Cloud Security under the EU Data Protection Directive and draft General Data Protection Regulation

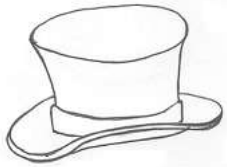
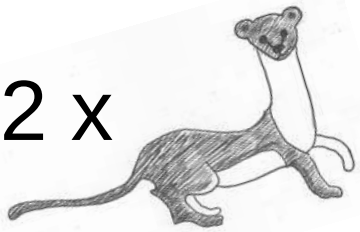
Kuan Hon

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

Introduction

- Self – 4 x  3 x  2 x 
- CLP, MCCRC & A4Cloud
- Questions – please leave till Panel session

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

Data Protection Directive – recap

- "Controller" ("purposes & means") legally-obliged to comply with data protection (DP) principles when processing personal data (PD); regulated by national DPAs
  - + rules for "special category" sensitive data e.g. health
  - "processing" incl. storage, transmission – digital data
  - controller may use "processor" to process PD for it
    - incl. cloud provider
    - controller remains responsible / liable !

Queen Mary University of London
Centre for Commercial Law Studies

Cloud computing - recap

- Use of IT resources over a network (typically the Internet), scalable up / down with demand
  - **SaaS** – IT resources = software applications
    - E.g. webmail, Facebook, Salesforce, Office 365, Google Apps, Dropbox
  - **IaaS** – IT resources = raw IT resources (storage, compute, networking) e.g. Amazon Web Services
  - **PaaS** – IT resources = platform for developing, hosting, deploying software apps e.g. Microsoft Azure
- Public (shared), private, hybrid

Cloud – key points

- Benefits – costs-savings and flexibility
  - efficiencies & economies of scale – through use of **shared, standardised, commoditised resources**, PAYG / free
  - agility, innovation – startups save on capex
- Risks – supply chain, **third party resources**
  - possible provider "layers" ("sub-processors")

Customer ---- DropBox ---- Amazon
SaaS IaaS

  - renting "someone else's computer"

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

5

“Security” under DPD – Art. 17

- National differences, but…
  - “appropriate **technical and organizational measures** to protect personal data against **accidental or unlawful destruction** or **accidental loss, alteration, unauthorized disclosure or access**… and against ***all other unlawful forms of processing”*** - > technical security
  - ensure security level “**appropriate to the risks”** of the processing and nature of the data - **state of the art, cost** – i.e., risk-based approach

If using processor for PD

- Part of “Security” under Art. 17
- Controller must:
  - ➢ pre-contract - choose a processor providing **sufficient guarantees** re. “security”
  - ➢ written contract with processor –
    - act only on “**instructions”** from controller
    - equivalent security obligations on processor
  - ➢ post-contract - ensure compliance
    - still responsible & liable

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

7

WP196 - Art. 29 Working Party (2012)

- Cloud - loss of control & lack of transparency
- Pre-contract - risk assessment (e.g. ENISA's)
  - incl. DP compliance of contract - esp. **security obligations, international transfers**
- Contract "must", generally:
  - allocate responsibility (esp. if **sub-providers**)
  - contain "standardised" DP safeguards incl. -
    - tech / org measures, data export, **accountability mechanisms** e.g. audits / certifications
  - & more – SLAs / penalties, purpose; sub-processor consent, location, contract; data subject access…
- N.B. authoritative but non-binding…

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

8

Cloud security - reality

- **Differing degrees of control – *not* one size fits all !**

SERVICE OWNER	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

Table © Cloud Security Alliance reproduced with permission

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

9

Cloud contracts – realities

- Providers' standard terms – negotiate ?
  - ➢ practicalities of negotiating cloud contracts research
    - public sector, financial services
- Pre-contractual info / audits re. provider security
  - ➢ individual audits impractical, can increase risks
  - ➢ independent third party expert audit, share summary
    - industry-standard security / cloud certifications / codes
      - e.g. ISO27001, ISO27018, CSA CCM, CIF Code
      - NB. assess against *own* position / risks – DPAs

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

10

Cloud contracts – security terms

- Security requirements – whose security policy ?
  - standardised – vs. different customers, conflicts ?
- Security audit rights; logging obligations
  - WP196 – third party auditor chosen by ***controller***
  - regulated sectors like financial services
- Disclose data to authorities: legally-binding ?
- Breach notification / handling
- Deletion – WP196: all copies, “irretrievably” ?
  - “pointers” – Google Apps

11

Problems with current laws & cloud

- Laws based on 1970s outsourcing (12Cs, 9Ds)
  - ➢ deliver data, processors' access to intelligible data, "active" processing as per controller's "instructions"
    - vs. direct ***self-service*** use of IT resources ("instructions" ?)
    - vs. shared, ***standardised***, commoditised resources, at scale
    - vs. infrastructure provider ***knowledge*** of PD (e.g. encrypted)
      - rent a computer – manufacturer / rental co. not "processor"
  - ➢ location-independent – customers, providers, resources
    - logical remote access, physical (CNIL's cloud guidance…)
- GDPR *perpetuates* 1970s models / assumptions !

