

# European Data Protection

## Structure, substance and challenges

Dr. David Erdos  
Faculty of Law  
University of Cambridge



# Overview

- Development and Current Structure
- Key Terms/Scope
- Substance and Scientific Derogations
- Conclusions

# EU Data Protection: Development



- **Emergence:** Prompted by **amorphous fears** which **computerization** posed to **privacy and integrity**.
- **Trans-European Spread:** Spurred by threat which national regimes posed to **free flow of information**.
- **Greater harmonization** over time (Resolutions to Convention to Directive to promised Regulation)
- But area remains dominated by complex mixture of **national** and **EU** norms.

## EU Data Protection: Structure

- **Pan-EU framework** in general terms in **Treaty** but more specifically in **Data Protection Directive 1995**.
- Directive is “**arms-length**” – must be transposed into local law and grants **flexibility** to **Member States**.
- **Which law(s) must be followed?** This depends on which **controller(s)** is (are) deemed responsible for the **processing of personal data** and where they are **based**.

# EU Data Protection: Key Terms

- **Controller**

**Anyone** who (either **alone** or **jointly** or **in common** with others) **determines** the **purposes** for which and the **manner** in which any **personal data** are, or are to be **processed**. (A. 2)

- **Processing**

Carrying out **any operation** or set of operations on data. (A. 2)

Will be covered if it involves a **digital device** or a **structured manual file** (A. 3 (1)).

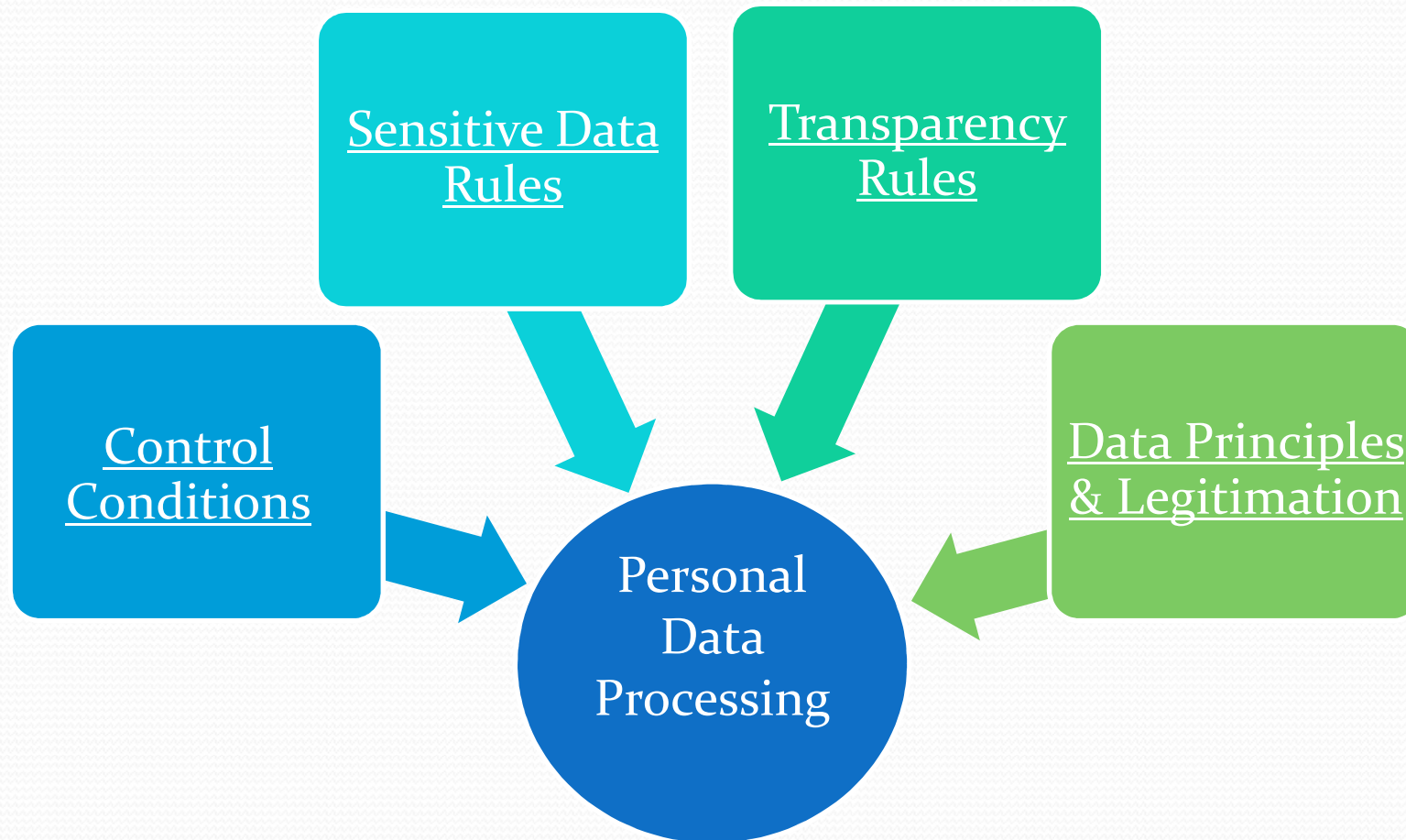
## EU DP: Personal Data

**Any** information **relating to** an **identified** or **identifiable** natural person. (A. 2)

- **Identified: direct** (e.g. name) or **indirect** (e.g. image)
- **Identifiability** covers situations where possible to identify by reference to **other information**.

