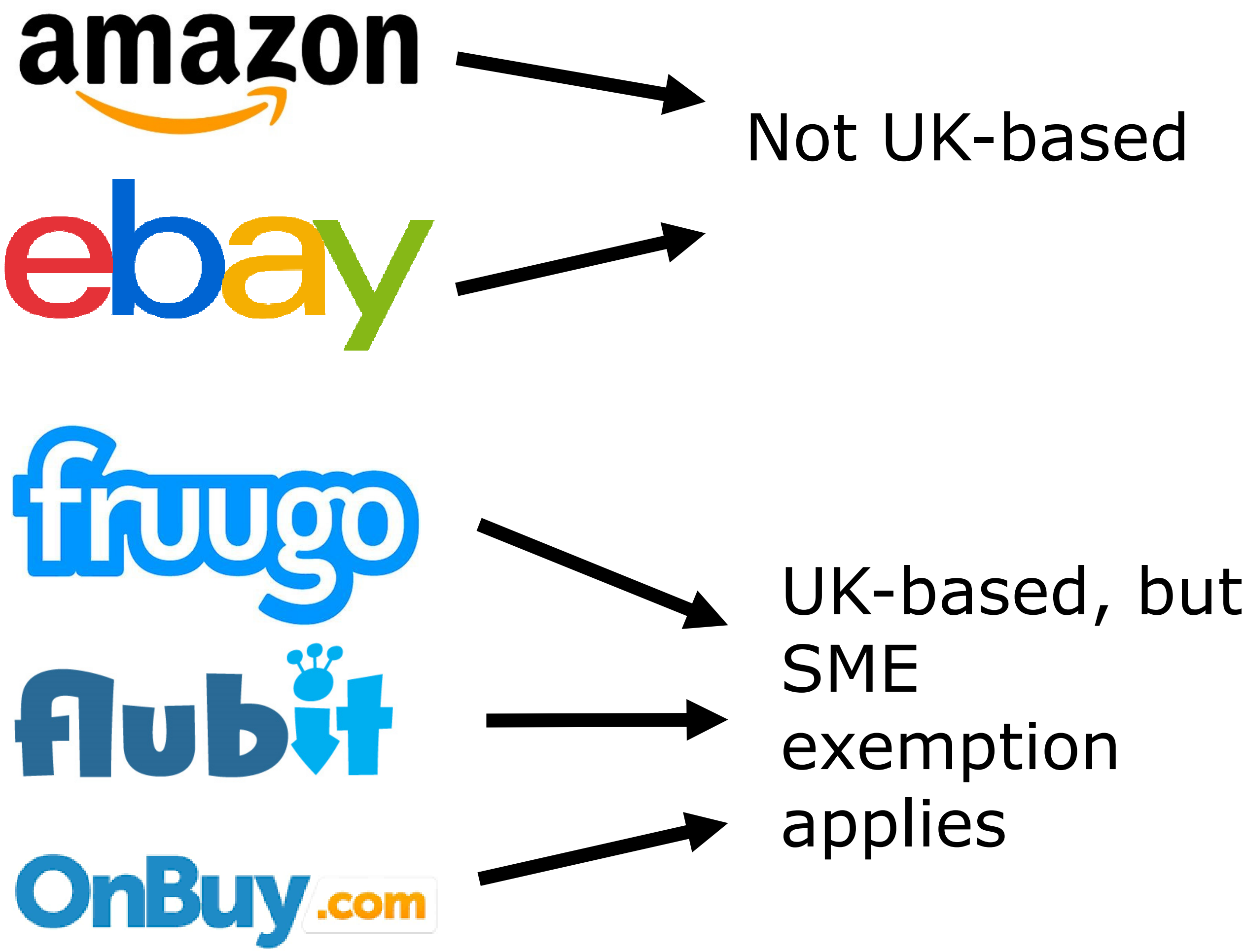
Source: DCMS

Examples?

Online marketplaces – Regulation 1(2)

- “a digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace’s website or on a trader’s website that uses computing services provided by the online marketplace”

Examples?



Not UK-based

UK-based, but SME exemption applies

- Total number of UK-based online marketplaces:

2

Source: DCMS

Cloud computing services – Reg 1(2)

