UiO : Faculty of Law
University of Oslo

COINS Summer School 2019 – Cybersecurity and Law

Luca Tosoni (luca.tosoni@jus.uio.no)
Peter Davis (p.a.e.davis@jus.uio.no)

Agenda

- Introduction (Peter)
- Privacy and Data Protection
  - GDPR 1 year on (Luca)
  - GDPR Article 25 (Data Protection by Design/Default) (Peter)
  - GDPR Articles 32-34 (Security of Personal Data) (Luca)
- Cybersecurity
  - NIS Directive (Peter)
  - Cybersecurity Act (Luca)
  - Anti-encryption laws; Australian *Assistance and Access Act* (Peter)

Introduction

Topics

- Cybersecurity – CIA/NIS
- Privacy
  - Not restricted to ‘informational’ privacy
  - Freedom to / freedom from (US/EU perspectives)
  - See Koops et al., *A Typology of Privacy*
- Data Protection
  - Significant overlap with privacy and cybersecurity

What is regulation?

- Generally, an attempt to alter behaviour
- Note terminological distinction between EU Regulation (cf. Directive) and regulation more generally
- Hard law (e.g. legislation, case law)
- Soft law (e.g. standards, guidelines)
- Norms
- Lessig – laws, norms, markets, architecture

Difficulties with regulating cyberspace

- Technical / multidisciplinary
- Legally novel and complex
- Political
- Dynamic
- International
- Increasing prominence & ubiquity

Instruments

- General Data Protection Regulation “GDPR” (EU-2016/18)
- Directive on network and information systems “NIS Directive” (EU-2016)
- Regulation on ENISA and Cybersecurity Certification “Cybersecurity Act” (EU-2019)
- Assistance and Access Act (Australia-2018)

Why regulate the cyber?

- Why regulate at all?
- Why do we regulate at an EU level?
  - 'To improve the functioning of the internal market / digital single market'
  - Protection of fundamental/human rights
    - Privacy (Art. 7 Charter; Art. 8 ECHR)
    - Data Protection (Art. 8 Charter)
    - Security (Art. 6 Charter; Art. 5 ECHR)
    - Right to cybersecurity?
  - Protection of essential services (NIS Directive)
  - Capability sharing and economies of scale

General Data Protection Regulation
GDPR

GDPR Introduction

- Previous iteration: Data Protection Directive (1995)
- Material and territorial scope
  - When does the GPDR apply?
- Actors
  - Who has rights and/or obligations under the GDPR?
- Rights and Obligations

GDPR Scope

- Material Scope
  - Processing of personal data
    - Personal data = any information relating to an identified or identifiable natural person (data subject)
    - Processing = any operation or set of operations performed on personal data
- Territorial Scope
  - Processing of PD by an establishment of a controller/processor in the EU
  - Applies extraterritorially if the processing activities are related to:
    - the offering of good or services, even if free, to data subjects in the EU; or
    - the monitoring of behaviour that takes place in the EU

GDPR Actors

- Data Subject
  - Identified or identifiable person
- Controller(s)
  - Entity that (perhaps jointly*) determines the purposes and means of processing PD
- Processor(s)
  - Entity that processes data on behalf of the controller (e.g. cloud service provider)
  - “the controller shall only use processors providing sufficient guarantees to implement appropriate… measures” – Art 28
- Data Protection Authorities (and EDPB)

GDPR Rights/Obligations

- Data Protection Principles (Art 5)
  - E.g. lawfulness, fairness, transparency; data minimisation; purpose and storage limitation, information integrity (incl. security)
- Lawful basis for processing (Art 6)
  - E.g. consent, legitimate interest
- Information / access / rectification and erasure (Arts 12-20)
- DP by design/default (Art 25)
- Security (Arts 32-34)

GDPR – One Year On

GDPR: One Year On

- Key dates
  - Adoption: 27 April 2016
  - Entry into force: 26 May 2016
  - Application: 25 May 2018

- Regulation = harmonized rules/no national implementation
  - But, open clauses/some implementation required under the GDPR
    - All MS, but a few (e.g. GR, SL), adopted implementing laws

GDPR: One Year On

GDPR in numbers

- Awareness of GDPR
  - 67% of Europeans have heard of GDPR
- Awareness of DPAs
  - 57% of Europeans know of DPAs; 20% know which one is responsible
- Queries and complaints
  - Almost 150.000
  - Most common: telemarketing; promotional emails; CCTV
- Data breach notifications
  - Almost 90.000
- Total fines levied
  - €56 Million (until May 2019)

GDPR: One Year On

Main issues experienced by organisations in complying with the GDPR

- Considerable investments and workload
  - E.g documenting accountability; updating privacy notices
- Old legacy information technology systems
  - E.g. difficult to deal with access and erasure requests; data portability
- Many GDPR provisions are formulated broadly
  - E.g. what does processing ‘on a large scale means’?
- Proper implementation of information obligations
  - How detailed should a privacy notice be?
  - Meaningful explanation of automated-decision making
- Conditions for valid consent
- Controller/processor relationship

