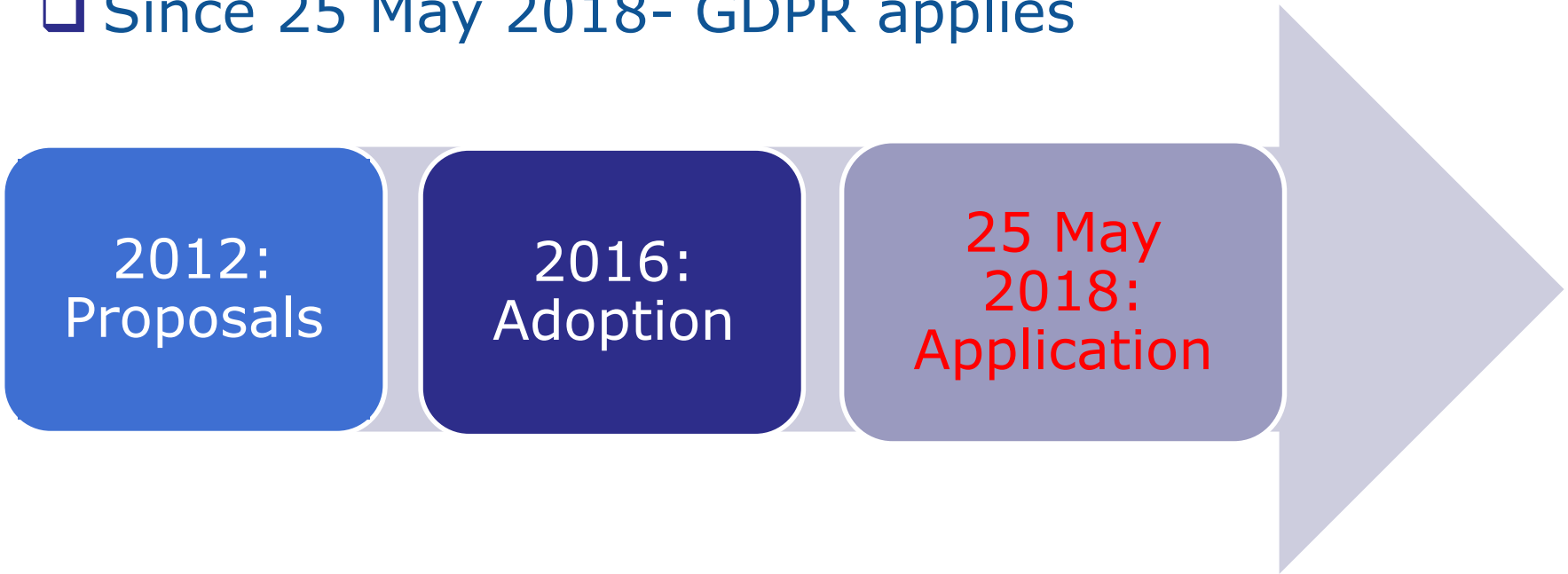
General Presentation on Data protection- ELRA

24 May 2019

DG JUSTICE and CONSUMERS

The EU Data Protection Reform Package: timeline

- General Data Protection Regulation (GDPR)
- 2016-2018 Transition period
- Since 25 May 2018- GDPR applies



Why a new European framework for Data Protection?

- **Technology developments and globalisation:** addressing the challenges and seizing the opportunities of the digital economy

- **Constitutionalisation of the fundamental right to data protection** (Lisbon Treaty)

- **Fragmentation of legislative framework** (different transposition of Directive 95/46/EC into national laws)

A harmonised and simplified framework

- **One single set of data protection rules for the EU** (Regulation)
- **One interlocutor and one interpretation** (one-stop-shop and consistency mechanism)
- **Creating a level playing field** (territorial scope)
- **Cutting red tape** (abolishment of most prior notification and authorisation requirement), including as regards international transfers

Who does what under the GDPR?

- Role of COM: guardian of the treaties; dialogue with MS, DPAs, stakeholders to ensure all actors are ready; grants; communication toolkit

- Central role of enforcers of GDPR: DPAs and EDPB

- Legal advice in individual cases: DPO, in-house lawyers; DPA for general indications

Key concepts and principles

- **Evolution rather than revolution**: basic architecture and core principles are maintained (principles, legal bases, concept of personal data)

- **Recital 72 Dir 95/46, taken up in Art 86 GDPR**

- Definition of personal data:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- **Article 29 Working Party Opinion 4/2007 on the concept of personal data - WP 136 (20.06.2007)**

Definition of: Processing (Art.4(2))

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Personal data protection principles (Art.5)

- Fair, lawful, transparent processing
- Purpose limitation
- Data minimisation
- Data accuracy
- Storage limitation (data retention)
- Accountability

Legal bases for processing (Art.6)

- Consent – new standard: "clear affirmative action" (silence or inactivity – no longer valid consent)
- Contract
- Vital interests of the data subject
- Legal obligation to process (EU law or national law)
- Exercise of public authority
- Legitimate interests of the controller