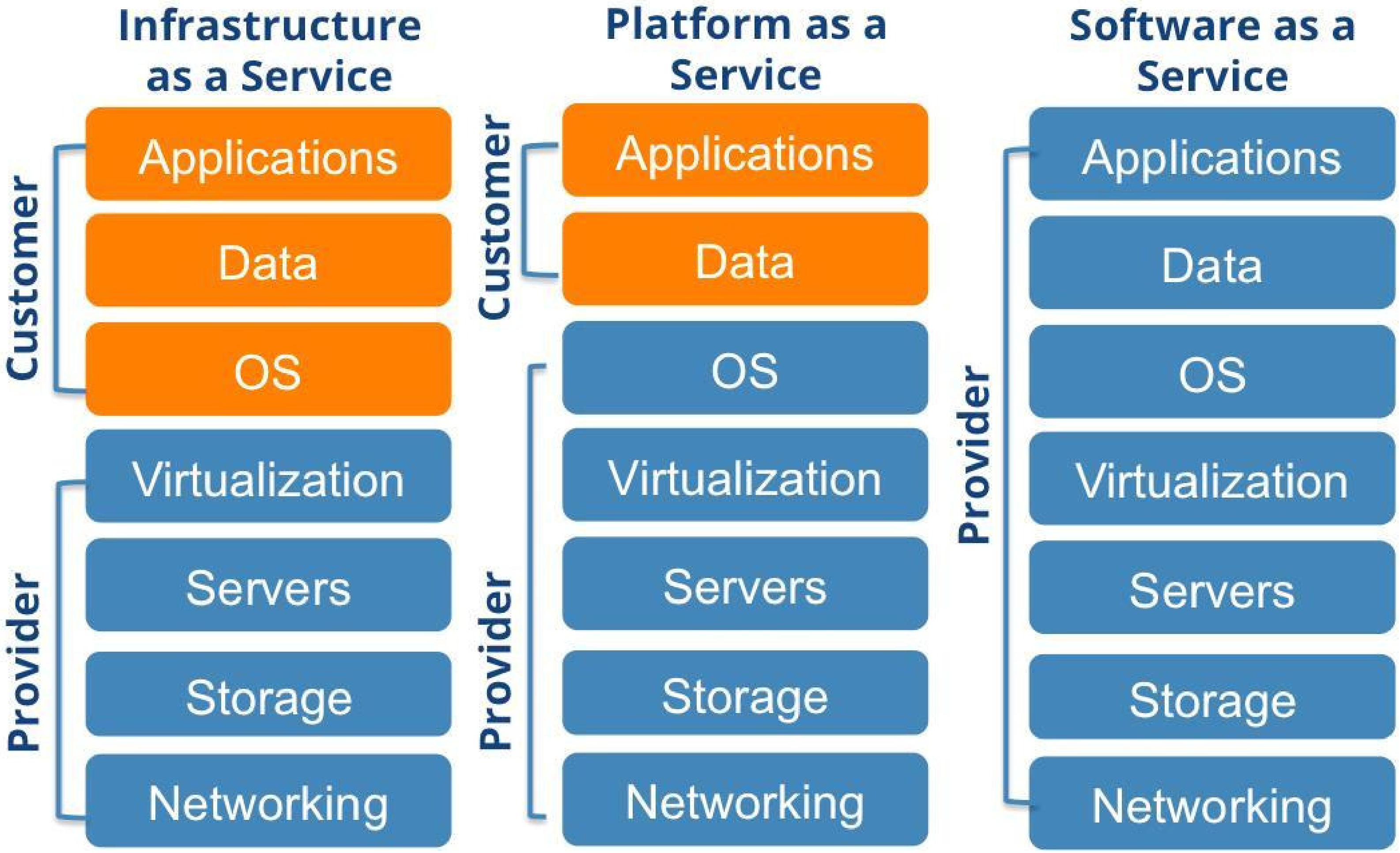
- “a digital service that enables access to a scalable and elastic pool of shareable computing resources”

- **Estimated** number of UK-based cloud computing services:

c. 200

Source: DCMS – but we are checking!

Examples?



Infrastructure as a Service

Customer

- Applications
- Data
- OS

Provider

- Virtualization
- Servers
- Storage
- Networking

Platform as a Service

Customer

- Applications
- Data

Provider

- OS
- Virtualization
- Servers
- Storage
- Networking

Software as a Service

Provider

- Applications
- Data
- OS
- Virtualization
- Servers
- Storage
- Networking

NIS covers the **providers**, not the **customers**

Cloud computing service models

- Micro and small enterprises are **not covered**

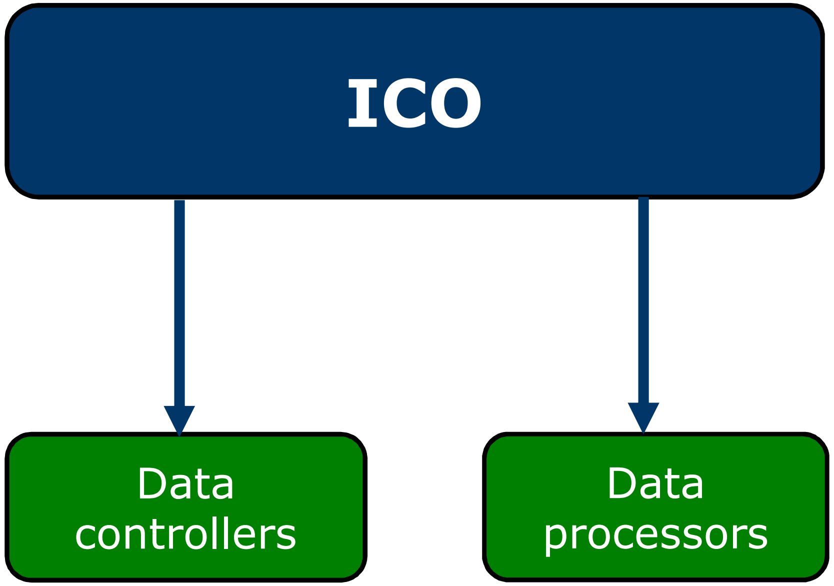
- Organisations with:
  - Fewer than 50 staff AND
  - Turnover or balance sheet of less than €10m

- Commission Recommendation 2003/361/EC
  - Defines SMEs for purposes of EU law
  - Used in the NIS Directive and reflected in UK NIS Regs

