Queen Mary
University of London

EU Data Protection Directive: Basics Concepts

Professor Anne Flanagan
Centre for Commercial Law Studies
Queen Mary University of London

Multi-disciplinary Cooperation for Cyber Security, Legal and Digital Forensics Education Project

December 2014-March 2016

BIRMINGHAM CITY University

Queen Mary University of London

The Directive

- 95/46/EC
  - General directive
  - Scheme of:
    - rights
      - Data subjects
        - » Those natural persons identified or identifiable from personal data
    - obligations
      - Data controllers
        - » Those legal or other persons who determine the means and nature of processing
    - Duties and powers
      - Member States
        - » Usually those that must be designated to the national regulatory authority

Core concept: personal data

- Threshold issue for Directive
  - If not personal data, does not apply (other consequences: subject access, FOIA disclosure)
- Definition (Art 2(a))
  - Any information relating to an identified or identifiable natural person
    - Identifiable: who can be identified directly or indirectly by reference to:
      - An identification number or
      - To one or more factors specific to his identity:
        - » physical, physiological, mental, economic, cultural or social

Application

- All processing of personal data
  - By controller in EU
    - Public and private
    - Person who determines the means and purposes of the processing
      - Data Processor is one who follows orders of controller
  - Or done on equipment in EU
- Carve outs for: household processing, processing for national security, prevention or detection of serious crime

Household Processing?

- Lady has a website devoted to activities of her fellow church members
- Person has Facebook account with 500 ‘friends’
- Homeowner has CCTV camera outside his house

Personal Data?

- Date of birth
- Size 9 shoe
- First and last name
- Email address
- Car Make and Model
- Thermostat reading
- Job title
- Telephone number

Personal Data I

- Encompasses data regarding private and professional life

  See e.g.:

  - *Commission v Bavarian Lager* C28/08 P (2010)(names of those attending meeting with Commission comprised personal data under EU Regulation 45/2001 irrespective of whether privacy interests attached under Article 8 ECHR)
  - *Volker and Schecke* C 92/09 (2010)(EU publication of recipients of agricultural subsidies comprised personal data where recipients were natural persons)

Personal Data: Identifiable

- "Account should be taken of all the means likely *reasonably* to be used either by the controller or by any other person to identify the said person" Recital 26 (emphasis added)

Identified/Identifiable

- "Can a living individual be identified from the data, or, from the data and other information in the possession of, or likely to come into the possession of, the data controller?"

  UK ICO Guidance on determining what is personal data (2012)

  - Knowing the name of the person is not essential to 'identifying' person
    - E.g., Mary Smith alone does not serve to identify anyone

Personal Data?

Google v Vidal-Hall [2015] EWCA Civ 311)

- BGI collected by Google in Safari browser provided Google with browsing history
- Cookie identified IP address of user
- Google had two sets of data:
  - unique IP addresses,
  - websites visited, as well as geographic location, when available.
- Google did not link the data

Google v Vidal Hall

- Held: Personal data
- It could distinguish that individual from another; individuating one from a group
- Google knew unique IP address, when that person was in their 'virtual home'
- Did not matter whether the two sets of data were linked in fact

Durant v FSA

- *Durant v FSA* (CA 2003)(holding that personal data must be significantly biographical in that it has the individual as its focus being information that affects his or her privacy, whether in a personal or business capacity; not merely the mention of a name in agency's complaint file)
  - Likely basis for Commission proceedings against UK (not disclosed)
  - Very contextual analysis

UK and Personal Data

- Not overruled although several CA decisions do not follow and suggest that limited application
  - *Edem v ICO* (provided that context available to link name to particular individual, including job title, names are always personal data; *Durant* limited to particular factual scenarios where information requested is not "obviously about" an individual or clearly "linked to" them).

