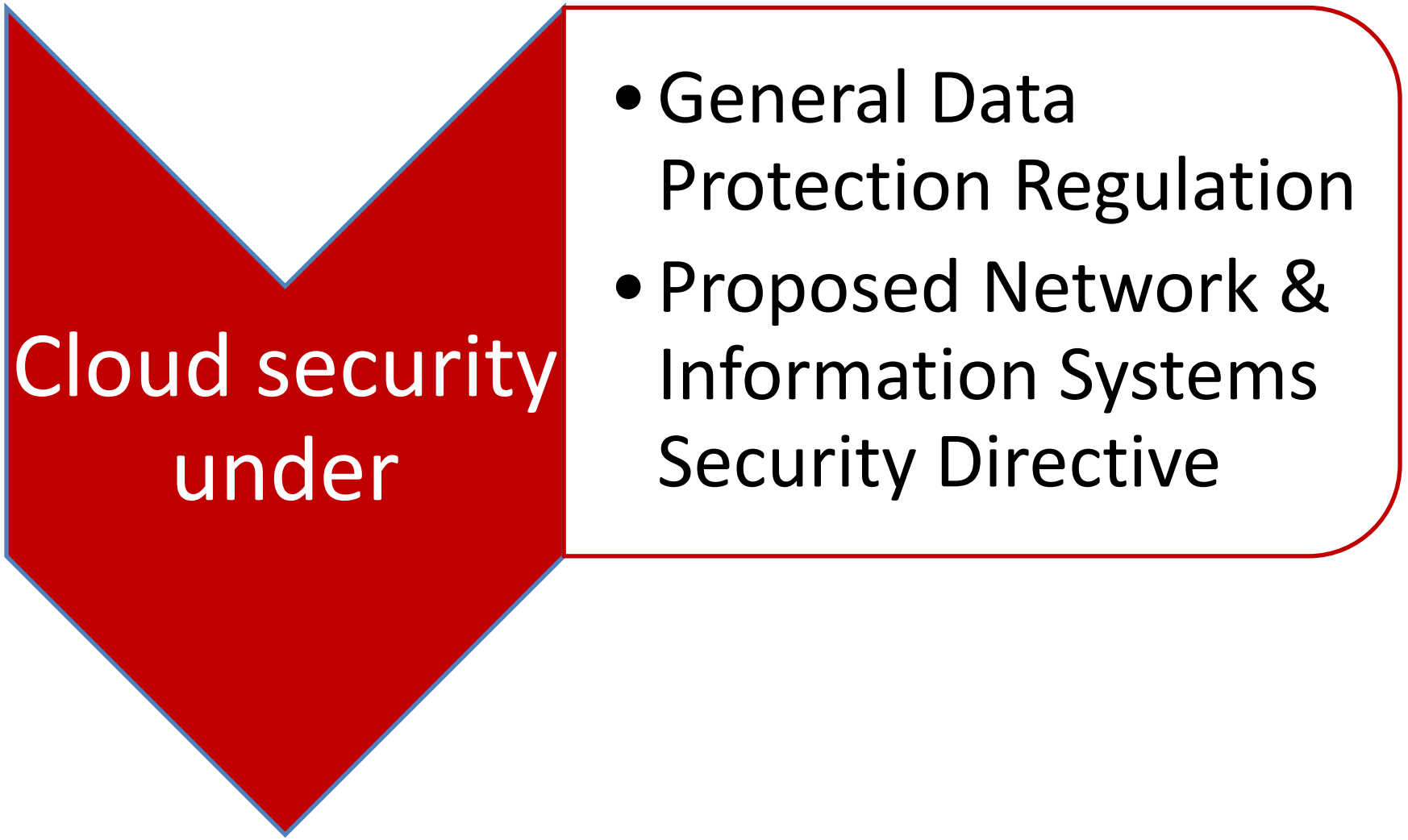
Cloud Security under Forthcoming Laws

Kuan Hon
kuan.hon@pinsentmasons.com
@kuanØ | k@kuan0.com

The laws, they are a-changin'…



@kuanØ

GDPR

GDPR - recap

Aim: modernise & harmonise EU DP laws

Now law; applies from **25 May 2018**

- Regulation, not Directive – directly effective
- 2 year lead / transition time

Accountability focus, big fines

Security – changes for both cloud customers & providers

@kuanØ

GDPR's key changes affecting cloud

New processor
(cloud provider)

