A Modern European Data Protection Framework

These slides accompany the explanation of the acquis to Albania and North Macedonia and can only be used for that purpose. Their content is subject to further development of the acquis and interpretation by the Court of Justice of the European Union

European framework for Data Protection

- Art. 8 of the Charter of Fundamental Rights
- Art. 16 of the Treaty on the Functioning of the EU
- General Data Protection Regulation 2016/679
- Law Enforcement Directive 2016/680
- Case law

Why a new EU framework for data protection?

- **Technological developments and globalisation:** Trust comes from high data protection standards, backed by a system of individual rights and robust enforcement

- **Data protection as a fundamental right**

- **Fragmentation of legislative framework** (different transposition of the previous Data Protection Directive into national laws)

Main objectives and major changes

a. **RULES FIT FOR THE DIGITAL SINGLE MARKET (a harmonised and simplified framework)**

b. **PUTTING INDIVIDUALS IN CONTROL OF THEIR DATA (an updated set of rights and obligations)**

c. **A MODERN DATA PROTECTION GOVERNANCE**

a. 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 requirements), including as regards international transfers

b. An updated set of rights and obligations

- **Evolution rather than revolution**: basic architecture and core principles/obligations/rights are maintained
- **Putting individuals in better control of their data…** (e.g. consent to be given by clear affirmative action, better information about data processing)….
- **…including through the introduction of new rights** (e.g. right to portability) and **obligations** (e.g. data breach notification)
- Obligations graduated in function of the nature and potential risks of processing operations (**risk-based approach:** DPO, DPIA, data breach notification)
- Stronger rights, clearer obligations, **more trust**

c. 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** (max. 2/4% of global turnover in light of nature, duration, gravity etc. of the violation)

Impact on economy

USER TRUST: BASIS FOR DIGITAL ECONOMY

- Protection and security of data are the main concerns of users going online around the world
- Strong protections/control over data ensure trust

PRIVACY AS A SELLING POINT

- Being trusted constitutes competitive advantage
- Giving value to technology leadership
- Data protection is sound business practice: incidents can seriously harm reputation (Yahoo, Equifax, Facebook/Cambridge Analytica, …)
- Mark Zuckerberg: 'This is a major trust issue …'

Impact on companies

TAKING STOCK OF ONE'S DATA

- GDPR requires companies to analyse which data they collect and how they use it
- Helps companies to avoid unnecessary collection of data and to better use the data they hold

NEW MARKET OPPORTUNITIES FOR PRIVACY-FRIENDLY TECHNOLOGIES

- Privacy by design encourages innovative ways of strengthening data protection
- Innovation can reduce "regulatory burden" (risk-based approach, technological solutions)

Legal certainty

SIMPLIFICATION AND HARMONISATION

- Harmonised set of rules and coherent application across the EU enhances legal certainty

- Cutting red tape and thus compliance costs, more reliance on accountability and co-regulation

Global dimension

FACILITATING GLOBAL BUSINESS OPERATIONS

- GDPR represents global trend: typical features of a modern data protection law
- Compliance greatly facilitates access to any data market in the world
- Multinationals increasingly embrace GDPR as international standard
- Opens up new market opportunities for GDPR compliance tools, services, etc.

International transfers

ADRESSING THE CHALLENGES OF GLOBALISATION

- Personal data is being **transferred across an increasing number of borders** and stored on servers in multiple countries
- **Trade** relies more and more on personal data flows
- These transfers **should be facilitated, forced localization is counterproductive**
- The **protection should travel with the data**!
- **Convergence as trade facilitator**: Promoting high standards of data protection contributes to free, stable and competitive commercial flows

DIRECT APPLICATION VS. INTERNATIONAL TRANSFERS

- **Territorial scope of application** (Article 3 GDPR): no extra-territorial application but "effects-based"

  Foreign companies processing data of Europeans directly fall under the GDPR if they:

  - process data in the context of the activities of an EU establishment
  - target the EU market by offering goods or services to European customers or monitoring their behaviour

- **International data transfers** (Chapter V of GDPR)