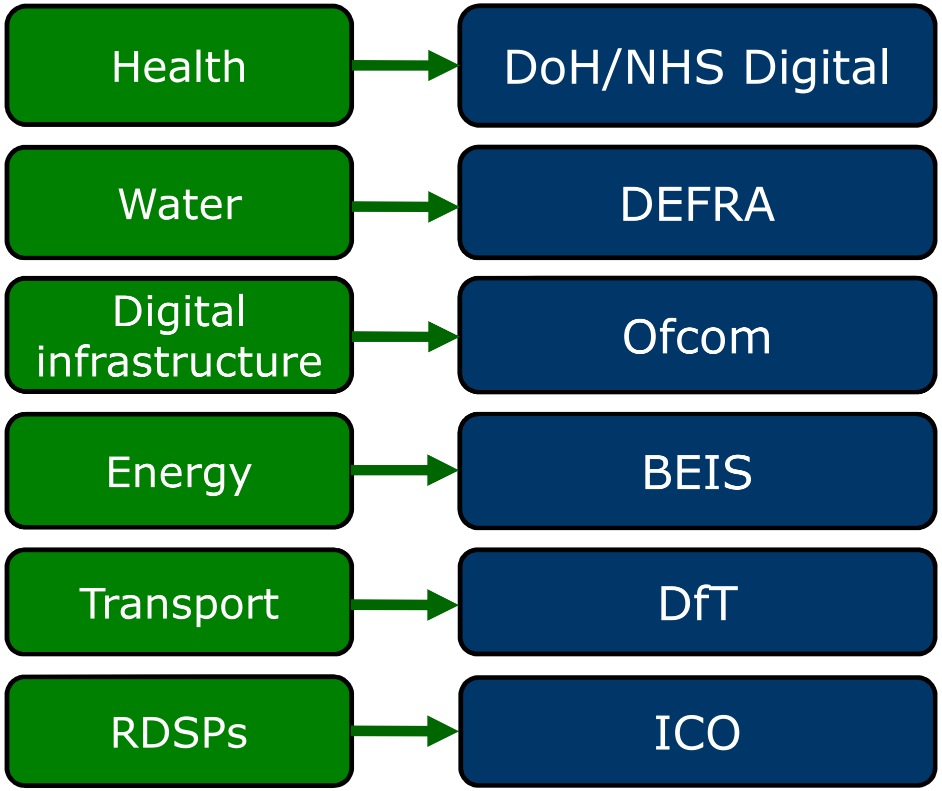
SME carve-out – Regulation 1(3)(e)(ii)

Multi-regulator model

GDPR: one 'Supervisory Authority' (to rule them all)



NIS: multiple 'Competent Authorities'



Health → DoH/NHS Digital

Water → DEFRA

Digital infrastructure → Ofcom

Energy → BEIS

Transport → DfT

RDSPs → ICO

SPOC and CSIRT

Single Point of Contact

- Single point of contact on security of network & information systems
- Liaison with other authorities in cross-border incidents

Computer Security Incident Response Team

- Monitor incidents at national level
- Provide early warning, alerts, etc.
- Incident response
- Risk analysis
- Incident notification & communication to CAs

What are RDSPs required to do?

Security measures

Incident notification

Registration

- “Identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems”

- “Prevent and minimise the impact of incidents”

- Ensure the measures cover:
  - security of systems and facilities, incident handling, business continuity, monitoring, auditing, testing, and compliance with international standards…

Security requirements – Reg 12 (1) & (2)

Incident reporting – Reg 12(3) to (7)

- RDSPs to notify the ICO of incidents that have:
  - "a substantial impact on the provision" of their service(s).
- Notification:
  - "Without undue delay" and "no later than 72 hours" after awareness of the incident
  - Include information on time, duration, nature and impact
  - **RDSPs must assess incidents themselves**
  - Only required to notify if they have access to information to allow the assessment

Commission Implementing Regulation on digital service providers
EU 2018/151

- Key info:
  - Finalised: 30 January 2018
  - Applied: 10 May 2018
  - Has **direct effect**

- Specifies:
  - Security elements (Article 2)
  - Parameters for incident assessment (Article 3)
  - Thresholds for determining the impact of an incident (Article 4)

The “DSP Regulation”

- Regulation 12(2)(c) – when implementing their measures, RDSPs must:
  - Take account of **Article 2** (security elements)

- Regulation 12(7)(a) and (b) – when assessing if an incident has a substantial impact, RDSPs must:
  - Take account of the parameters in **Article 3**
  - Assess whether any of the “situations” in **Article 4** apply
    - These are numerical thresholds

What are the parameters?

- The parameters:
  - Number of users affected
  - Duration of the incident
  - Geographical area affected (number of Member States)
  - Extent of disruption to the service
  - Extent of the impact on economic & societal activities

- Article 3 provides further information on each
  - For example, meaning of “duration of the incident”

What are the “situations”?

- Article 4 – numerical thresholds for when an impact is considered “substantial”
  - Service unavailable for more than **5m** “user-hours”
  - Incident results in a loss of integrity, authenticity or confidentiality of data or related services, and the loss affects more than **100,000 users** in the Union
  - Incident creates a **risk** to public safety, security or life
  - Incident causes **material damage** to at least **one** user of more than **€1m**

- At least one must occur.

What are the ICO’s functions as a Competent Authority?

Incident notification and investigations

Enforcement powers (and penalties)

International co-operation

And maintain the RDSP register…

- The ICO will:
  - Receive notifications and investigate cases
    - With follow-up action where necessary
  - Share notifications with the NCSC
  - Inform “relevant authorities” in other Member States
  - Inform the public (in certain circumstances)
  - Make annual reports to the NCSC

Incident notifications – Reg 12

- Range of powers available:
  - Information Notices
  - Powers of inspection
  - Enforcement Notices
  - Penalties

Our functions are funded by grant-in-aid for 2 years and then **cost recovery**

- These are:
  - **Separate** from GDPR/DPA 2018 powers
  - All **post-incident** upon incident notification or concerns raised – contrast with OES CAs

Enforcement powers – Regs 15, 16, 17 and 18

Four tiers of fines – Reg 18

- Up to:
  - **£1,000,000** – for "any contravention" which "could not cause an incident".
  - **£3,400,000** – for "material contraventions" that cause incidents which lead to "reduction of service provision"
  - **£8,500,000** – for "material contraventions" that cause incidents which lead to "disruption of service provision"
  - **£17,000,000** – for incidents leading to "an immediate threat to life" or "significant adverse impact" on the economy

International co-operation – Reg 13

- ICO to co-operate and assist CAs in other Member States where:
  - RDSPs have systems in another state
  - Digital services located in another state have systems in the UK

- Includes:
  - Sharing information with other CAs
  - Making requests for enforcement action
  - Receiving requests for enforcement action

Overlap between NIS and GDPR

- Where an OES or a DSP is a data controller they still have to comply with the GDPR **irrespective** of NIS obligations
- Where an RDSP is also a data processor it still has to comply with the GDPR **irrespective** of NIS obligations
- Security requirements are very similar – just more specific for RDSPs
- DCMS original policy intent: Align NIS with GDPR as far as possible
  - Not quite – but the same 72 hour notification window
- But, more obviously…

GDPR Article 4(12) – "Personal data breach"

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

NIS Regulations – Regulation 1(2) – "incident"

'Any event having an actual adverse effect on the security of network and information systems.'