- Obligations, and
- Liabilities

Expanded requirements when a controller (cloud customer) uses a processor (cloud provider)

- Due diligence
- Contract terms
- Ensuring compliance

@kuanØ

Processor issues

New obligations on processors (cloud providers)
- security, **international transfers**, record-keeping, DPO

Processor (cloud provider) **liability**
(>> security breach)

- Damage incl. non-financial – compensation if any contributory breach
- Exempt if prove “not in any way responsible” for “event” giving rise to the damage
- Recourse against others “involved” in same processing – if paid full compensation
- N.B. **contractual allocation, indemnities** !
- SCL article – older version of GDPR

@kuanØ

GDPR's contract requirements

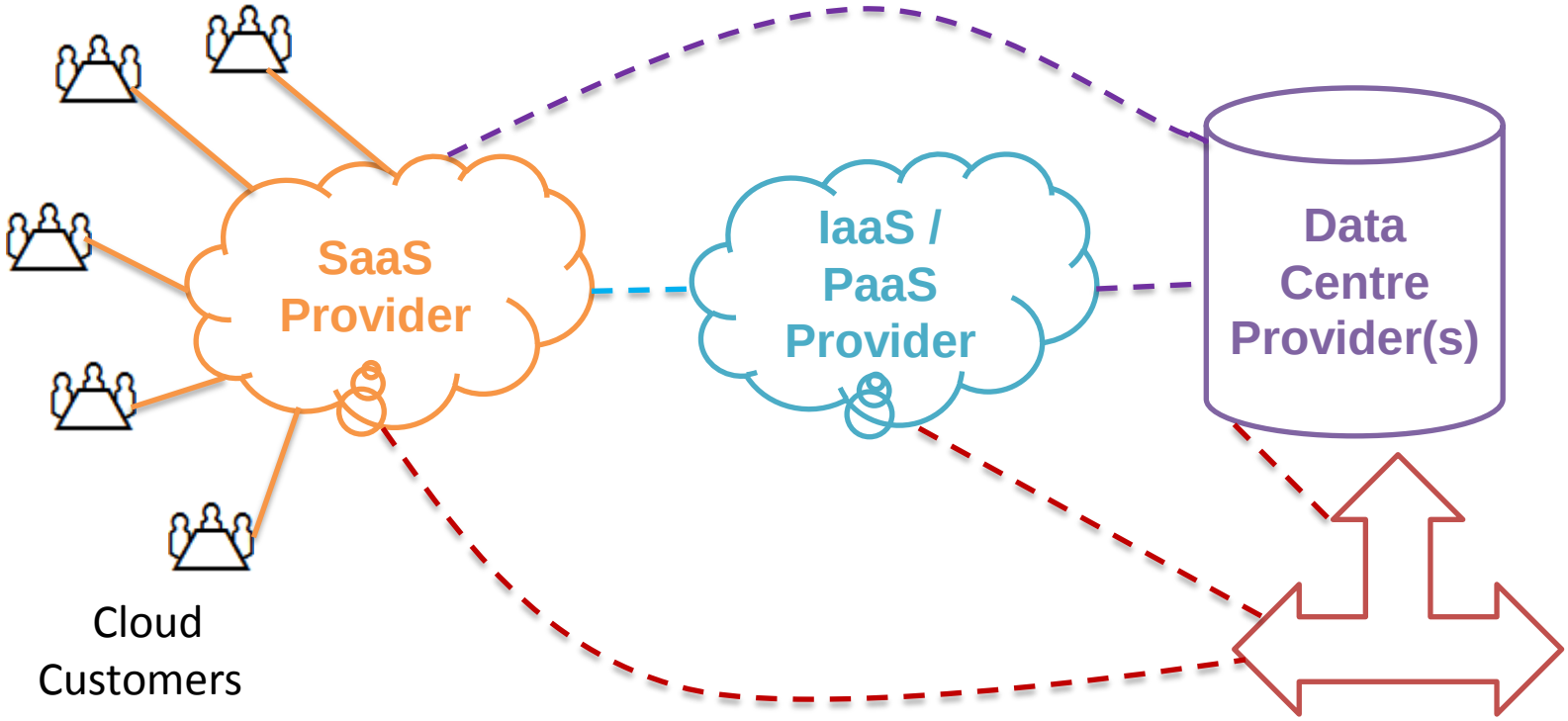
Many prescriptive provisions, including

- Subject-matter, duration, nature, purpose, type, categories…
- **Security & employee confidentiality obligations**
- **Information / audit rights** for controller
- "Assist" re. controller obligations (nature of processing, info.)
  - **Security, breach notification**, **DPIA**, prior consultation
- **Sub-processors** – prior consent, notify changes; **"flow down"**
  - impossible except for biggest cloud providers ?

Problem for commoditised, standardised public cloud !

@kuanØ

Cloud – many sub-processors



[Not just cloud!]

@kuanØ

GDPR contracts – fine !