Art 29 WP Opinion on the concept of personal data

- All information concerning or which may be linked to an individual
  - Not to be 'unduly' restricted
    - Anticipate evolutions
    - Encompasses
      - objective (facts)(e.g., your blood type) and
      - subjective (assessments or opinions)(e.g., evaluation of your creditworthiness) information

Personal Data

- Three core concepts of how data may relate to an individual as personal data–
  - Content (information given about a person, eg, medical or employment data or info in smart chip),or:
  - Purpose (used to evaluate, treat or influence the status/behavior of an individual), or;
  - Result (where usage of information can affect someone's interests, e.g., use of GPS system can also serve to monitor speed, location, performance etc. of taxi driver)

Art 29 WP Opinion

- Directly (name or identifier)or indirectly identifiable (linkage or combination of distinguishing information
  - Keys, purpose to identify (graffiti 'tags' database)
    - 'reasonably likely' not mere theoretical possibility

Relating to: CJEU

C 141/12 *YS v Minister voor Immigratie* (2014)

Applicant for residence in Netherlands sought access to immigration file

Held:

- Information relating to an individual is personal data
- Analysis of lawyer concerning whether YS entitled to stay under law does not relate to YS, is only information about legal assessment of YS' situation
  - Otherwise access right to data becomes a right of access to documents

Anonymous Data

- Identify/Identifiable are tests of PD, therefore if does not identify individual, not within Directive
  - See Recital 26 ("…protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable")
    - MS to determine but Art 29 WP Opinion 05/2014 on Anonymisation Techniques
      - Case by case analysis that considers all the means likely reasonably to be used by controller or 3rd party

Personal Data: Anonymous Data

- Anonymisation of data:
  - Removing identifiers (direct and indirect- former alone is insufficient)
  - Substituting for identifiers and adding, changing or grouping data to preclude or blur patterns/ remove linkages/rescale data (e.g., randomization and generalization, noise, barnardisation)

Anonymisation

Test:

1. Can you single out an individual?
2. Can you link records to an individual?
3. Can information about an individual be inferred?

Continual assessment of techniques in light of linkage capabilities

UK ICO Code of Practice

- Risk management approach to assess re-identification– no perfect anonymisation
  - Considerations of: nature of other relevant info, possibility for significant harm
    - Consent may be advisable where borderline and risk of significant harm but ICO position that not required

Processing of Personal Data

All processing of personal within DPD is to be done only in accordance with its principles

- Any operation performable on/with personal data
  - Obtaining, storing, transmitting, recording and holding data, erasing or destroying, anonymizing it
  - Anything you can do with data

Principles (Fair Processing)

- Fairly and lawfully processed
- For specified and legitimate purposes
- Data must be adequate, relevant and not excessive for the purpose
- Not kept longer than needed for purpose and not further processed
  - Unless further legitimate basis

Data Processing Principles

- Accurate and up to date
- Technical and Organisational Measures against unauthorised access, loss or destruction of data
- Cannot be transferred outside EEA unless there is adequacy of protection for data

Legitimate Basis for Processing

Processing is legitimate only when:

1. pursuant to data subject's unambiguous consent

consent"

- "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."
- Unambiguous undefined

Or

1. If based on necessity as DPA provides:

Necessary Processing

- For performance of contract with data subject
  - or to take steps at the request of the data subject prior to a contract; or
- For compliance with a legal obligation of controller;
- To protect vital interests of data subject; or
- For performance of a task carried out in the public interest or in exercise of official authority; or
- For legitimate interests pursued by the controller or by third party or parties to whom the data are disclosed
  - except where these are overridden by the interests for fundamental rights and freedoms of the data subject.

Sensitive Data

- Narrower justifications for legitimate processing
  - Explicit consent
  - Fewer ‘necessary’ bases

What do you think is ‘sensitive’?