International strategy

DIVERSIFIED TOOLKIT FOR TRANSFERS

- Precise criteria for **adequacy decisions** (also partial or sector-specific)
- **Simplification** (abolishment of prior notification/authorisation) and **expanded possibilities of using other transfer tools** (model clauses, BCRs)
- Introduction of **new tools** (e.g. certification mechanisms, approved codes of conduct)

STRATEGIC VISION FOR INTERNATIONAL TRANSFERS: COMMUNICATION OF JAN. 2017

- at **bilateral level** focus on **adequacy** (*Japan, Korea…)*
- at **multilateral level** promotion of convergence (in particular in the framework of **Convention 108** of the Council of Europe)

Universal trend, not just an "EU approach"

- Trend of **convergence towards universal model** (core principles, enforceable rights, oversight by independent authority, judicial redress)

- **Japan, South Korea**: recent modernisation based on fundamental rights approach
- **India**: Supreme Court decision and White paper
- **Brazil**
- Other examples
- Modenisation of Convention 108

Core rights of data subjects in the EU

- Information
- Access
- Rectification
- Erasure (incl. "right to be forgotten")
- Restriction of processing
- Portability
- Objection
- Automated decision-making

Core obligations of controlles (data protection principles)

- **Purpose limitation**
- **Data minimisation**
- **Data accuracy**
- **Limited retention**
- **Data security**
- **Accountability**

Personal data

Personal data only includes information relating to living natural persons (data subjects) who:

- can be **identified or who are identifiable** directly from the information in question; or
- who can be **indirectly identified** from that information **in combination with** other information.

GDPR

- **Individuals** (except processing carried out for purely personal/household activities
- **Business operators and organisations**
- **Public authorities** (except ***criminal law enforcement***: Law Enforcement Directive (EU) 2016/680; ***national security, defence*** **and** ***foreign policy***: no EU jurisdiction, thus regulated by Member States laws within the limits of national constitutions, ECHR/Union law and Convention 108; **EU institutions**: Regulation 45/2001)

Specific processing situations and limitations

- **Journalism and academic, artistic or literary expression** (Article 85): derogations if necessary to reconcile right to data protection with freedom of expression/information
- **Access to documents held by public authorities** (Art 86): disclosure to the extent balanced with data protection rights
- **Employment context** (Article 87): more specific rules to safeguard rights and interests of employees
- **Archiving, scientific or historical research, statistics** (Article 89): special safeguards (e.g. pseudonymisation, data minimisation), limitations of certain rights if necessary
- **Churches and religious associations** (Article 91): own data protection rules and specific supervision

Accountability

The controller shall be responsible for, and be able to demonstrate compliance with data protection principles.

- Two key elements:
  - controllers are **responsible for complying** with the GDPR;
  - controllers must be able to **demonstrate** their **compliance**.
- Not a box-ticking exercise: being responsible for compliance means that controllers need to be **proactive** and **organised** about their approach to data protection, while demonstrating their compliance means that they must be able to **evidence compliance steps**.
- Being able to show that risks have been considered and addressed through concrete measures and safeguards can help controllers to **mitigate against any potential sanction**
- Special accountability tools: DPIA, data breach notification, DPO.

Risk-based approach

*"Taking into account the nature, scope, context and purposes of processing as well as the **risks of varying likelihood and severity** for the rights and freedoms of natural persons, the controller shall **implement appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*" (Art. 24)

No **"one-size-fits-all"** approach, but **different obligations according to the risk of processing**, e.g.:

- Designation of **representative**, Art. 27(2)(a) (risk);
- **Records**, Art. 30(5) (risk);
- **Data breach notification**, Art. 33, 34 (risk/high risk);
- **DPIA**, Art. 35 (high risk);
- **DPO**, Art. 37 (large-scale processing, systematic monitoring or sensitive data).

See also Recital 74 and, for relevant factors in the assessment, Recitals 75/77.