Fine 2% / €10m for **both** controller & processor if contract is non-compliant

No "grandfathering"

@kuanØ

Contracts - practical steps

Providers - change standard terms, from **25 May 2018**

- More detailed **allocation of obligations, liability; indemnities**
- Increase **pricing; extra charges for providing "assistance" etc.**
- (Unlikely to agree to GDPR terms before 25 May 2018 - more onerous)

Customers - contracts expiring after **25 May 2018** (if negotiable)

- Add **change of law / change control** term re.:
  - Comply with **GDPR requirements,** who bears **costs of change**
  - **Responsibility & liability allocation, indemnities; pricing / charges**
- Start considering changes / negotiating position
- NB. existing (even non-cloud) contracts too

Commission / supervisory authority may adopt standard terms

- CSA leadership role
  - draft & put forward **cloud-appropriate terms** ?

@kuanØ

GDPR's security requirements

Controllers & **processors** (incl. cloud)	
C I A, incl. encryption	**+ resilience / bus. continuity** **+ regularly test & evaluate** effectiveness
Risk-based incl. state of art, costs + **steps to prevent persons with authorised access** from processing except on controller's "instructions" (or EU / Member State law)	
Practical impact – apply security best practices	NB. organisational measures – people, processes
	NB. accountability focus – **records / logs…**