Sensitive Data

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life
- Member States can create additional exemptions from ban if safeguards and substantial public interest
  - Various rules, not harmonized
    - Nature of consent : some states consider that consent not possible
- Other special categories: eg, criminal history, national identifiers
  - Limited processing, e.g, database under control of national authority

Processing Sensitive Data

- May not be processed without explicit consent or more delimited bases of necessity, including
  - Employment law rights and obligations
  - Necessary to protect vital interests of data subject and incapable of consent
  - Certain legitimate processing by foundation, association or other non-profit-seeking body with a political, philosophical, religious or trade union aim.
    - relate solely to members of the body or to persons who have regular contact in connection with its purposes.
  - To establish or defend a legal claim
    - actual and really prospective claims

Data Controller

- Obligations for compliance apply to the data controller
  - The person or persons who determine the means and purposes of processing
    - May be joint
- Data processor performs processing under the supervision and control of the processor and pursuant to its instructions
  - Separate legal entity
  - Security according to law of processer MS
- Public and private entities
  - May have greater exemptions from compliance with principles for certain public interest processing

Boundaries

- Context
  - E.g., Social Networking (WP Opinion 163
    - SNS providers are consider ordinarily the controllers
      - Provide format and structure for user participation
        - » E.g., what information is collected, managing and deleting accounts
        - » What is shared/accessed by third party advertisers
    - Application providers providing apps that run along side/ within SNS and process personal data are also controllers when used by users
    - Users
      - Where processing is merely social, then consider within household exemption
        - » number of 'friends' may be a consideration
      - Where used as a platform beyond social, exemption does not apply
        - » E.g., where user is representing a company or
        - » to advance commercial, political or charitable goals

Boundaries

- Google Spain:
  - Newspaper account of old debt payment failure by lawyer continued to appear in top search results for lawyer's name
  - Is Google Spain the controller?

Boundaries

Search engines

- Google Spain
  - Determined means and nature of republication

Cloud providers

- Focus will be on whether provider has control and ability to process
  - Not merely fact that provides a facility

Big data analysers

- May not know what they are looking for but determine nature and extent of processing

Reforms

- Lack of harmonisation, clarity and legal certainty, difficulty in compliance among the key drivers of reform
- Principles to be adhered to but greater specificity
- Seeking one stop shop

Personal Data

- The Regulation's proposed definition of personal data is broader than that in the DPD. In addition to the DPD's factors, the Regulation presently includes:
- **location data**,
  - unique identifier or
  - one or more factors specific to the **physical**, **physiological**, **genetic**, **mental**, **economic**, **cultural or social or gender identity** of that person.

Article 2, Proposed GDPR as adopted by Parliament in March 2014.

Personal Data

- Recital 24: **IP addresses**, **cookies**, **radio frequency identification tags** should be included in the scope of the Regulation, **unless** those identifiers **do not relate to an identified or identifiable natural person**
- **Sensitive Data similarly broader, encompassing:**
  - **philosophical beliefs**, **sexual orientation** and **gender identity**, **trade-union activities**, **biometric data**, **administrative sanctions**, **judgements**, **suspected offenses.**
- See ibid, Article 9.

Consent

- Consent must be: **freely given**, **specific**, **informed and explicit indication of his or her wishes** by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.
- Burden of proof on controller

Article 4(8)Proposed GDPR as adopted in March 2014

Consent

To be purpose-limited

- lose its validity when the purpose ceases to exist or
- as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected

Article 7, Proposed GDPR as agreed March 2014

Obligations of Controller

- Notify processing

  To data protection authority
- Provide information to data subject
  - Who, what, why, and where of data processing
- Contracts with processors
- No 3rd country transfers
- Accountability of controller

Rights of Data Subjects

- To access data held by controller
  - In understandable format
- To have old, inaccurate data corrected or removed
- To object to processing
  - Direct marketing
  - That interferes with fundamental rights unless legitimate interests of controller outweigh
- To redress for breach of Directive

Reforms

- Right to port data to new controller
- Right to be forgotten (have data deleted)
- More accountability for data processor
- Appointment of DPO if over 250 employees
- Risk management approach
- Privacy by default; privacy by design
- Certifications, seals as evidence of compliance