GIDE
GIDE LOYRETTE NOUEL

The Japanese Chamber
of Commerce and Industry

NISHIMURA
& ASAHI

HOW JAPANESE COMPANIES SHOULD TAKE INTO ACCOUNT THE GENERAL DATA PROTECTION REGULATION (GDPR)

Thierry Dor

Conference, Paris

27 September 2017

The EU Legal Framework

- **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- **The new "data protection package" applicable as of 25 May 2018:**
  - **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

  - **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the 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, and on the free movement of such data.

Other privacy initiatives and pending matters

- **Adequacy decision (« Privacy Shield ») replaced the « Safe Harbor » (United States) in June 2016**

- **Proposal of the European Parliament and of the Council for a Regulation on Privacy and Electronic Communications** repealing the e-Privacy Directive 2002/58/EC

- **Finalization of negotiations on the modernization of Convention 108** of the Council of Europe by the end of 2017

Material scope

- **Articles 1, 2 and 55(3):**
  - Natural persons
  - Personal data
  - Exclusions:
    - Manual processing not contained in a filing system;
    - Activities which fall outside the scope of Union law;
    - Common Foreign and Security Policy (CFSP);
    - Purely personal or household activities;
    - Police and criminal justice;
    - EU institutions and bodies.
- **Recitals 14 to 19, 26 and 27:**
  - Exclusions:
    - Deceased persons;
    - Legal persons;
    - Anonymous information.

Territorial scope

- **Article 3 paragraph 2:**

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

- **Article 27 on representatives**

Principles and lawfulness of processing

- **Principles:**
  - Lawfulness, fairness, transparency
  - Purpose limitation
  - Data minimization
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality

- **Lawfulness:**
  - Consent
  - Contract
  - Compliance with a legal obligation
  - Protection of vital interests
  - Performance of a task carried out in the public interest or in the exercise of official authority
  - Legitimate interests pursued by the controller, subject to the interests or fundamental rights and freedoms of the data subject

A Regulation giving some leeway to Member States for its application

- Several provisions of the Regulation may be specified by Member States; however, it does not amount to minimal harmonization:

  — **Rules on child's consent** (information society services) by Member States law (between the age of 13 and 16 years old): Article 8(1)

  — **Processing in the context of employment**: Article 88

  — Further conditions/limitations, with regard to the **processing of genetic data, biometric data or data concerning health**: Article 9(4)

Some « novelties » (1)

- Further information obligations
- Enhanced right to erasure (“right to be forgotten”) and to object
- Right to data portability
- Reinforcement of the obligations of processors
- Obligation to maintain records of processing activities applicable to both controllers and processors
- Non-systematic notification of personal data breaches to the supervisory authorities and concerned data subjects

Some « novelties » (2)

- Impact assessment in high risk cases
- Data protection officer
- Facilitated data transfers to third countries
- Liability of controller/processor: a complex system
- Derogations related to processing for research and archiving purposes: Articles 5(1)(b) and 89
- Standardized icons by way of delegated acts of the Commission

No personal data are **collected** beyond the minimum necessary for each specific purpose of the processing

No personal data are **disseminated** to commercial third parties

No personal data are **retained** beyond the minimum necessary for each specific purpose of the processing

No personal data are **sold or rented out**

No personal data are **processed** for purposes other than the purposes for which they were collected

No personal data are retained in **unencrypted** form

Important changes: one stop shop

- Lead supervisory authority
- Supervisory authority handling the complaints and other supervisory authorities concerned
- Consistency mechanism and dispute resolution by the European Data Protection Board
- Effective judicial remedies

Important changes: fines and penalties

- **Harmonization of administrative fines:**
  - Up to 10 million € or up to 2% of the total worldwide annual turnover, whichever is higher for standard infringements;
  - Up to 20 million € or up to 4% of the total worldwide annual turnover, whichever is higher for more severe infringements.

- **In addition to administrative fines:** « *Each Member State shall lay down the rules on other penalties applicable to infringements of this Regulation* »

Next steps (1)

- **GDPR implementation at the national level:**
  - Transposing the Police and Criminal Justice Directive
  - Specifying certain provisions of the Regulation:
    - France bill “CNIL 2” not yet published
    - Germany law passed
    - UK “Data protection Bill 2017”

- **Implementing and delegated acts to be adopted by the Commission**

Next steps (2)

- **Guidelines published by the Article 29 Data Protection Working Party:**
  - Guidelines on Data Protection Officers ('DPOs'), 5 April 2017
  - Guidelines on the Right to Data Portability, 5 April 2017
  - Guidelines on the Lead Supervisory Authority, 5 April 2017
  - Guidelines on Data Protection Impact Assessment (DPIA), 4 April 2017
  - Opinion on data processing at work, 8 June 2017

- **Upcoming Guidelines by the Article 29 Data Protection Working Party** on certification, data transfers to third countries, administrative fines, consent and profiling, transparency and data breach notifications.

THANK YOU

ありがとうございます