@kuanØ

Processors' security obligations

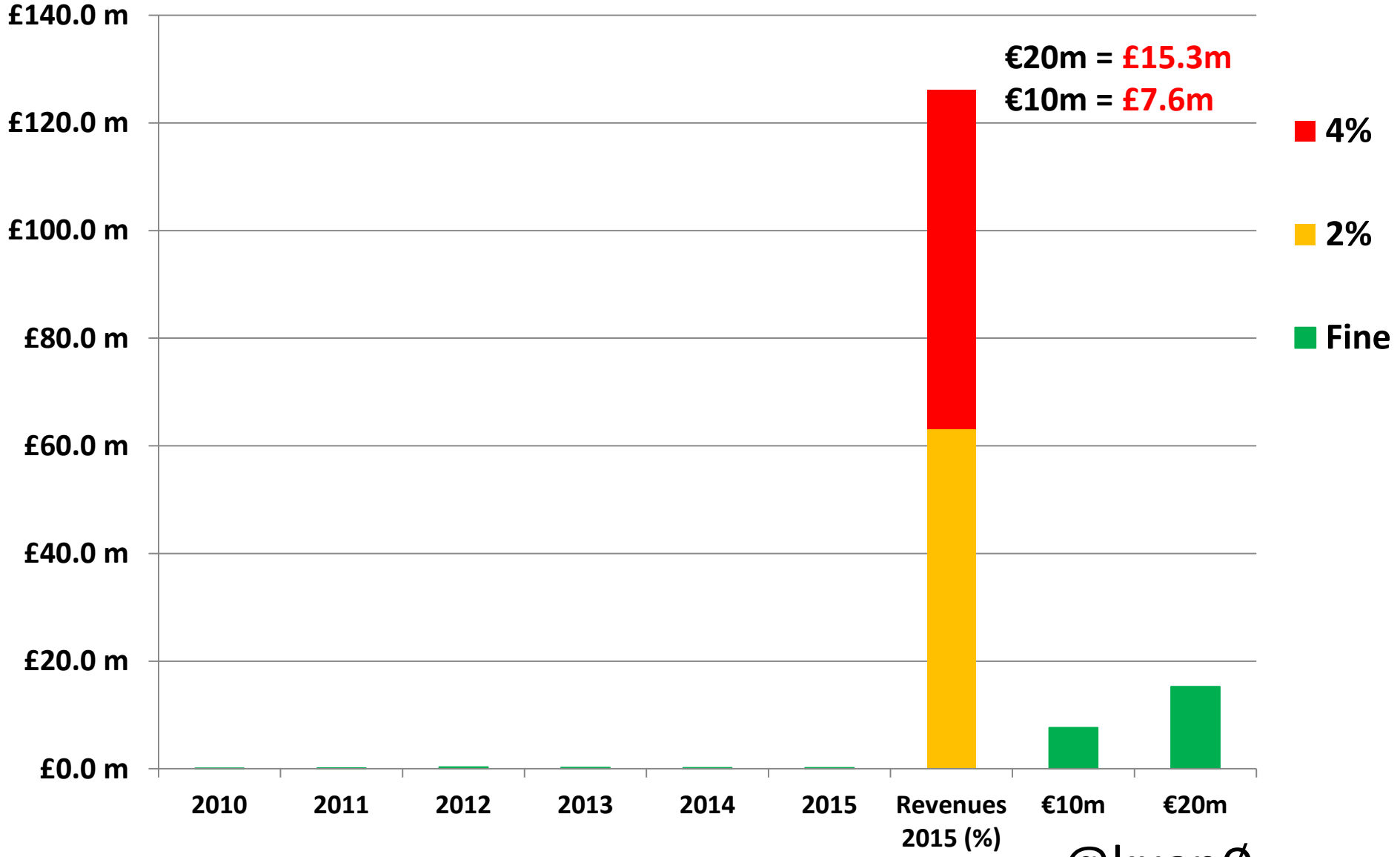
@kuanØ

Other GDPR changes re. cloud security

Fine for breach of security requirements	• **Controller: 4% / €20m** • Processor: 2% / €10m • (+ Compliance may help mitigate fines)
Approved codes / certifications – help show compliance	• **CSA leadership role** – propose CCM etc ?
"Personal data breach" notification obligations	• Controller • To authority; individuals (encryption) • **Processor to controller**

@kuanØ

Largest ICO Fine v. Large UK FS co.'s revenues 2015



@kuanØ

Implications for cloud

"Guaranteed" security & "strict" liability *vs* price ?

- Costs to customise etc., *vs* public cloud

Risks – infrastructure providers

- Raise prices; refuse services; close EEA ops, free services; not use EEA DCs ?
- Impact on innovation / services to EEA citizens

Or will laws be ignored ? Enforceable, fines..

Favouring large incumbents over small startups ?

- Control / influence supply / contract chain, afford certifications

@kuanØ

Killing cloud quickly with DP

The GDPR's coming, soon to be law they say
Middle of 20-18 will be the fateful day !
What will this mean for clo-ud ?
Will cloud be here to sta-ay ?
Don't want to be pessimistic, not sure how we'll find a way
Killing cloud quickly with DP, killing cloud quickly, with DP
Tearing up SaaS, PaaS and I-aaS
Killing cloud quickly, with DP…?