GDPR: One Year On

- EDPB/national DPA guidelines
  - EDPB: around 25 guidance documents published
  - National DPAs
    - Many: e.g. UK ICO guidelines on cookies
- Sanctions
  - Mainly about poor security measures (!)
  - Highest fine: *c.* €245 million
- Case law
  - Around 10 cases pending before the CJEU
    - Concern e.g. data transfer mechanisms; valid consent; territorial scope of de-referencing (right to be forgotten)

GDPR
Data Protection by Design and Default

Article 25 – DP by Design and by Default

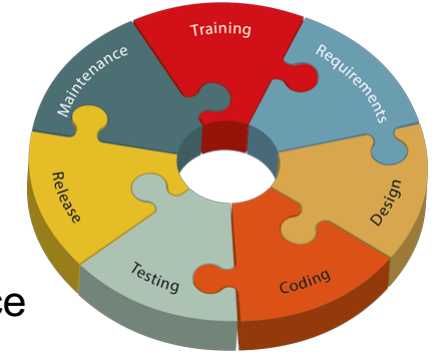
- What is it?
- To whom does it apply, and when?
- How does it relate to security (cf. privacy?)
- What is the difference between design and default?
- What does this mean on a practical level?

Article 25 – what?

- Imposes a duty on controllers to put in place technical and organisational measures to implement GDPR principles
- Qualified duty
  - "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks"
- Similar to Article 32 but duty applies when the controller determines the means of processing PD (i.e. at earlier stage than actual processing)

Article 25 – what types of measures?

- Technical
  - E.g. automatic deletion/anonymisation after certain period, "pseudonymisation",
  - Recital 78 – "with due regard to the state of the art"
- Organisational
  - From practices (such as admin access) to business strategy
    - Recital 78 - "In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design/default"
- Further guidance expected
  - Codes of conduct (Art 40)
  - European Data Protection Board opinions
  - Certification (Art 42)
  - Datatilsynet (Norwegian DPA) has given some guidance



Article 25 – design vs default

- Design = potentially broader
- Default = focus on data/storage minimisation
  - “the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.”
  - “such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.”

Article 25 - who?

- Ostensibly, just to controllers, for all processing activities
  - But note qualifications – the greater the risk, the more 'organisational and technical' measures must be considered (see also Art 35 Data Protection Impact Assessment)
- How much 'control' does the 'controller' actually have?
  - Parallels with supply chain risk?
- Recital 78 extends scope to 'producers' of products
    - "…producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."

Article 25 – so what?

- Article 25 measures may be considered under Article 83(2)(d) regarding fines
  - Note recent fine from Romanian DPA
    - €130,000 to Unicredit Bank for disclosing addresses and ID no.s to payment recipients
- Increasing prominence? Note Cybersecurity Act Recital 12
  - Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security by design').

GDPR
Security of Personal Data

GDPR: Security of Personal Data

Security obligations (Art. 32 GDPR)

- Apply directly to both controllers and processors (new!)
  - Sub-processors must be bound by contract to the same obligations
- Appropriate *technical* and *organizational* measures
  - Appropriate to the specific risks of the data processing
    - risk-assessment required
  - Non-exhaustive list of criteria to be taken into account
    - State of the art
    - Costs of implementation
    - Nature, scope, context and purposes of the processing
    - Likelihood and severity of risks
- Obligations of means, not of result

GDPR: Security of Personal Data

Examples of security measures

- pseudonymisation and encryption of personal data
- ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

GDPR: Security of Personal Data

Accountability

- Compliance may be shown by adhering to an approved code of conduct or cerification mechanism

Liability and fines

- Administartive sanctions up to €10 million or 2% of the total worldwide turnover
- Most of the sanctions for violatiations of the GDPR imposed so far concern poor security measures!
  - E.g. UK ICO proposed to fine British Airways £183.39 million (equivalent to €243.47 million) – equal to 1.5% of British Airways' annual turnover in 2017– for a violation of Art. 32
- Compensation for material and/or non-material damage suffered as a result of an infringement of Art. 32

GDPR: Data Breach Notification

- Obligation to notify serious data breaches (Arts. 33-34) (new!)
- What is a «personal data breach»?
  - Art. 4(12) GDPR
    - ‘personal data breach’ means 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
  - Key attributes of a breach
    - Violation of ‘security measures’
    - A *type* of security incident (i.e. one of the key elements of information security needs to be compromised)
    - Affects personal data

GDPR: Data Breach Notification

- What breaches should be notified?
  - Only breaches that are likely to result in a risk for to the rights and freedoms of natural persons (e.g., risk of physical, material and non-material damage)
- When?
  - Without undue delay (normally within 72 hours)
- What to notify?
  - Nature of personal data breach
  - Categories and approximate number of individuals affected
  - Name and contact details of DPO
  - Likely consequences
  - Mitigating measures
- To whom?
  - For controllers: DPA and (in case of high risks) persons affected
  - For processors: controllers

Cybersecurity Definitions

ITU Cybersecurity Definition

- Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
  - Availability
  - Integrity, which may include authenticity and non-repudiation
  - Confidentiality

Cybersecurity Act Cybersecurity Definition

- ‘cybersecurity’ comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;
- ‘cyber threat’ means any potential circumstance or event that may adversely impact network and information systems, their users and affected persons.