Art.9: Processing of special categories of personal data

Examples: Personal data revealing racial/ethnic data, political opinion, religious or philosophical beliefs, trade union membership

General Rule: such processing is prohibited;

Derogation: List in Paragraph 2

Explicit consent; reasons of substantial public interest; archiving purposes in the public interest, scientific or historical research purposes, statistical purposes,

Art 9(2)(d) Special Categories of Data

Art 9(2)(d):

processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or ***trade union aim*** *and on condition that the* ***processing relates solely to the members or to former members*** *of the body or to* ***persons who have regular contact*** *with it in* ***connection with its purposes*** *and that the personal data are* ***not disclosed outside that body without the consent of the data subjects***

An updated set of obligations

- Obligations graduated depending on the nature and potential risks of processing operations (**risk-based approach**):

- DPO
- DPIA
- Data breach notification
- Role of codes of conduct and certification
- Stronger rights, clearer obligations, **more trust**

Rights of individuals ("data subjects")

Clearer rights for data subjects

- Transparency, clear, accessible language
- Right of information
- Right of access
- Right to correct, delete, block
- Right to object
- Right not to be subject to automated decision making
- **New right**: right to portability; communication of data breach to data subject

Information (Art. 13-14)

To be provided **at the time** when personal data are obtained

- Identity and contact details of the controller (+DPO)
- Purposes of processing and legal basis
- Recipients or categories of recipients of the data
- Time limit for storing data
- Rights of individual, including complaint to a DPA
- Whether there is automated decision-making including profiling

Right of access (Art.15)

- **Confirmation** as to whether or not personal data concerning him or her are being processed
- **Copy** of the data undergoing processing
- **Information** about purposes of the processing, categories of personal data concerned, recipients, time-limit for storage, rights of individuals, logic involved in automated decision-making

- Can be exercised at regular intervals, free of charge for first copy – for any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs

Right to correct, delete, restrict (Art.16-19)

- **Rectification** of inaccurate of incomplete personal data
- **Deletion** of data that are no longer necessary for the purposes, when individual withdrew consent, or data have been unlawfully processed
- **Marking (restriction of processing)** of the data to verify accuracy or objection, or instead of deleting them at request of the individual

Right to portability (Art.20)

- Right **to receive the personal data** concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format
- And **to transmit** those data to another controller

- Right can be exercised where data were collected based on consent or on a contract, and data are processed by automated means

Right to object (Art.21)

- Right to object on grounds relating to the person's particular situation, where processing is carried out by a public body for the performance of its tasks or for the legitimate interests pursued by the controller

- Right to object to direct marketing

Right not to be subject to automated decisions (Art. 22)

- no decision solely based on automated processing with legal effects or similarly significantly affecting individuals unless
    - explicit consent
    - contract
    - EU or national law with safeguards

For contract and consent – possibility to obtain human intervention, to express point of view and to contest the decision.

International transfers of personal data (CH.V)

1. Clear rules defining **when EU law is applicable** (including to operators established outside of the EU)
2. A **renewed and diversified toolkit** for international transfers

- Precise and detailed *criteria for adequacy decisions*, possibility of *partial or sector-specific* adequacy, new possibility to adopt *adequacy decisions in the law enforcement* sector
- *Simplification* (abolishment of prior notification/authorisation) and *expanded possibilities of use* of other tools for transfers (standard contractual clauses, BCRs)
- Introduction of *new tools* (e.g. certification mechanisms, approved codes of conduct)

A modern governance system

- **Better equipped DPAs and better cooperation amongst them** (e.g. joint investigations)
- **A new decision-making process for cross-border cases** (the consistency mechanism)
- The creation of the **European Data Protection Board** (guidance and dispute settlement)
- **Credible and proportionate sanctions** (2/4% of global turnover in light of nature, duration, gravity etc. of the violation)
- **Art 83(7) Fines on public authorities- MS prerogative**

Powers

Supervisory Authorities have:

- **Advisory Powers** (advise controllers, issue opinions…)
- **Investigative powers (**order to controller/processor to provide information; carry out investigations; obtain access to personal data from the controller);
- **Corrective powers** (issue: warnings, reprimands, order controller to comply with data subject request to exercise rights; order controller to communicate data breach; temporary/definitive ban; fines)

General conditions to impose administrative fines

Fines need to be **effective, proportionate** and **dissuasive**,

GDPR provides list of factors (11) to be considered by the SA before imposing fine (nature, gravity, duration of infringement, intentional or negligent character, any action taken to mitigate damage suffered to data subject, degree of co-operation with SA, manner in which infringement became known to SA etc)

Since May 2018: Way forward

- COM is analysing the MS legislation specifying certain GDPR clauses;
- The EDPB has issued and will continue issuing guidelines
- COM will continue consulting the multi-stake holder expert group;
- COM will organise stocktaking event on 13 June 2019
- COM will submit an Evaluation report by 25 May 2020

Thank you very much for your attention!

Questions, comments?