Full article www.scl.org/site.aspx?i=ed46375

Photo of Roberta Flack by Roland Godefroy CC BY 2.5

@kuanØ

Summary

Start now ! Fines will get boardroom attention…	
Processors' new obligations / liability	
Controllers & (sub-) processors	• Contracts for both – inventory, changes; liability allocation, indemnities, seek fault-based • Cloud solutions ? CSA – standard clauses ?
Re-engineer systems / processes to comply, incl.	• Controllers - DP by design & default, incl. security; DPIAs, incl. security
Codes & certifications etc. - increased role	• CSA – certifications etc ?

@kuanØ

NETWORK & INFORMATION SYSTEMS SECURITY DIRECTIVE

Overview

Security & incident notification obligations

Operators of "essential services"

+

"Digital service providers"

All data, not just personal data

Supervision

Regulatory powers - info, audits, remediation, notify other MS, (after consulting) public

MS rules on penalties for infringement

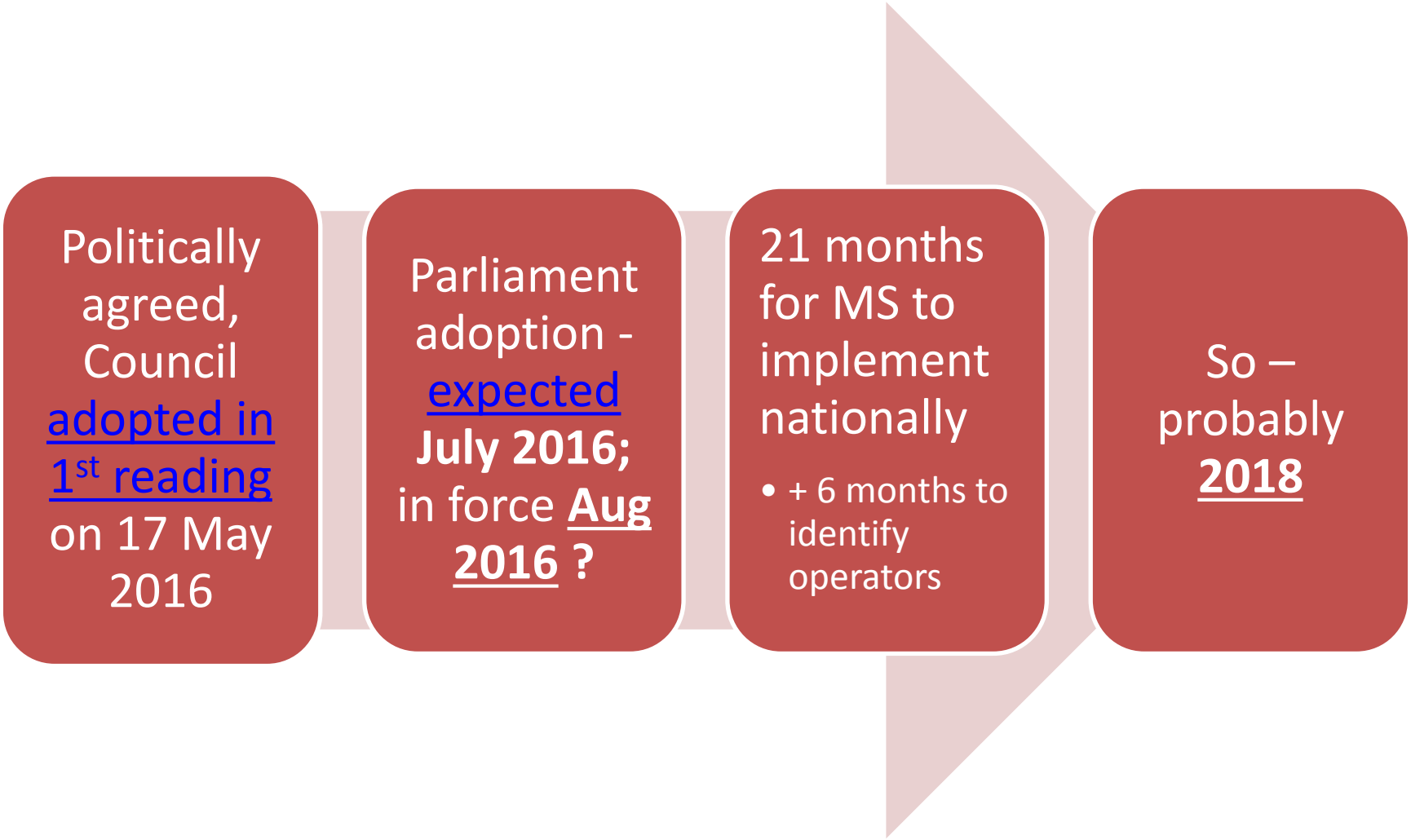
Other points

Minimum harmonisation, Directive

To improve MS cyber-capabilities, co-op / info sharing (CSIRTs etc.)

@kuanØ

Timetable



@kuanØ

“Operators”

MSs to identify operators (list / objective criteria) & determine national regulator(s)

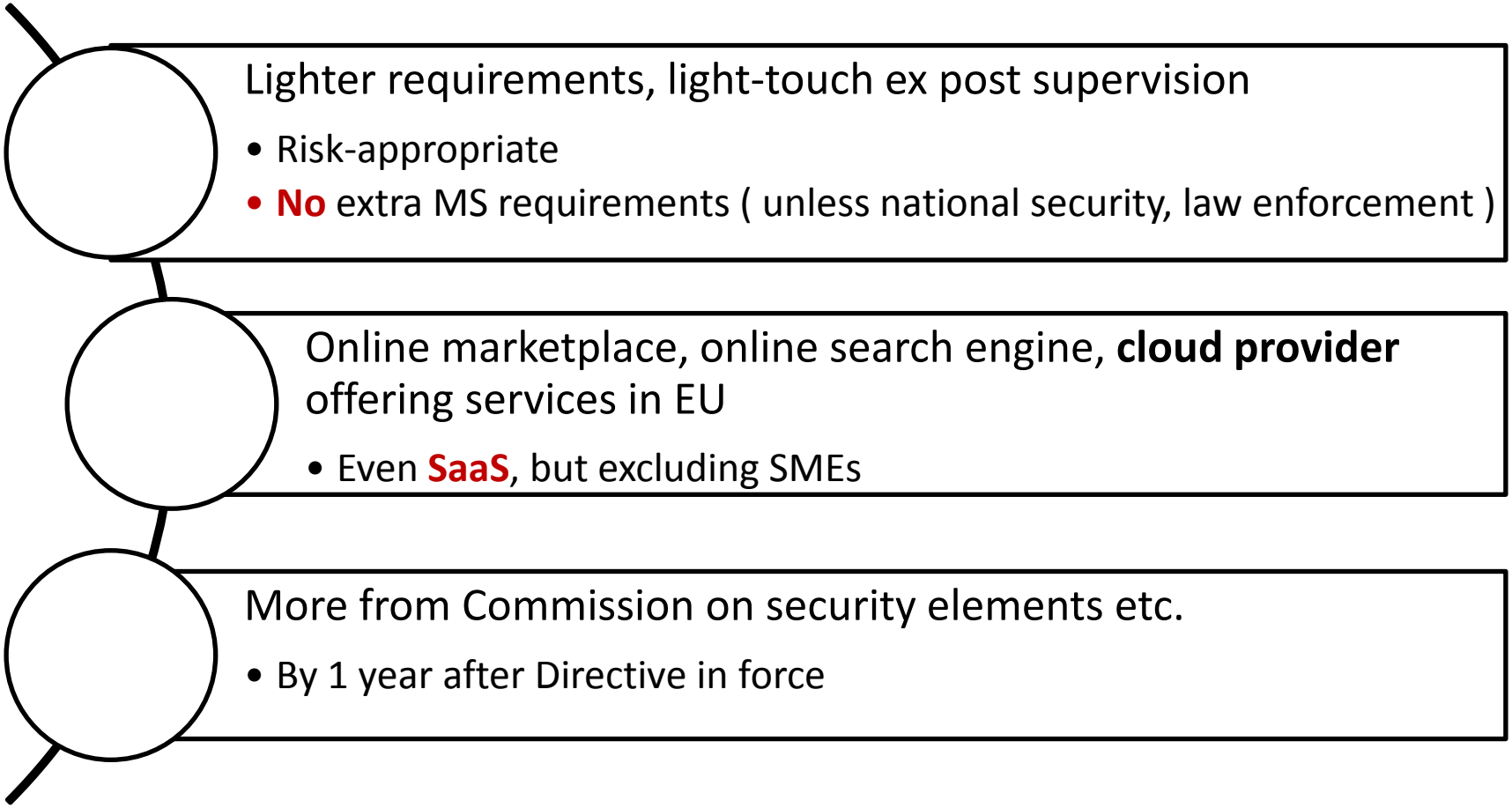
- Banks, financial market infrastucture, energy, water, transport, health, digital infrastructure (IXPs, DNS providers, TLD name registries)
- Exceptions - Framework Directive, EIDAS TSPs, equivalent sectoral obligations

