Draft General Data Protection Regulation - Codes, Certifications, Seals

Kuan Hon

Research Consultant, 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

Codes, certifications / seals – DPD

- DPD – obligations on "controllers" who process personal data
  - controllers may use "processors" (not directly liable)
  - supervised by DPAs; role of A29WP
- Currently – codes of conduct to be encouraged (Art. 27), including A2WP approval
- Not much take-up. But e.g.
  - UK ICO anonymisation code; privacy seals – 2016 ?
  - Commission's Cloud Select Industry Group on Code of Conduct for cloud computing, & A29WP…

GDPR – progress - recap

- Commission - draft General Data Protection Regulation (GDPR) – Jan 2012
  - & separate crime / law enforcement Directive
- European Parliament – different – Mar 2014
- Council - yet another version – Dec 2014
  - "nothing is agreed until everything is agreed" (PGA)
  - expected June 2015
- EU institutions must agree **same** text – flowchart
  - "trilogue", conciliation ? **+ 2 years**
- Regulation not Directive – but…

Queen Mary University of London
Centre for Commercial Law Studies

Codes, certifications, seals - GDPR

- Processors – will be **directly** liable under GDPR
- A29WP -> EDPB

- Certifications, to award seals / marks
  - purpose - transparency, compliance, data subjects' assessment of protection level, i.e. trust
  - both controllers and processors
- Misuse of seal / mark – power to fine
  - If intentional / negligent – Coun
  - Deleted - Parl

Codes to facilitate GPDR compliance

- Industry (DPA – Coun) to draft codes; stakeholders
- Submit for DPA opinion (“shall” submit, “shall” approve if “appropriate safeguards” – Coun)
  - DPA publishes if approved; if multi-MS – EDPB opin first (Coun)
  - Commission may (Parl) declare “in line” with GDPR, **EU-wide validity,** (Parl) enforceable data subject rights, publicise
- Scope - fair processing, collection, notification etc; +
  - consumer rights; delete re. international transfers, etc. (Parl)
  - e.g. pseudonymisation, security, breach notification (Coun)
  - + international transfers (Coun) – “binding and enforceable commitments” re. data subject rights

5

Codes – effect, & monitoring

- To demonstrate compliance (Coun: “an element” only)
  - controller’s compliance generally (Coun)
  - *processors*’ “sufficient guarantees” for controller (Parl, Coun)
  - security
  - relevant to DPIA (Coun only) – *not* DP by design
- Factor in deciding whether / how much to fine (Coun)
- Mandatory monitoring – mechanism for DPA-accredited bodies to monitor compliance with code (Coun)
  - Detailed requirements for accreditation including complaints, enforcement
  - Public sector bodies exempt !

Certifications (Council)

- Certification bodies - requirements e.g. expertise; accredited by DPA *or* national accreditation body (as MS decides) - 5 years max.
  - report to DPA reasons for granting / withdrawing certification !
- Criteria - DPA or EDPB approves; published
- Validity – max. 3 years, certifier withdraws if not met
- EDPB public register: “certification mechanisms”, seals, accredited bodies, foreign accreditees, (in)valid certs.
- Adherence to approved certification - effect
  - “an element” to demonstrate compliance generally; security; DP by design / default; processor “sufficient guarantees”
  - provides “appropriate safeguards” for data exports iff “binding & enforceable commitments” to apply them
  - factor in deciding whether / how much to fine

European Data Protection Seal

- Parliament's draft - instead of external certifications
- *Only* DPA certifies "compliance" -> DP mark (EDP seal)
  - voluntary, affordable, transparent, not "unduly burdensome" (fee)
  - DPA may accredit third party auditors to conduct audits for it
  - DPAs to agree "harmonised" mechanism & fees
- Validity – max. 5 years, iff "continued" GDPR compliance
- Public e-register of valid / invalid "certificates" (EDPB)
- Commission to specify mechanisms' criteria/requirements, conditions to grant / withdraw, accreditation, "recognition"
  - with enforceable data subject rights
- Fine for misuse of seal / mark (Commission) – deleted..

European Data Protection Seal - effect

- Provides “appropriate safeguards” permitting international transfers, without requiring “specific authorisation”
  - iff both controller & recipient has seal (exporting *processor* ?)
- Shield for seal-holder against fines, iff
  - “valid” seal of controller “or processor” – either, both?
  - non-compliance was unintentional & not negligent
- Uncertainties
  - invalidity of seal through non-compliance (circular re. shield !)
  - register’s impact – if non-compliant, but register shows seal valid ?
    - is register conclusive, or not ? e.g. controller relies on it re. processor’s seal
  - “recognition” within EU / outside – no clear requirement
  - “enforceable” data subject rights - very vague

Issues

- Costs / time – so incentives to get certified etc. – e.g. legal benefits ?
  - ➢ European Data Protection Seal best (Parl)
    - shield etc.
  - ➢ Certifications – “an element”; recognition within EEA ?
- Other liability issues
  - ➢ certifiers / accreditors’ liability e.g “bad” certification
  - ➢ processors’ position

@kuanØ

Queen Mary University of London
Centre for Commercial Law Studies

10

Thanks for listening !

Paper - GDPR impact on cloud computing

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

@kuan0 | kuan0.com
blog.kuan0.com

11