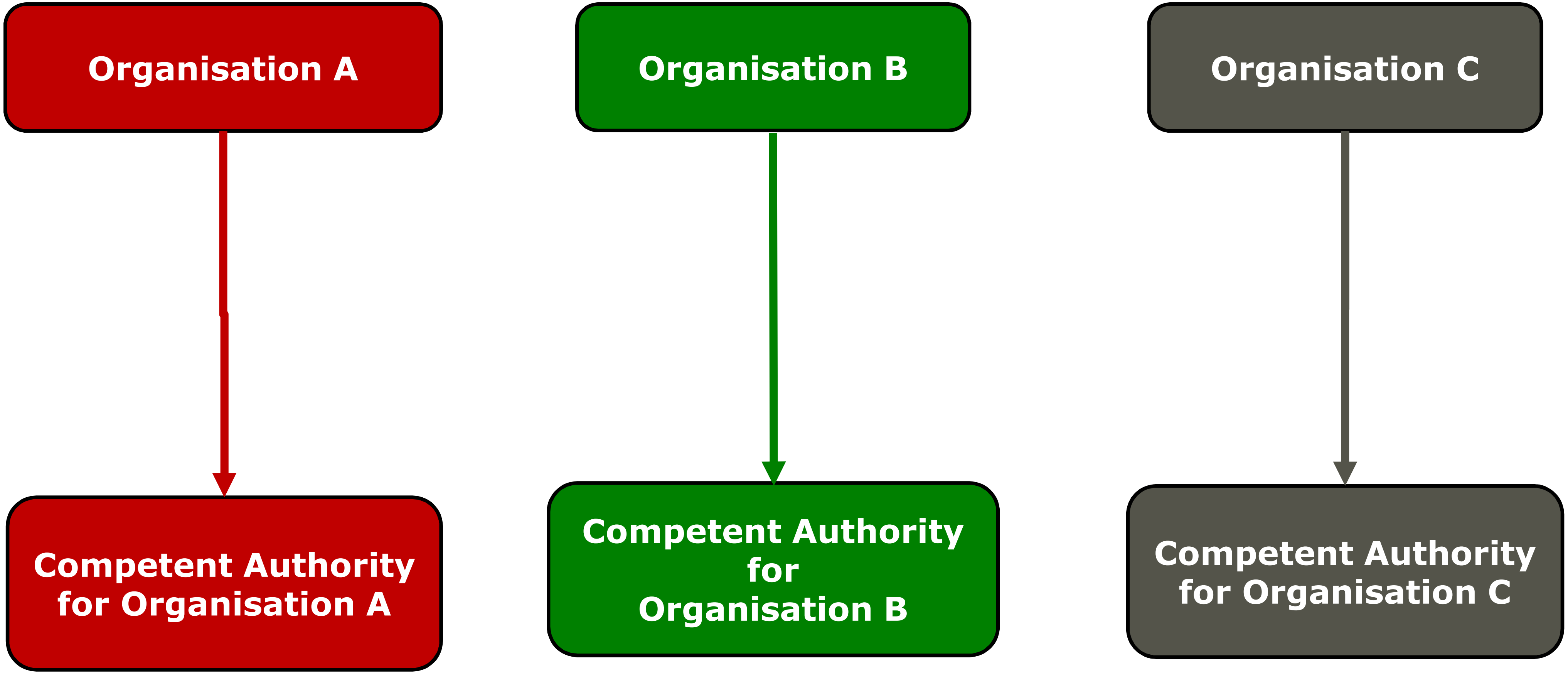
A NIS incident may be, or may lead to, a GDPR personal data breach…

What happens with OES incidents?