*“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)*

# Wide Default Substantive Standards



N.B. There is a heavy overlap between many of these provisions

## EU DP: Scientific Derogations

- Directive **glosses** a limit number of special provisions in favour of “**scientific**” processing.
- Also suggests **general derogations** (e.g. sensitive data rules (Recital 34)) may be apposite in this context.
- **Art. 8:** Lifting of sensitive data ban
  - [For reasons of **substantial public interest**]
  - Subject to provision of **suitable [specific] safeguards**
  - Should be **notified** to the **European Commission**.
- **Art. 13:** Limits of wide range via legislative measure where necessary to safeguard “... *rights and freedoms of others*”.



## Five Data Principles (A. 6)

Personal data must be

1. Processed fairly and lawfully;
2. Stored for **specified** and **legitimate** purposes and not used in a way **incompatible** with those purposes;
3. adequate, relevant and **not excessive** in relation to the purposes for which they are stored;
4. accurate and, where necessary, kept up to date;
5. preserved in a form which permits **identification** of the data subjects for **no longer than is required** for the purpose for which those data are stored.

# Legitimacy and Compatibility

- **Legitimacy:** must meet an **A. 7 criteria** e.g.

- *The data subject has **unambiguously** given his **consent***
- *Processing is **necessary for legitimate interests** unless overridden.*

- **Compatibility:**

- **Presumption** that scientific purposes **not incompatible** so long as follow suitable safeguards in national law. Cf. **Recital 29:**

*“these safeguards must **in particular rule out** the use of the data in support of **measures or decisions** regarding any particular individual”*

## Transparency Notice: Direct Collection (A. 10)

Controllers must ensure data subjects have information as to:

- (a) The **identity** of the controller;
- (b) The **purposes** of the processing for which the data are intended
- (c) Any **further information** which, having regard to the specific circumstances, are necessary to guarantee **fair processing**, such as
  - The **recipients** or categories of recipients of the data,
  - Whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  - The existence of the right of access to and the right to rectify data concerning him

## Transparency Notice: Indirect Collection (A. 11)

Controllers must ensure data subjects have information as to:

- (a) The **identity** of the controller;
- (b) The **purposes** of the processing;
- (c) Any **further information** which, having regard to the specific circumstances, are necessary to guarantee **fair processing**, such as
  - The categories of data concerned
  - The recipients or categories of recipients
  - The existence of the right to access to and the right to rectify the data concerning him.

- This duty will not apply if constitutes a **disproportionate effort** and follow **safeguards** laid down in national law.
- For example, in **Italy** collection from third parties requires **general publicity** and **DPA notification**.

## Transparency: Right of Access etc. (A. 12)

*“at reasonable intervals and without excessive delay or expense:*

- *confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him in an intelligible form of the data undergoing processing and of any available information as to their source.”*

Linked right to have data **deleted**, rectified or **blocked** if legal violation (especially if data is inaccurate)

- Approx. ½ Member States provide some kind of scientific derogation is set out from subject access in local law.
- For example, in **Italy** can refuse if **disproportionate effort** but all non-public data stored must be **de-identified**.

## Sensitive Data Rules (A. 8)

- Specifically protects data revealing/concerning/relating to

*• racial or ethnic origin, • political opinions • religious or philosophical belief • trade union membership • health or sex life • offences, criminal convictions or security measures*

- Default rule is **ban** on private sector processing although generally **lifted** if:
  - Explicit **consent** of the data subject or
  - Information manifestly **made public by data subject**.
- Approx. ½ Member States provide for **scientific lifting** of this ban but often subject to **onerous conditions**.

## Control Conditions: Data Security

*“Member States shall provide that the controller must implement **appropriate measures** to protect personal data against ... **unlawful** forms of **processing**.”*

*Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security **appropriate** to the **risk** representing by the **processing** and the nature of the data to be protected.”*  
(A. 17 (1))

- Generally **risk-based** open textured approach.
- But coupled with **detailed rules** especially as regards the use of any data **processor** (i.e. entity processing on behalf of controller).

## Control Conditions: DPA Notification (A. 18)

- General out obligation to **notify** DPA of *inter alia*:
  - Controller's name and address
  - Purposes of processing
  - Categories of data
  - Potential categories of recipient
  - Proposed transfers to third countries
  - Security measures
- All but the last must be placed on a **public register**.



## Controls: Third Country Transfer (A.25-26)

“1. The Member States shall provide that the **transfer to a third country** ... may take place **only if** ... the third country in question ensures an **adequate level of protection**.

2. The adequacy of the level of protection afforded by a third country shall be assessed **in the light of all the circumstances** surrounding a data transfer operation or set of data transfer operations” (Art. 25)

- **(Qualified) presumption** not applicable where e.g.
  - Unambiguous **consent**,
  - Necessary on **important public interest** grounds,
  - Commission certified **contractual clauses**,
  - **State authorization** of safeguarded transfers.



## Conclusions

- **EU Data Protection** constitutes something of a **labyrinth** especially for the unwary.
- Provision of **transparency notices** and crafting of protective **safeguards** are clearly advisable.
- In principle, it **should not prevent** the sharing and use of peer review data for **scientific purposes**.