Requirements != GDPR ?

- Security - “appropriate and proportionate” technical & organisational measures to manage risks to NIS security (*vs* individuals; processing)
  - **state of the art** (costs ?)
- Notification - “incident” (event – actual adverse effect on NIS security) *vs* “personal data breach”

@kuanØ

DSPs


Lighter requirements, light-touch ex post supervision
• Risk-appropriate
• No extra MS requirements (unless national security, law enforcement)
Online marketplace, online search engine, cloud provider offering services in EU
• Even SaaS, but excluding SMEs
More from Commission on security elements etc.
• By 1 year after Directive in force

@kuanØ

Incident notification

Operators of essential services

- "Without undue delay" to competent authority / CSIRT
- If "**significant** impact" on essential service's continuity
  - Incl. **incident affecting DSP** relied on for essential service

DSPs

- "Without undue delay"
- If "**substantial** impact" on provision of service in EU

Guidance ?

- Commission & national authorities - TBA

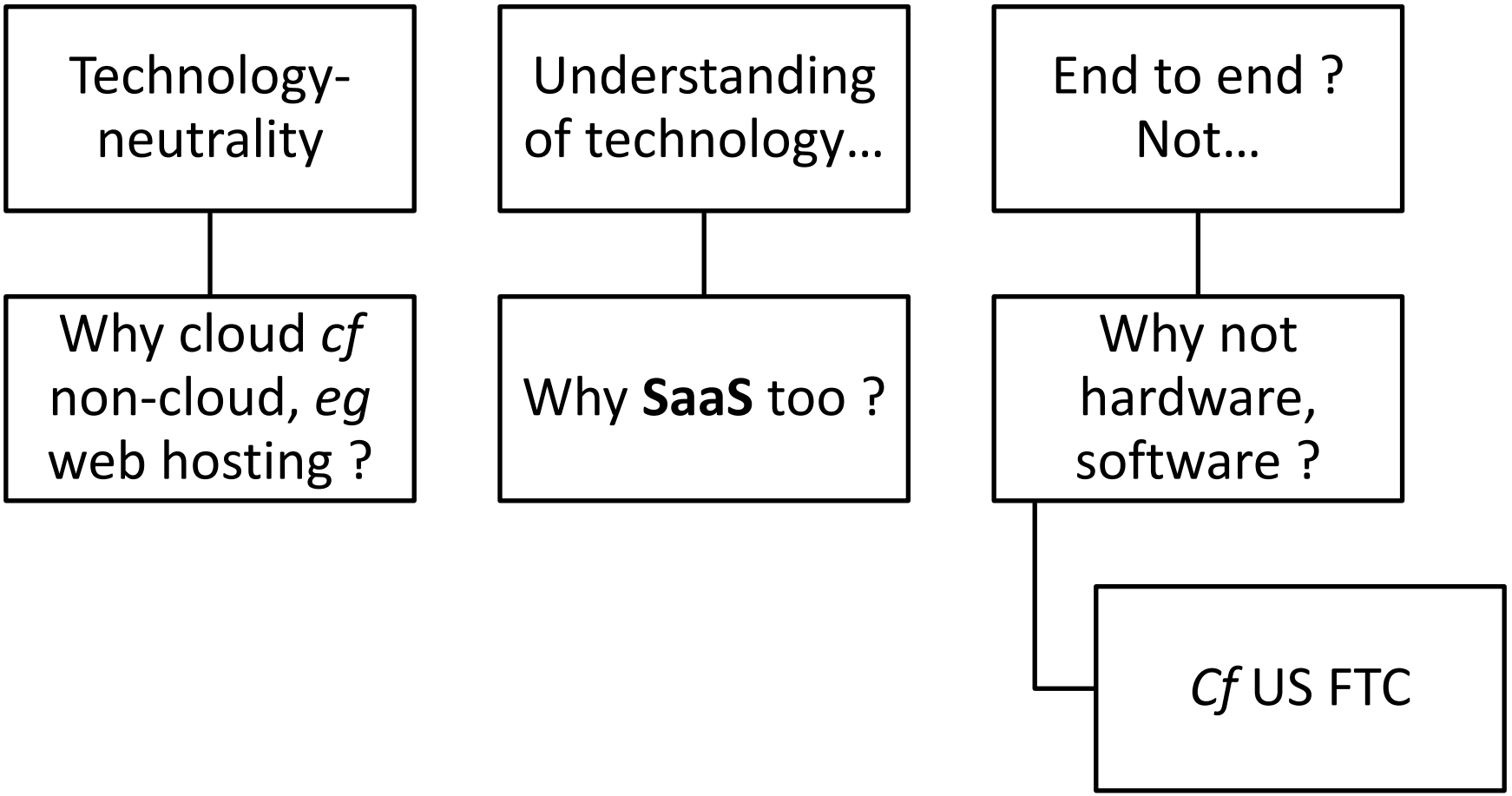
@kuanØ

Possible problems

Operators – multiple Member States	Slightly different security & notification requirements under NISD / GDPR
• “Essential” in some only ?	• Eg notify different authorities ?

@kuanØ

Technology issues



@kuanØ

Practical steps

Start preparing now ! And monitor

- Operators – national law, guidance
- DSPs – + Commission acts

Operators – essential services relying on cloud

- Compliance with security & notification obligations in cloud ?