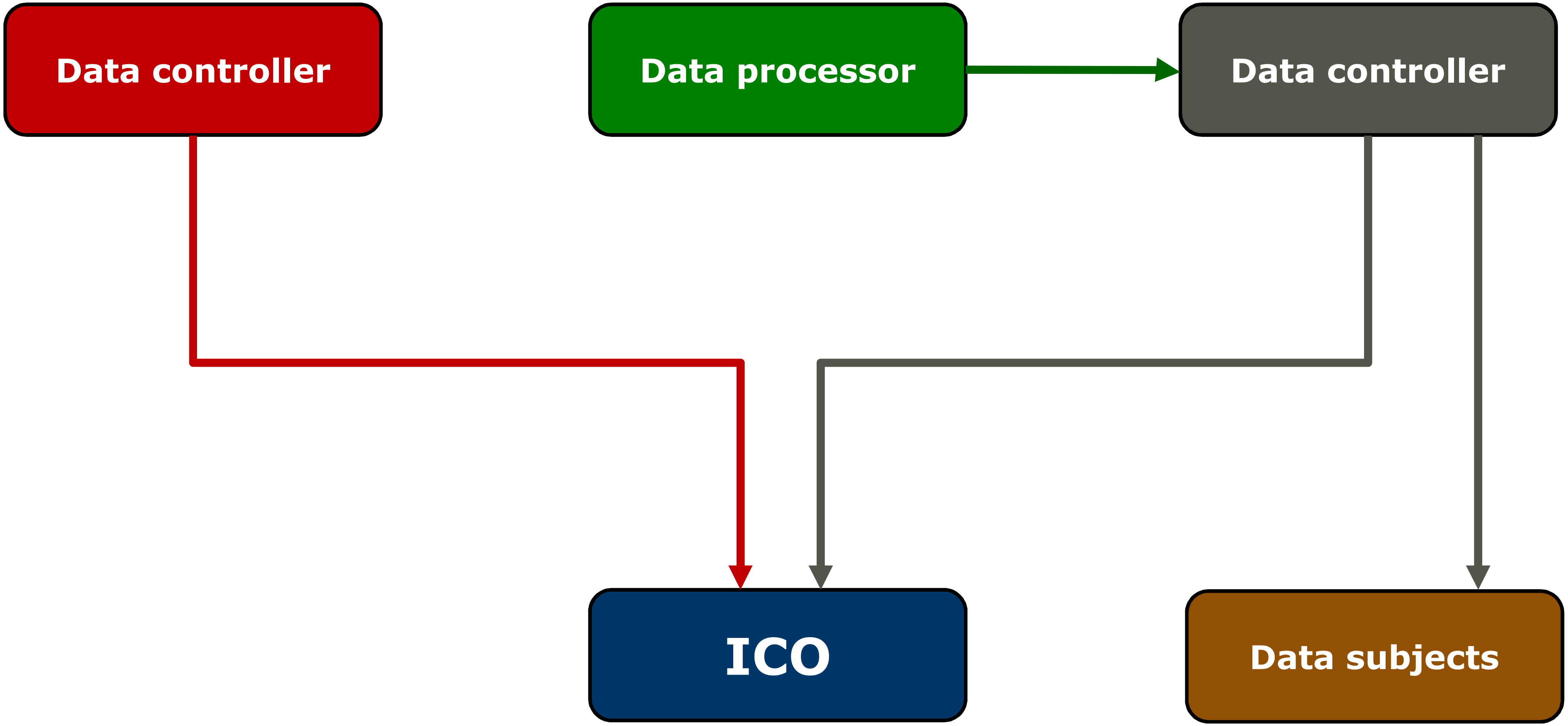
- The OES has to notify us **anyway** if it’s a Personal Data Breach

- But: Regulation 3(3)(f) - the OES’s competent authority must also:
  - ‘Consult and co-operate with the Information Commissioner when addressing incidents that result in breaches of personal data’

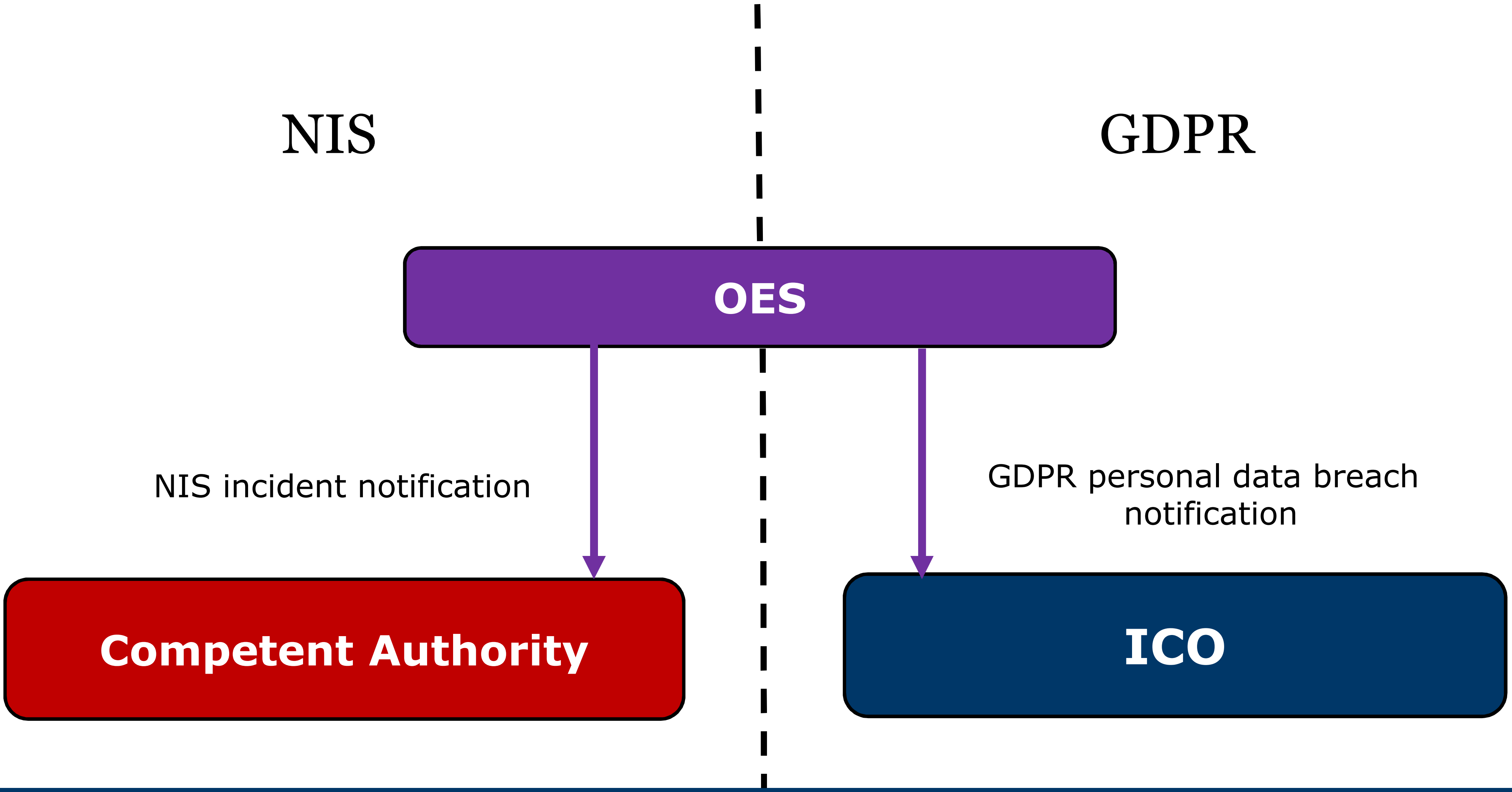
- Reflects Article 15(4) of the Directive
  - Added by the ICO during the SI drafting process…


