INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

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.

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM

INFORM

Background

- Law Enforcement Directive (LED) on protecting personal data processed for the purpose of criminal law enforcement (EU 2016/680) entered into force on 5 May 2016
  - Complements Regulation EU 2016/679 General Data Protection Regulation (GDPR).
- Aims to protect right of individuals to protection of their personal data while guaranteeing a high level of public security
- Principles set out by Directive and their practical consequences for various policies pursued by Member States were put into shade of GDPR
- Parallel Approach: EU Parliament emphasizes 'package' approach, ensuring GDPR and DP Police Directive were dealt with in parallel
  - Political agreement was found in trilogue negotiations.
- **Agreement included following points:**
  - **Broader scope of application:** in addition to covering activities aimed at **preventing**, **investigating** and **prosecuting** criminal offences, scope has been extended to cover prevention of threats to public (not national) security
  - **Rights**: Data subjects can receive compensation if suffered damage as consequence of processing that has not respected rules
  - **Protection of rights**: new Directive provides for appointment of a DPO to help competent authorities
  - **Monitoring and compensation:** Rules aligned with GDPR in order to ensure that same general principles apply.
  - **Supervisory authority:** established in GDPR also deals with matters falling under LED

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.

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM

INFORM

Legislative background

- Commission presented a proposal for a Directive on processing of personal data for the purposes of police and judicial cooperation in criminal matters (DP police directive)
- Aim of new rules is to improve and facilitate common work of police forces in exchanging information, and help fight crime more effectively
- Directive sets out standards for processing of data of people who are under investigation or have been convicted, when authorities exchange files, nationally or transnationally
  - e.g. specific purpose of processing data, duration of data retention and the rights of the people concerned
- Directive aims to contribute to building an area of freedom, security and justice with high level of data protection (DP), in accordance with EU Charter of Fundamental Rights.
  - Processing of data for law enforcement must comply with principles of necessity, proportionality & legality, with appropriate safeguards for individuals
  - Oversight and effective judicial remedies should be ensured by independent national DP authorities

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.

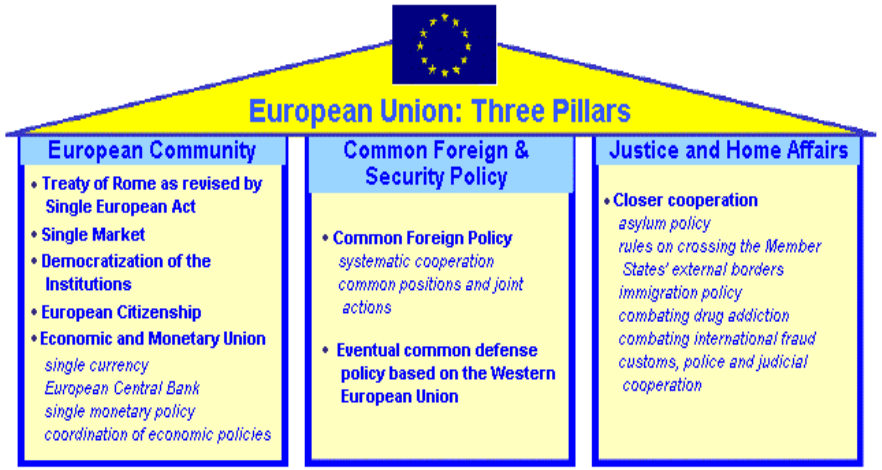
How does legislation fit together?

Legislative Background

- Reasoning: EU Parliament adopted 1st reading position on 12 March 2014, with several amendments, including:
  - Importance of consistent rules across MS, high level of data protection, facilitating exchange of data between competent authorities of Members States (Recitals 4, 7)
  - Applicability of core DP principles in this 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 if it is strictly necessary for the investigation of a serious crime or the prevention of a clear and imminent danger (Recital 38)
  - Impact assessment to 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 PNR Directive
  - Adopted on same day as data protection reform package

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.

- Scope
  - If competent authority, then satisfies personal scope
  - Must also satisfy the material scope, i.e. processing for the purposes of law enforcement
    - 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

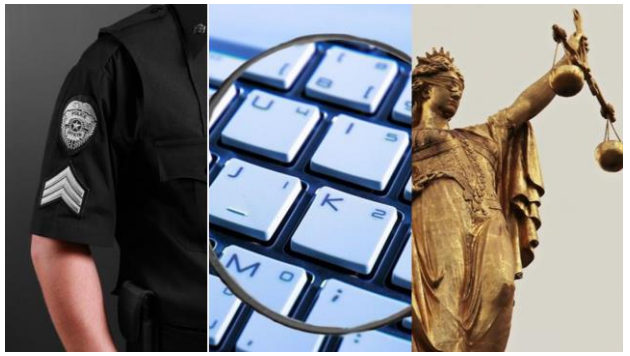


- Competent authority can only process for LE purposes

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.

- **Scope continued:**
- Processing of personal data by **"competent authorities"** for the purposes of the **prevention, investigation, detection or prosecution** of criminal offences or the execution of criminal penalties
  - Collectively known as the **"law enforcement purposes"**
- Free movement of such data between the EU Member States
  - Repeals Council Framework Decision 2008/977/JHA (Data Protection Framework Decision – DPFD)
    - 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.
    - Did not include domestic data

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.