NIS Directive definition of ‘security of NIS’

- ‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

NIS Directive

NIS Directive - preliminary

- [A Directive] Concerning measures for a high common level of security of **n**etwork and **i**nformation **s**ystems across the Union
- Directive -> MS must implement the Directive themselves, so variances are permitted/expected.
- Purpose: to achieve a high common level of NIS security to improve the functioning of the internal market
  - Note no reference to right to security
  - Note national security not within competence of EU, so NIS is limited in terms of subject matter it can cover

NIS Directive – subject matter

- MSs must adopt national strategy on security of NIS
- Establishes Cooperation Group for info sharing/cooperation between MSs
- Creates a computer security incident response teams network (CSIRTs network) to increase trust between MSs
- Security and breach notification requirements for operators of essential services and certain digital service providers

NIS Directive – who?

- Operators of essential services
  - Energy, transport, banking, financial market infrastructures, health sector, drinking water, digital infrastructure (TLDs, DNS, IXPs)
    - Operators are notified by MSs (Art 5(1))
    - Art 5(2): services that are “essential for the maintenance of critical societal and/or economic activities”; rely on NIS; NIS incidents would have significant disruptive effects on service
- Digital service providers
  - Online marketplaces, search engines, cloud computing services
  - (except small enterprises)
- Notable absences
  - Social networks, telecommunications (subject to other rules)

NIS Directive Article 14 – OES – what?

- Incident notification
  - To CSIRTs/ competent authority (e.g. UK – ICO; UK Civil Aviation Authority)
  - "of incidents having a significant impact on the continuity of the essential services they provide"
    - "incident" = any event having adverse effect on security of NIS
    - "significant impact" = number of people, geographic spread, duration
      - Different test for digital services – "substantial impact"
- Security obligations
  - "appropriate and proportionate technical and organisational measures to manage the risks posed to the security" of NIS
    - Similar for digital services

NIS Directive – so what? Enforcement

OES

- Authorities can assess compliance *ex ante,* including audit powers
  - No evidence of non-compliance necessary
- Authorities may issue binding compliance instructions

DSP

- Authorities can assess compliance *ex post* when provided evidence of non-compliance
- Authorities may order remedy of non-compliance

Fines – depends on MS. UK max £17m; France max €125k. If personal data, GDPR fines may also apply.

Cybersecurity Act

Cybersecurity Act

- Regulation (EU) 2019/881
  - No implementation necessary at national level
- Entry into force
  - 27 June 2019 (with some exceptions)
- Main objectives
  - Strengthening ENISA (permanent mandate)
  - Establishing the first EU-wide cybersecurity certification framework

Cybersecurity Act

Cybersecurity certification

- What is certification?
  - Formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance
- Pre-Cybersecurity Act
  - Cybersecutiy ceritfication was quite patchy
    - a number of international initiatives, such as the so-called Common Criteria (CC) for Information Technology Security Evaluation (ISO 15408)
    - Various national certification schemes: often no mutual recognition
    - Market fragmentation and interoperability issues

Cybersecurity Act

European Cybersecurity Certification Framework

- No directly operational certification schemes, but a system (framework) for the establishment of specific certification schemes for specific ICT products/services
  - E.g. connected and automated cars, electronic medical devices, industrial automation control systems and smart grids

- Certificates issued under those schemes will be valid and recognised across all EU Member States

- Certification voluntary, unless required by sectoral legislation

Cybersecurity Act

Certification schemes

- The schemes will have to define, among other things, a number of specific elements setting out the scope and object of the cybersecurity certification, such as:
  - Categories of products and services covered
  - Detailed specification of the cybersecurity requirements (for example by reference to the relevant standards or technical specifications)
  - Specific evaluation criteria and methods,
  - Level of assurance they are intended to ensure (i.e. basic, substantial or high)

Cybersecurity Act

Process for the adoption of certification schemes

- ENISA will prepare the certification schemes will be prepared by ENISA, with the assistance of the European Cybersecurity Certification Group
- Commission will adopt the certification schemes by means of implementing acts
- National cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme will cease to apply from the date established in the implementing act adopting the scheme

Cybersecurity Act

Certification process

- Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services will be able to submit an application for certification of their products or services to a conformity assessment body of their choice

- Conformity assessment bodies must be accredited by an accreditation body