Organisation A
Organisation B
Organisation C
Competent Authority for Organisation A
Competent Authority for Organisation B
Competent Authority for Organisation C

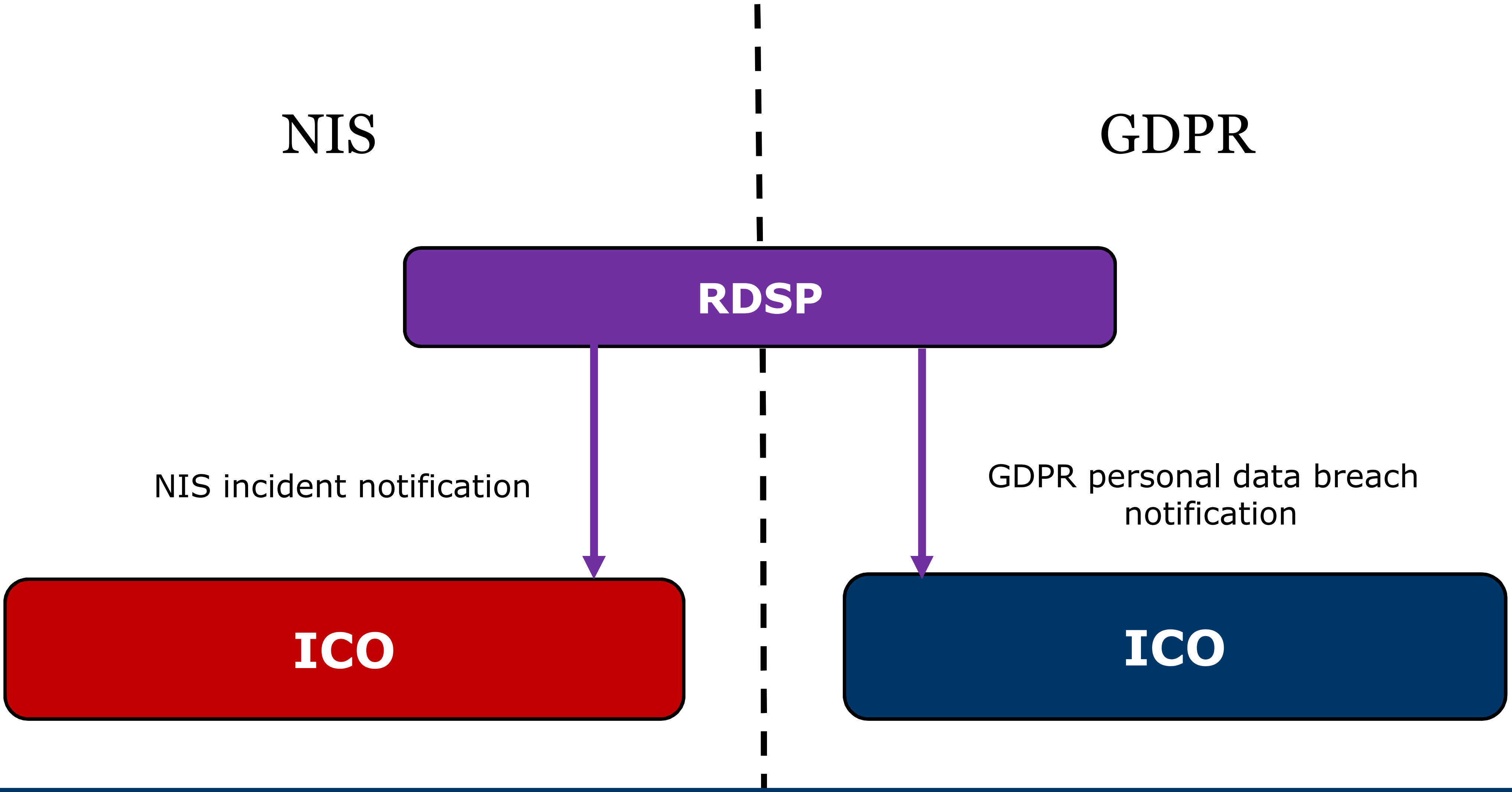
Incident notification under NIS



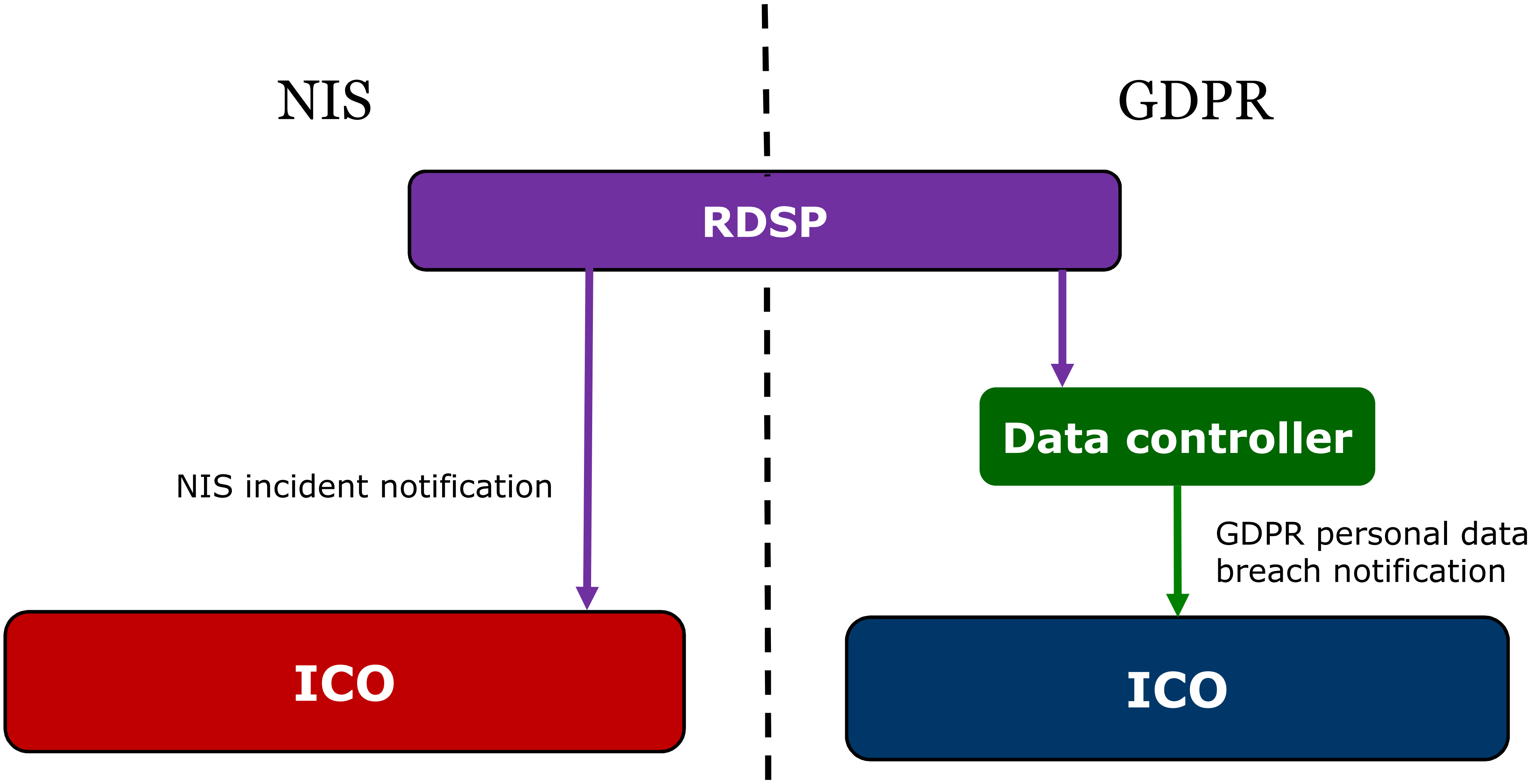
Personal data breach notification under GDPR


NIS
GDPR
OES
NIS incident notification