Data protection officer

- DPOs are a central element of **accountability** by giving advice, monitor compliance and foster data protection culture; act as **intermediaries** (e.g. contact point for individuals and DPAs).
- **Requirement to appoint DPA**:
  - **public authority** or **body** (except courts acting in their judicial capacity);
  - core processing activities require **large scale, regular and systematic monitoring** of individuals (e.g., online/location tracking, risk scoring); or
  - core processing activities consist of **large scale processing of sensitive data**.
- **"Core activities"** refers to operations necessary to achieve objectives; includes activities where processing forms **"inextricable part"** of controller's core activities (e.g. processing of patient data in hospital); **not support functions**.
- **"Large scale"** relates to number of individuals, data volume, time/space (e.g. hospital, search engine).

Role and powers of DPAs

European Data Protection Board (EDPB)

Nature and composition

- **Replaces Article 29 Working Party** established by Directive 95/46.
- **Independent EU body** with legal personality.
- Represented by its **Chair**, who is elected for a renewable term of five years (currently the Head of Austrian DPA).
- Composed of the **Head of one supervisory authority per Member State** and of the European Data Protection Supervisor.
- **European Commission** has the right to participate in activities and meetings of the Board without voting right.

Main tasks

- **Ensure the consistent application of the GDPR** (in particular through the consistency mechanism and dispute resolution).
- **Issue guidelines, recommendations and best practices** which are publicly available and open to public consultation prior to adoption.
- **Advise** the Commission on any issues related to the protection of personal data in the EU.
- **Provide the Commission with an opinion** on adequacy assessments of third countries or international organisations.
- **Promote cooperation**, training programmes and **exchange of knowledge** between supervisory authorities.
- **Carry out the accreditation of certification bodies** and maintain a public register.

The EU Data protection institutional set-up

European Court of Justice

- Provides definitive interpretation of GDPR

National Courts

- Review DPA decisions

National Data Protection Authorities

- Issue decisions incl. fines
- Can provide advice on GDPR

European Data Protection **Board**

- Issues guidelines, opinions, etc.
- Advises EU institutions
- Consistency mechanism

European Data Protection **Supervisor**

- Supervises EU institutions
- Advises EU institutions
- Secretariat for EDPB

European Commission

- Supports/monitors implementation of GDPR
- Prepares/adopts adequacy decisions, negotiates int'l agreements

Sanctions: administrative fines

- **Central element of enforcement toolbox, not a "last resort"; independent from/in addition to other (corrective) measures**
- **Discretion whether** and **what amount**…but fines must be **effective, proportionate and dissuasive**; e.g. not in case of **"minor infringements"**
- Decision guided by **a numer of factors** that need to be applied considering the facts of each individual case:
  - **Basic factors**: nature, gravity, duration, degree of responsibility (measures to ensure compliance, e.g. security/privacy policy), fault (intention, negligence), consequences/harm
  - **Aggravating factors**, e.g. previous infringement, non-compliance with prior DPA order, financial gain from infringement
  - **Mitigating factors**, e.g. adherence to Code of Conduct, notification of infringement to DPA, cooperation with DPA, actions to limit harm

Data protection in law enforcement

The specific nature of police and judicial activities in criminal matters requires differentiated rules on the protection of personal data, in order to facilitate the free flow of data and promote co-operation between the member states in these areas.

The new directive protects rights of individuals while guaranteeing a high level of public security

LED (Law Enforcement Directive)

*The directive on protecting personal data processed for the purpose of criminal law enforcement entered into force on **5 May 2016**. Member states had until **6 May 2018** to translate the directive into national law.*

LED

*The Directive applies to both **cross-border and national processing** of data by member states' competent authorities for the purpose of law enforcement.*

This includes the prevention, investigation, detection and prosecution of criminal offences, as well as the safeguarding and prevention of threats to public security.

It does not cover activities by EU institutions, bodies, offices and agencies, nor activities falling outside the scope of EU law.

LED

Harmonising data protection rules in the law enforcement sector, including rules on international transfers, will facilitate cross-border cooperation between police and judicial authorities, both within the EU and with international partners, and thus create the conditions for a more effective fight against crime.

LED monitoring

*The **supervisory authorities** can be the same as those established under the general data protection regulation.*

*It provides rules on **mandatory mutual assistance** and a general obligation to cooperate.*

*It lays down that the **European Data Protection Advisory Board** shall also perform its tasks for the processing activities covered by this directive.*

Thank you