

Directive 2016/680 Personal Data in Law Enforcement

Dr Mark Leiser FHEA FRSA

Assistant Professor

eLaw – Center for Law and Digital Technologies

Leiden University



This project is funded by the EU. This presentation has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this presentation are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

■ Background

- Law Enforcement Directive (LED) on protecting personal data processed for purposes of criminal law enforcement (EU 2016/680) entered into force on 5 May 2016
 - Complements Regulation EU 2016/679 General Data Protection Regulation (GDPR)
 - Right of individuals to protect personal data while guaranteeing high levels of public security
- Principles set out by Directive and practical consequences pursued by Member States put into shade of GDPR
- EU Parliament emphasizes 'package' approach, ensuring GDPR and Police DP Directive were dealt with in parallel
 - Political agreement was found in trilogue negotiations
- **Agreement included following points:**
 - **Broader scope of application**
 - Activities aimed at preventing, investigating and prosecuting criminal offences
 - Scope extended to cover prevention of threats to public (not national) security
 - **Data Subject Rights**
 - **Monitoring and compensation:** Rules aligned w/ GDPR to ensure same general principles apply
 - **Supervisory authority:** established in GDPR; Also deals with LED matters

■ Background

- EU Parliament adopted 1st reading position with amendments, including:
 - Importance of consistent rules across MS
 - High levels of data protection
 - Facilitating exchange of data between competent authorities of Members States (Recitals 4, 7)
 - Applicability of core DP principles into sector: lawfulness, fairness and transparency (Recital 26)
 - Right of every person not to be subject to measure that is based on profiling by means of automated processing except unless strictly necessary for the investigation of a serious crime or prevention of a clear and imminent danger (Recital 38)
 - Data subjects can receive compensation if suffered damage as consequence of processing not respecting rules
 - Appointment of a DPO to help competent authorities
 - Impact assessment to be carried out in cases when data processing entails high risk for a person's rights
 - Considered requirements regarding data protection 'by design and by default'
- EU Passenger Name Records Directive
 - Adopted on same day as data protection reform package



■ Scope

- Processing of personal data by “**competent authorities**” for purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties
 - If competent authority, then satisfies personal scope
 - But must also satisfy material scope, i.e. processing for the purposes of law enforcement
- Important: “competent authority” can only process for “Law Enforcement Purposes”
 - Border Control processing = GDPR applies
 - Criminal proceedings = LED applies
 - Rights already covered in criminal procedural law
 - National Security outwith scope of LED
 - EU law prohibits access by Intelligence services to DB
 - EuroDac
- Movement of such data between the EU Member States
 - Repeals Council Framework Decision 2008/977/JHA (Data Protection Framework Decision – DPFDD)
 - Decision was limited to processing of personal data transmitted or made available between Member States and further processing of such data as regards as well transfers to competent authorities in third Countries
 - Former did not include domestic data

■ Who are “competent authorities”?

- All organizations listed in national legislation
 - i.e. Schedule 7, UK Data Protection Act 2018
- Any other person if and to extent that person has statutory functions for law enforcement purposes
 - Trading Standards, Data Protection Authority
- If law requires personal data to be processed for law enforcement purpose, then organization required by law to process personal data is controller
- Grounds for processing are limited to:
 - Consent of data subject
 - Necessary for functions of competent authority
- Any processing carried out by a ‘competent authority’ which is not for primary purpose of law enforcement will be covered by GDPR
- Any processing not for law enforcement purpose (i.e. the Human Resource division of a police force) is subject to GDPR
 - Quiz: Is CCTV processing for a law enforcement purpose?
 - No – not if collected by a controller not classed as a “competent authority”



■ Key Points

■ Data collected by law enforcement authorities are (Article 4):

- Processed lawfully and fairly
- Collected for specified, explicit and legitimate purposes and processed only in line with these purposes
- Adequate, relevant and not excessive in relation to the purpose in which they are processed
- Accurate and updated where necessary
- Kept in a form which allows identification of the individual for no longer than is necessary for the purpose of the processing (time limits)
- Appropriately secured, including protection against unauthorized or unlawful processing
- Transparency requirements are not as strict, due to the potential prejudice to an ongoing investigation

■ Time Limits (Article 5)

- EU countries must establish time limits for erasing personal data or for a regular review of need to store such data

■ Individuals concerned ('data subjects') (Article 6)

- Law enforcement authorities must make distinction between data of different categories of persons:
 - Those for whom there are serious grounds to believe they have committed or are about to commit a criminal offence
 - Those who have been convicted of a criminal offence
 - Victims of criminal offences or persons whom it is reasonably believed could be victims of criminal offences
 - Those who are parties to a criminal offence, including potential witnesses

■ Key Point: Principles

- Most of focus of Directive is on whether processing is necessary
 - If processing is necessary for law enforcement purpose, then fairness provisions are negated if informing data subject would likely “undermine” law enforcement purpose
- Disclosures from one law enforcement purpose for any further law enforcement purpose by another controller is likely to be compatible
 - **First Principle:** Fairness and lawfulness are well established requirements of data protection law; Any processing carried out for law enforcement purposes must be necessary
 - **Second Principle:** collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
 - **Third Principle:** adequate, relevant and not excessive in relation to the purposes for which they are processed
 - **Fourth principle:**
 - Requires facts kept separate from opinions
 - Distinction between subjects, convicted, victims and witnesses
 - Every reasonable step must be taken to ensure personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay
 - **Fifth principle:** Requires appropriate time limits must be established for periodic review of need for continued storage of personal data for any of law enforcement purposes