- Contracts – security, incident notification requirements; negotiation with providers !
  - Cloud sub-processors ?

Cloud services (& more)

- Systems, processes, etc. as well as contracts

@kuanØ

Overall summary of practical steps

Start now ! GDPR fines – board…

Contracts – inventory, change control etc.

Systems / processes – change; best practices

- Both **security** & **detection** / **notification** measures
- NB. **differences** between GDPR / NIS
- Rehearsals etc.

Consider insurance

- Will the new laws boost cyber-insurance market ?

@kuanØ

Further info

- Data security developments under the General Data Protection Regulation (older GDPR draft) http://www.pinsentmasons.com/en/media/published-articles/gdpr-latest-data-security-developments/
- GDPR contract issues, impact on service providers (on older GDPR draft) http://www.scl.org/site.aspx?i=ed43376
- GDPR impact on cloud generally http://www.scl.org/site.aspx?i=ed46375
  (shorter version https://iapp.org/news/a/gdpr-killing-cloud-quickly/)
- Policy problems affecting cloud http://www.iicom.org/intermedia/intermedia-january-2016/dark-clouds
- GDPR's application to non-EU organisations https://drive.google.com/file/d/0B_8WW30Fjs1MRlQ5NW1LMkxQczg/view?usp=sharing

- See also http://www.kuan0.com/publications.html and http://www.kuan0.com/presentations.html

@kuanØ

Thank you!

Kuan Hon

Half lawyer | half geek | mostly harmless

Twitter: @kuanØ
Email: k @ my domain below; also
kuan.hon@pinsentmasons.com

www.kuanØ.com | blog.kuanØ.com