- **"Competent Authorities"**
  - Any processing carried out by a 'competent authority' which is not for the primary purpose of law enforcement will be covered by GDPR
  - Any processing *not* for a 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"
- **Who are "competent authorities"?**
  - All organizations listed in the national legislation (i.e. Schedule 7, UK Data Protection Act 2018)
  - Any other person if and to the extent that the person has statutory functions for law enforcement purposes
    - Trading Standards, DP Authority
  - If the law requires personal data to be processed for a law enforcement purpose, then the organization that is required by law to process the personal data is the controller
  - Grounds for processing are limited to (a) consent of the DS, (b) necessary for the functions of competent authority

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.

- **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; and
    - 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.

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.

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM

INFORM

Key Points

- **Directive requires that 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 the personal data or for a regular review of the need to store such data.
- **Individuals concerned ('data subjects') (Article 6)**
  - Directive requires that law enforcement authorities make clear distinction between data of different categories of persons including:
    - 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.

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.

Comment on Principles

- Most of the focus of the 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**: Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.
  - **Fourth principle**: requires facts separate from opinions and distinction between subjects, convicted, victims and witnesses and every reasonable step must be taken to ensure that 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 the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes

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.

Key Points

- 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 requirements to record metadata for automated processing systems
- Logging: requirement to keep logs of processing operations in automated processing systems.
  - Include a 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 that they are compliant
- Sensitive processing
  - More categories than in the DPA, including genetic or biometric data.

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.

- Processing special categories of data
  - Article 8 (lawfulness of processing) and 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 the vital interests of the DS require the processing of 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*"

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.

Rights

Rights: Information available or provided to data subject

- Individuals have the right to have certain information made available to them by the law enforcement (i.e. data protection) authorities including:
- the name and contact details of the competent authority which decides the purpose and means of the data processing;
- why their data is being processed;
- the right to launch a complaint with a supervisory authority and the contact details of the authority;
- the existence of the right to request access to and correction or deletion of their personal data as well as the 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

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.

- Data Controller Obligations
  - Categorization: Directive requires that law enforcement authorities make clear distinction between data of different categories of persons including (Recital 31):
    - 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

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.

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

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.

Rights

- DS have rights of access to personal data, rectification, erasure, restriction
- Rights negated if satisfying the 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

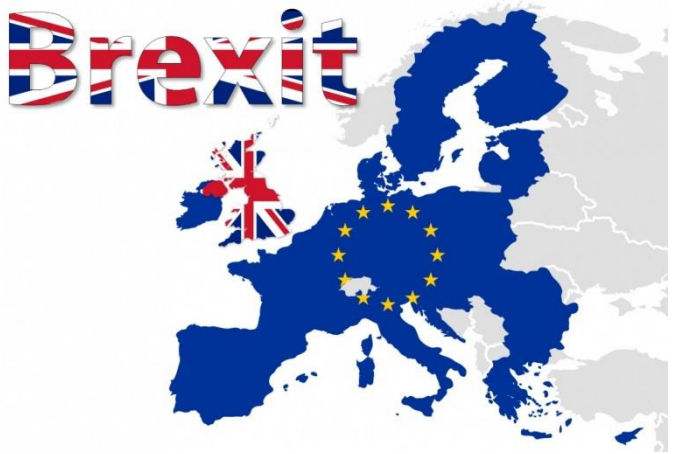
This project is funded by the EU. This presentation has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this presentation are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

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 the 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 the 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.)

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.

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM



- **Borders, #Brexit and Adequacy Agreements**
  - Without an adequacy agreement :

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

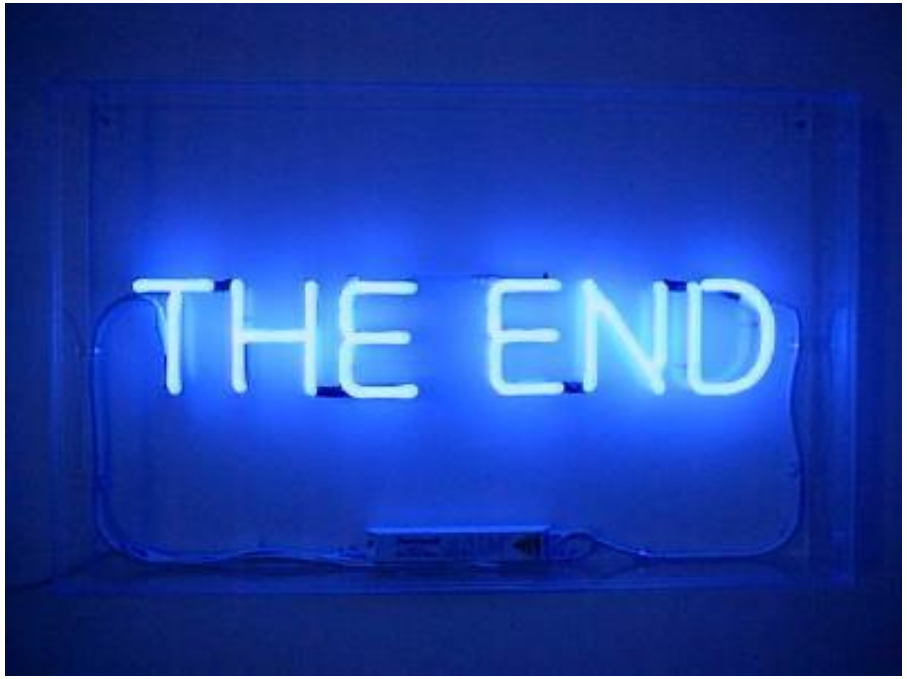
Cannot process the data of EU/EEA data subjects in the UK

- **Example:** A 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 the 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 still will not have 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

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.

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM

INFORM



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.