GDPR & Service Providers (Cloud Focus)

Kuan Hon

Senior Researcher, Cloud Legal Project &
Microsoft Cloud Computing Research Centre,
Centre for Commercial Law Studies
Queen Mary, University of London

w.k.hon@qmul.ac.uk

Queen Mary University of London
Centre for Commercial Law Studies

Data Protection Directive obligations

- Currently on “controller”
  - with exemptions e.g. personal use
- Controller may use “processor”
  - requirements when using processor, incl. **processor agreement** on certain terms
- **Direct processor data protection law obligations – few Member States (MS)**

Queen Mary University of London
Centre for Commercial Law Studies

Cloud providers

- Processors (storage), sometimes controllers
- Current laws – 1970s outsourcing (12Cs, 9Ds):
  - cf. controller's direct **self-service** use of **commoditised / standardised, shared resources** (esp. **infrastructure providers** - IaaS, PaaS, pure storage SaaS)
    - no knowledge of data's nature, controller may encrypt
  - cf. direction of travel – sub-processors & layers
- GDPR would perpetuate 1970s assumptions
  - not technology-neutral !

@kuan0

GDPR - ***direct*** processor obligations

- "Establishment" in EU + processing personal data in "context of activities" of that establishment
  - v. broad (*Google Spain*) – subsidiary, **DCs ?**
- Processing activities "related to" offering goods / services to EU data subjects or monitoring them
  - Parl – **+ processors**; free services too (Parl & Coun)
- **All - even if processing exempt** - personal (SNS / email / storage); crime / national security

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Processor liability

- Processors "involved" can be sued ***directly*** for damage from non-compliant processing
  - ➢ each liable for **entire amount of damage**
    - recourse claims (Council), written allocation (Parl); when processor is liable – iff not complied with GDPR processor obligations or lawful controller instructions (Council) – but causation ?
  - ➢ **"may"** be exempted if **prove it's not responsible for "the event"** (Council – "shall", but "in any way" ?)
- "Processors" – incl. **sub-processors** (layered cloud – Dropbox on Amazon); & **DC providers ?**
- *Processors' princelier pockets ?*

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Regulators' powers over processors

- Same as over controllers – extensive powers
- Processor must cooperate - info, orders etc
- **Audit powers, access to premises (on-site inspections)**
- Fines – up to 5% annual worldwide turnover or €100m if greater (Parl)

Queen Mary University of London
Centre for Commercial Law Studies

Requirements when using processors

- Expanded requirements re. processor contracts
  - info re. processing purpose etc. – infrastructure cloud and *prying processors*
  - "instructions" – self-service cloud (as now)
  - "assist" controller re. obligations on security, breach notification, DPIA, prior consultation – commoditised cloud
  - data deletion – cloud - delete pointers
  - show compliance, site inspection (Parl), controller audits (Council) - cloud security / practicalities

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Other problems

- Direct (non-contractual) obligation (Council)
  - "immediately inform the controller if, in his opinion, an **instruction** breaches this Regulation or Union or Member State data protection provisions"
  - cf. self-service cloud ?
  - *policing processors ?*

- NB existing processor agreements
  - no grandfathering ? (not just cloud) !

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Sub-processors

- "Enlist" iff prior controller consent

- Sub-processor contracts
  - must impose **same obligations** on sub-processors – Council

- Cloud's "reverse direction" ?
  - and will sub-processors agree to such contract terms ?

Queen Mary University of London
Centre for Commercial Law Studies

Security (differences in versions)

- "Security of processing" – controllers **& processors**

- **Risk evaluation** to assess appropriate security level
  - cloud - commoditised mixed use infrastructure… *prying processors,* customisation, highest comm denom ? (cost)

- **Processor directly liable for security breach**
  - including if personal use, **no "controller"**
    - even if user's fault ? – processor must prove it's not responsible

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Other issues for processors

- International transfers – processors too
  - and more restrictive (own decision banned, tech protections considered insufficient)
- Record-keeping requirements, DPO etc
- Controller's DPIA / prior consultation
  - processor to conduct / assist ? - commoditised cloud
- Parliament would extend to processors:
  - Risk analysis, DP by design / default - *prying processors,* commoditised cloud
- Codes, certifications, seals – "an element" (Council), EDP seal shield ? (Parl)

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Summary – cloud-inappropriate

- Net very wide; obligations too in some cases
  - "related to" offering goods, EU data centres ?
- Infrastructure providers caught
  - even with encrypted data – knowledge irrelevant
- Liability risk (**no intermediary defence ?**)
  - Council would **exclude** E-Commerce Directive
- Unclear responsibility allocation
  - Often "controller or processor" – either, both, when ?
- Customisations required ? eg security
- Access to premises – controllers, DPAs

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Practical implications (not just cloud)

- Could non-EEA providers
  - raise prices - or refuse if EEA, PD etc ? (& if customer lies ??); stop EEA ops / free consumer services / EEA DC use?
  - impact on innovation / services - needs considered policy decision
  - or, will laws just be ignored, if too wide ?
    - Enforceability (outside EEA) ? DPA resources ? But potentially huge fines…
- Clarification needed – which processor obligations apply when, scope, liability; certifications / codes
- Providers & other (sub) processors - contract terms
  - liability allocation, indemnities etc (& seek fault-based ?)
- Codes & certifications – much increased role
- Big players may be winners (unintended consequence ?)
  - required contract terms (incl sub-processors); security, etc

@kuan0

Queen Mary University of London
Centre for Commercial Law Studies

Thanks for listening !

(longer version – on previous Council draft)

w.k.hon@qmul.ac.uk

cloudlegalproject.org
mccrc.eu

@kuan0 | kuan0.com
blog.kuan0.com

Queen Mary
University of London
Centre for Commercial Law Studies