GDPR personal data breach notification
Competent Authority
ICO

When a NIS incident is also a breach of personal data processed by an OES (OES = data controller)


NIS
GDPR
RDSP
NIS incident notification
GDPR personal data breach notification
ICO
ICO

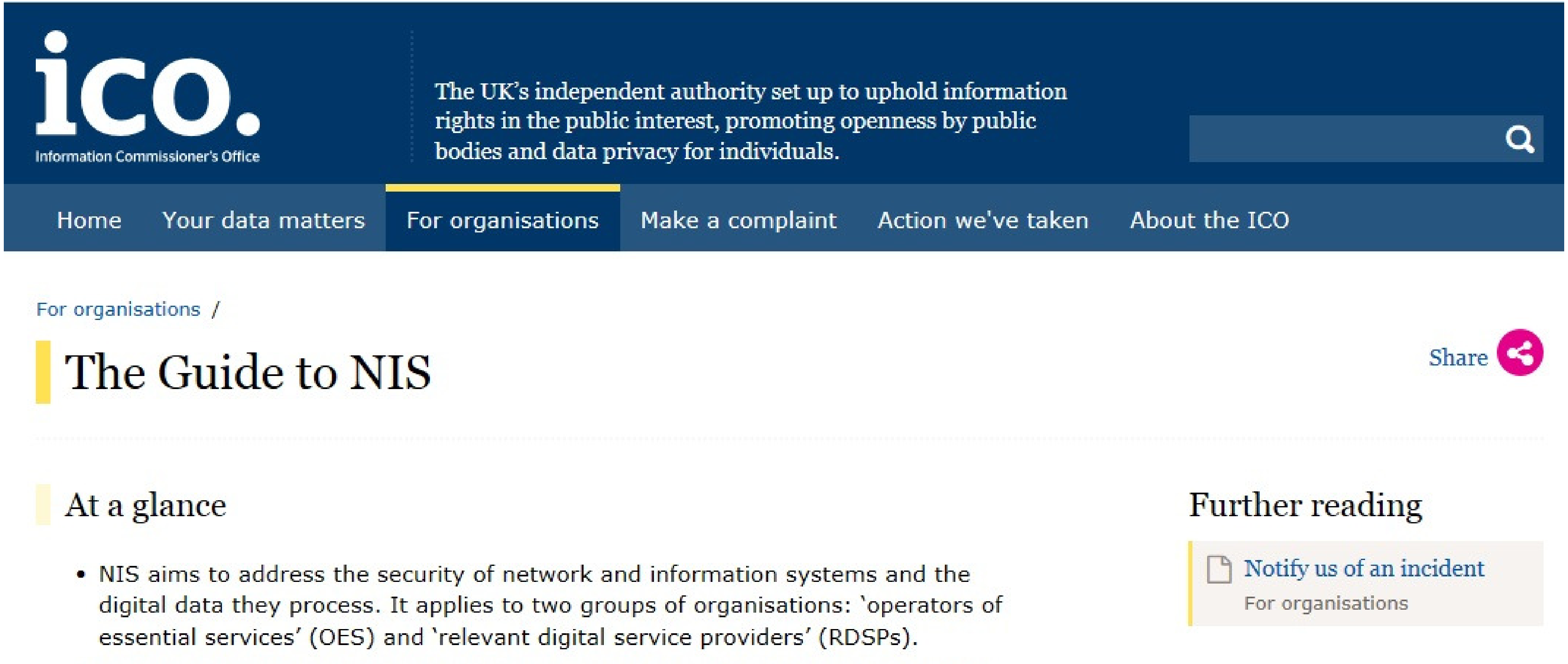
When a NIS incident is also a breach of personal data processed by an RDSP (RDSP=data controller)