■ Key Point: Principles

- How does this differ from the GDPR?
 - **Principle 1:** Reduced 'transparency' requirements
 - Standards for consent are not as strict
 - **Principle 4:** Requirement for categorization of data subjects: victims, witnesses, suspects, offenders
 - Requirement to distinguish whether data is fact or of personal assessment/opinion
 - Logging: Requirement to keep logs of processing operations in automated processing systems
 - Include log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies
- International
 - Procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure compliant
- Sensitive processing
 - More categories than in UK's former DPA 1998, including genetic/biometric data

■ Sensitive Data

- Certain conditions
 - Necessary for judicial and statutory purposes – for reasons of substantial public interest
 - Necessary for the administration of justice
 - Necessary to protect the vital interests of the data subject or another individual
 - Personal data already in the public domain (manifestly made public)
 - Necessary for legal claims
 - Necessary for when a court acts in its judicial capacity
 - Necessary for the purpose of preventing fraud
 - Necessary for archiving, research or statistical purposes
- **'Strictly necessary'**
 - Processing has to relate to a pressing social need
 - Must not be able to achieve it through less intrusive means
 - If can achieve purpose by some other reasonable means
- **Threshold of consent**
 - Consent of data subject can never *in itself* constitute legal ground for processing of special categories of data in context of Directive

- **Processing special categories of data**
 - Article 8 (lawfulness of processing) & Article 10 (processing special categories) must be read together
 - Processing special categories of data, if not foreseen by EU law, always requires specific legal basis in national law
 - Specific legal basis has to meet additional requirements setup by Article 10 LED
 - 10(b) illustrates a situation in which vital interests of DS require processing special categories of data
 - 10(c) illustrates situation where DS voluntarily relinquishes protection of DS by making sensitive data public
 - Strict necessity –
 - DRI Ireland: *“so far as concerns the respect for private life, the protection of that fundamental right requires, according to the Court’s settled law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary”*

■ Rights

- **Individuals have right to have certain information made available to them including:**
 - Name and contact details of the competent authority which decides the purpose and means of the data processing
 - Why their data is being processed
 - Right to launch a complaint with a supervisory authority and the contact details of the authority
 - Existence of right to request access to and correction or deletion of personal data & right to restrict processing of their personal data
- **Data Breaches**
 - Procedures to identify, manage and investigate a breach
 - Processes in place to determine whether you need to report the breach to the DPA, based on the risks to individuals' rights and freedoms
- **Data protection by design and DPIAs**
 - Data Protection Impact Assessments mandatory where processing is likely to result in a high risk to rights, freedoms of individuals
 - New code planned, but existing one provides relevant guidance
 - DPA will deploy systems for formally checking DPIAs
 - New requirements for data protection by design
 - DPbD for IT infrastructure & any procured architecture (time limits, automatic deletion, systematic periodic review, anonymization, automatically limiting access to PD, and/or specific categories of data, deployment of masking, pseudo)
- **Data Protection Officers**
 - Role of DPO will be key element of ensuring accountability and governance
 - Essential part of DP reforms

■ Right of Access/Deletion

- DS have rights of access to personal data, rectification, erasure, restriction
- Rights negated if satisfying right:
 - Obstructs an official/legal inquiry, investigation or procedure
 - Prejudices the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
 - Jeopardizes public security, national security or the rights and freedoms of others
- Requirement of accuracy should not appertain to accuracy of statement but merely to the fact that a specific statement has been made (Recital 30)
- Rules similar to Freedom of Information 'neither confirm nor deny' frameworks
- DPA can verify whether exemption is properly applied

■ Security

- Principle applies to ALL processing of personal data for a law enforcement purpose
- For automated processing, each controller and processor must:
 - Do evaluation of risks (DPIA)
 - Prevent unauthorized processing or unauthorized interference w/ systems used in connection with it
 - Ensure possible to establish precise details of any processing that takes place (logging requirements)
 - Ensure systems function properly and may, in the case of interruption, be restored
- Ensure stored personal data cannot be corrupted if system used in connection w/ processing malfunctions
- National authorities must take technical/organizational measures to ensure level of security for personal data that is appropriate to risk
- Where data processing is automated, a number of measures must be put in place, including:
 - Denying unauthorized persons access to equipment used for processing (logging)
 - Preventing unauthorized reading, copying, changing or removal of data media
 - Preventing unauthorized input of personal data and unauthorized viewing, changing or deleting of stored personal data

■ Data Transfers

- Data transfers to “comparable” law enforcement agencies in Third Countries for law enforcement purposes can occur when:
 - An adequacy decision exists for that country
- When no adequacy decision?
 - Alternative safeguards for transfer (i.e. binding contract or the organization transferring can assess adequacy); #Brexit option
- When no safeguards or adequacy decision?
 - When special circumstances apply for transfer to the Third Country (e.g. vital or legitimate interests of data subject; serious security threat)
- In both cases, transfer must be fully documented
 - i.e. date, time, justification for transfer, details of recipient, etc.

■ Borders, #Brexit and Adequacy Agreements

- Without an adequacy agreement :



YES UK businesses want to store and process data in the EU/EEA



Cannot process the data of EU/EEA data subjects in the UK

■ Example:

- UK based DC will not be able to 'process' data from EU/EEA data subjects
- Only solution if business trades with those people is to move operation to EU/EEA
 - If no adequacy agreement, must employ Standard Contractual Clauses or Binding Corporate Rules with EU entity?
 - NB forthcoming FB Ireland challenge on SCC, leaving only
- Law enforcement data sharing will take a double hit
 - Not only will a lack of adequacy agreement under the Law Enforcement Directive end access to essential databases
 - Movement of commercial data into EU27 will make access to that data much harder
- Despite numerous promises UK no access to live data from Schengen Information Systems databases
 - Will not be able to assess the risk of EU citizens entering the UK, ironically UK had stronger border controls while in EU