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

12

GDPR - progress

- Commission - draft modernising General Data Protection Regulation (GDPR) – Jan 2012
  - & separate crime / law enforcement Directive
- European Parliament – different – Mar 2014
- Council - yet another version – 1 June 2015
  - Presidency - Latvia now, Luxembourg July-Dec 2015

- Paper - GDPR impact on cloud computing (under the A4Cloud EU project)

Queen Mary University of London
Centre for Commercial Law Studies

Key changes – moving target

- "Security" expanded + (new) **breach notification**
  - processor contract requirements - WP196 – perpetuating problems
- Processors – next
- New accountability provisions relevant to security
  - DPIA, prior consultation, DP by design & default
  - Certifications, seals, codes - shortly
- Strengthen DPA powers – but funding ? Fees abolished…
  - e.g. audits, & fines (5% turnover / €100m - Parliament)
- (+ others – International transfers - more restrictive; Subject access, RTBF, data portability, "class actions"; Jurisdiction & one-stop shop (summary report))

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

14

Processor obligations – security, etc.

- Data subjects could sue processors *directly*
  - ➢ burden of proof
    - personal use, no "controller" – user's fault ?
  - ➢ recourse rights ?
- Fault-based allocation of liability, or strict ?
  - ➢ debate in Council
- (+ DPOs, transfers, record-keeping; prior consultation, DP by design / default (Parl))

15

Certifications, seals, marks, codes

- To engender trust – but costs; “DP” not security
- Legal incentives to encourage adoption ?
  - Council – “an element” to show compliance
    - detailed provisions on third party certifications etc.
  - Parl. – European DP Seal - DPA
    - fines - shield if non-negligent, non-intentional breaches
- Applies to controllers / processors only
  - cf. tech standards ? - new European Data Protection Board may certify tech standards as GPDR-compliant (Parl) – but legal status of use ?

16

The future ?

- Council's version – today / future ??
  - ➢ timetable ?
- EU institutions must agree **same** text before GDPR can become law – flowchart
  - ➢ "trilogue" – starting next week ??
    - ○ conciliation ?
- Moving target !! + **[2] years after adoption**
- **Regulation** not Directive, to harmonise – but
  - ➢ specific areas of MS discretion (e.g. Amberhawk)
  - ➢ ambiguity

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

17

Consequences ?

- "Guaranteed" security & strict liability worth the price ?
  - costs to customise, overwrite, vs. cheap commodity public cloud
- Risks – "infrastructure" providers raise prices; refuse services if EEA, PD etc; close EEA ops / free services; stop using EEA DCs ?
  - impact on innovation / services to EEA citizens
- Or will laws be ignored, if too wide ?
  - enforceability - but fines…
- Control of supply / contract chain
  - big cloud players may be winners – dictate contract terms, sub-processors, afford certifications etc.

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

18

Practical implications

- Cloud providers & other (sub-) processors - contracts
  - liability allocation, indemnities etc (& seek fault-based ?)
  - if strict liability is intended – GDPR needs to be much clearer

- Codes & certifications etc. - may have much increased role

19

Recommendations (personal !)

- Laws, including GDPR, don't (but should)
  - ➢ regulate only those with access to *intelligible* PD
    - Education re. controller self-help – encryption where feasible, backups
  - ➢ prohibit (or require contracts to prohibit) unauthorised "use or disclosure" by processors (incl. after termination), *not* "instructions"
- E-Commerce Directive intermediary defences should explicitly apply to personal data processing
  - ➢ e-commerce, innovation; fairness (knowledge)
- Processors, certifications etc. – clarify; consequences
- ENISA should be given a formal role under GDPR
  - ➢ Commission, EDPB etc. – obtain and take account of ENISA's advice on ***all*** security issues (not just cloud)

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

20

Security laws, more generally

Queen Mary
University of London
Centre for Commercial Law Studies

Five Factors - MEERS

- **M**ulti-disciplinary meeting of minds
  - *One* track - lawyers *and* technologists !
    - different mindsets – binary vs. analogue
    - terminology confusion - e.g. “data protection”
- **E**vidence-based, expertise-informed law-making
  - take account of expert advice incl. ENISA
- **E**ducation, empowerment – lawmakers / regulators too
- **R**isk-based approach (vs. 100% security forever)
- **S**upport sharing of security info suitably (> gov / orgs)
  - reports by customers / others – encourage ethical disclosures, don’t gag / jail / fire ! (breaches not discovered internally…)
    - examples

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

22

Thanks for listening !

w.k.hon@qmul.ac.uk
cloudlegalproject.org
mccrc.eu

@kuan0 | kuan0.com
blog.kuan0.com

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

23