NIS
GDPR
RDSP
Data controller
NIS incident notification
GDPR personal data breach notification
ICO
ICO

When a NIS incident is also a breach of personal data processed by a DSP on behalf of another (data processor)

What guidance is available?

https://ico.org.uk/for-organisations/the-guide-to-nis/


ico.
Information Commissioner's Office
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Home
Your data matters
For organisations
Make a complaint
Action we've taken
About the ICO
For organisations /
Share

The Guide to NIS

At a glance

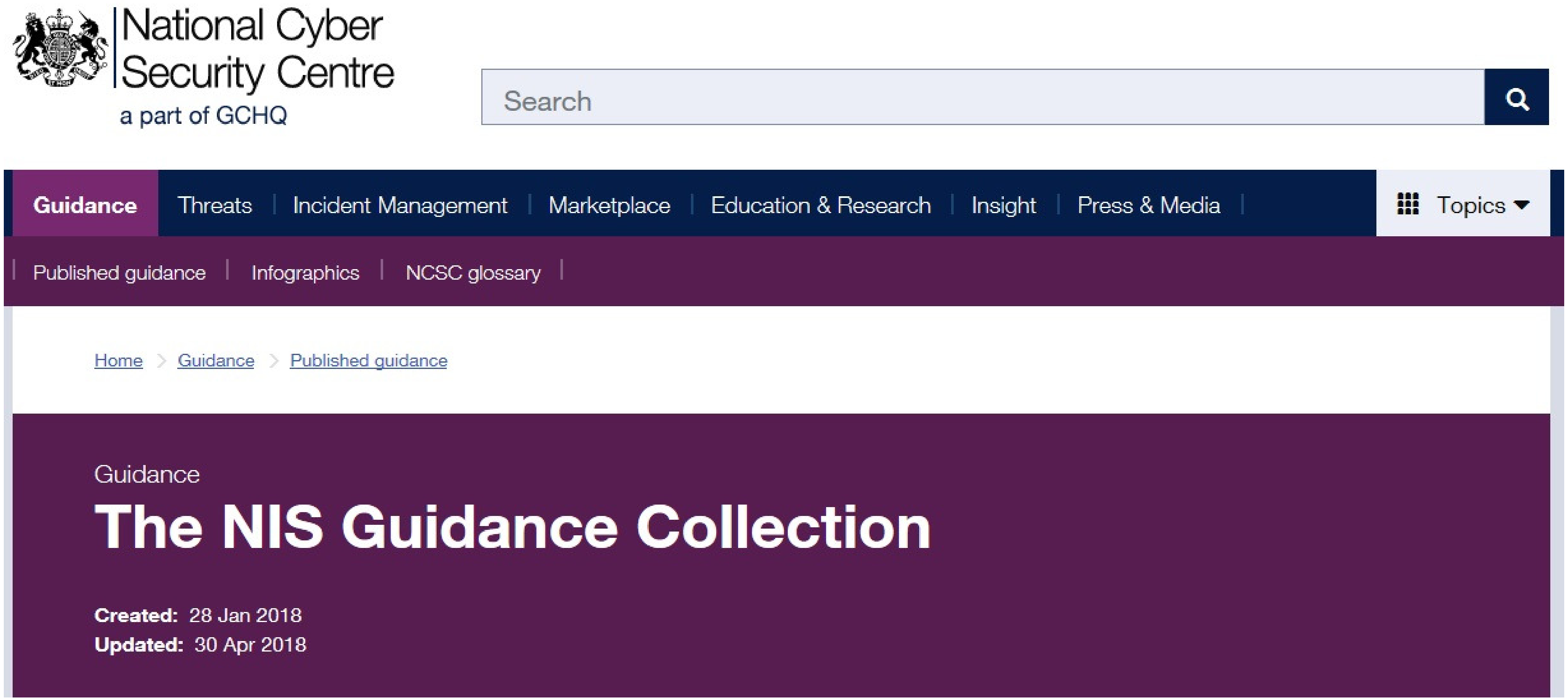
- NIS aims to address the security of network and information systems and the digital data they process. It applies to two groups of organisations: 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).

Further reading

Notify us of an incident
For organisations

The Guide to NIS – soon to be expanded!

https://www.ncsc.gov.uk/guidance/nis-guidance-collection/



Guidance

The NIS Guidance Collection

Created: 28 Jan 2018
Updated: 30 Apr 2018

NCSC NIS guidance – **note:** for OES **only**

Any questions?

NIS	**N**etwork and **I**nformation **S**ystems (note: NOT “security”)
NCSC	**N**ational **C**yber **S**ecurity **C**entre
OES	**O**perator of **E**ssential **S**ervices
GCHQ	**G**overnment **C**ommunications **H**ead**q**uarters
RDSP	**R**elevant **D**igital **S**ervice **P**rovider
CSIRT	**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam
SaaS	**S**oftware-**a**s-**a**-**S**ervice
SPOC	**S**ingle **P**oint **o**f **C**ontact
PaaS	**P**latform-**a**s-**a**-**S**ervice
CA	**C**ompetent **A**uthority
IaaS	**I**nfrastructure-**a**s-**a**-**S**ervice
ICO	☺

Acronymity

Resources

- NIS Regulations 2018
  - http://www.legislation.gov.uk/uksi/2018/506/made

- NIS Directive
  - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

- DSP Regulation
  - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0151&from=EN

Resources

- The Guide to NIS
  - https://ico.org.uk/for-organisations/the-guide-to-nis/
- EU SME definition – 2003/361/EC
  - https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003H0361&from=EN
- NCSC
  - https://www.ncsc.gov.uk
  - https://www.ncsc.gov.uk/guidance/nis-guidance-collection