International Conference
Enhance the Right to Data Protection in Eastern Partnership Countries
Tbilisi, 14-15 December 2016

Session I – International and European Data Protection standards - Trends

How DP Principles were developped worldwide and have had to be detailed or reinforced along with new challenges

Marie GEORGES, CoE expert

In the 1970s, the starting point

CONTEXT:, Built for military purposes, (the calculation of the missile V2's fly, **Computers (which are very expensive), start to be used for internal management and productivity in big enterprises and governmental departments.** So only in rich (western) countries. Thanks to the clever use and commercial ideas at IBM.

What happened? Very soon in the 70s, on both sides of the Atlantic, consciences of the risks of abuses with regard to concerned individuals (and democracy) **when personal data are invisibly digitalised and processed, SO**

✓ **in USA** (1970-1974), **the Health sector** elaborated the so called

- **Fair Information Practices (FIPS)**, the basic principles as direct answers to the identified risks of digitalised data in the hand of others but rather as guidelines, becoming mandatory only for the federal public bodies and only for the protection of Americans (no protection for foreigners while data are starting to be transferred)

✓ **In Western Europe**

- **Laws are adopted, setting up FIPS + independent supervisor authority + sanctions, Land of Hessen (Germany) 1971, Sweden 1973, France 1978…, against risks in a democratic society** of abuse of power with invisible processing of personal data being computerized in the hand of powerful others

✓ **International transfers already => "Guidelines" OECD(23/09/1980), COE**

70s Basis principles-FIPS as answers to risks

Fair Information Practices or Principles (US=>in // OECD, DP guidelines but not mandatory, CoE Convention with ++ see next slide)

for **answering to all possible abuses of digitalized data** in the hand of others :

- **Using or communicating data for non legitimate purposes,**
- **Collecting/processing too much data with regard to purpose,**
- **Storing data too long, with regard to purpose**
- **Multiple Security risks when using IT.**
- **Concerned individuals not being aware**

=>Two main components of still pertinent answers

1. Controllers 's obligations to respect individuals (called "quality of data" and "security" principles in the CoE convention)

- Responsibility of the following principles
- Data collection and processing only for specified and legitimate purposes
- Adequate, pertinent data and No more than necessary to achieve the purposes
- Data storage No longer than necessary to achieve the purposes
- Security of data and processing

2. Individuals (data subjects) " participation'" (rights to control the use of their personal data - called "complementary guarantees in CoE convention")=>

- to be informed on the data processing
- to access to own personal data,
- to have data corrected or erased as necessary

At the international level end of the 70s

- OECD DP Guideline of **23/09/1980** (rich countries**) the same FIPs…** in all Parties **with derogations for national security**... , SO allowing transfers of personal data among OECD Parties, **BUT Not mandatory**
- **Council of Europe Convention 108** 4 months later, 21/01/1981 allowing transfers among Parties, **open to third countries**

Based on the HR concept " Personal data = element of the right to personality=> not subject to appropriation, inviolable"

Purpose of the convention : Protection of fundamental freedom and rights , in particular private life, with regard to automated personal data collection and processing

The following prescriptions being **minimum BUT in the national law (in blue what is above FIPS and OCDE) :**

- **Protection of all data subjects no matter the nationality or place of residence**
- **With regard to automated personal data processing** (possible + to cover non automated files, and possible + for protecting legal entities "interests") ,
- **FIPs** (basic principles and complementary guarantees-rights-, see previous slide)
- **Reinforced protection for processing "sensitive data", against possible discrimination: prohibition except by law setting up appropriate guaranties (**origin, religion, political opinions, medical data, sexual life sexual, penal condemnations)
- **Exceptions or limitations of rights "by law (clear and precise), where it is necessary in a democracy" + proportional for**:
  - National Security , Public order , Monetary State interest (limitations)
  - Protection of the data subject (i.e exclusion of data processing for private life,..) and limitations for the freedom and rights of others (i.e freedom of expression)
- Where a national DP law in the origin Party insures a higher level of protection, transfers may be limited except with additional conditions in the Party of destination
- **Possible appeal to national justice … then to the supranational court (CoE members) : the European Court of Human Right**

2nd step 15 years later-EU Directive of 1995

UN GA adopts a resolution on content for DP Law in 1990 (=CoEs requirements + DPA)

EU CONTEXT : the "Opening of the internal market" raised the need of equivalence of DP protection in all Member States (opening based on 4 liberties: free flow of goods, services and assets, and of individuals; foreseen for 1990, in force in 1993)

When, where, who raised this need? With which results?

- During the International conference of DPAs, end of August 1989,
- organized in Berlin
- The German DPAs alerted publically its European colleagues
- with efficiency…. through an official letter sent to the President of the European Commission (who was French, while the Vice president Commissioner for internal market was German !!)

Whose initiative then and how:

- The EC - DG in charge of the "internal market" had elaborated a draft proposal for a directive "harmonizing the MS' DP Laws" with criteria:
- **Being a development of the Convention 108**
- **The level of protection it insures must be the highest among MS , because in the field of Human rights, so incorporating the most protective and efficient national provisions**
- **Taking care of data collected in the EU from outside the EU and of data flows to States out side EU, including Countries not being members of the Council of Europe.**

=> Huge US and UK lobbies against

Results: Finally the lobbies failed (UK being the only one abstaining to vote for). Meanwhile, 3 new MS within the EU. **The EU directive was adopted on 24 October 1995 by the 15 MS** (as part of the "EU acquis" further on new candidates to EU have had to align to it= **today 28 Member States**)

Core additional DP concepts within the different DP components EU directive of 95

1. To the FIPs + CoE' controllers and processors ' obligations and of processors

+ **List of legal criteria for "legitimate/lawful purposes" (free, informed, consent, obligations, public mission…** including the so called "b**alance of interests") + list of criteria on exceptions "sensitive data"**

+ **Obligation with regard to their processors (contract, security obligation of processors)**

+ with regard data subjects at time of collection of data : **Details on the content of information for transparency** of processing

2- 1st time of Rules for safeguarding protection with regard to transfers outside (EU) of personal data (including to non CoE convention Parties) , origin Fr. and Denmark

Concept of "adequate level of protection"= in international "law with equivalent effect", or by contractual solution/authorisation by DPA, some derogations=> add. protocol to CoE convention in 2001

3. to the FIPs+ CoE' data subjects rights + right of objection, the right not to be subject to a final decision based on calculated profiles (complete prohibition of this technique for justice decisions) so to object to such other decision, and **to know the reasoning behind the processing which result is opposed to individuals** (origin France)

4. Means to ensure application of the DP principles (of a general nature) +rights

A. Most important: mandatory Data Protection Independent Supervisory Authorities with "power to intervene" (criteria for cases of a priori control, complaints, control on the spot…) SEE NEXT Sessions for -> in the add. Protocol to Convention 108 in 2001

Introduction of the concept of **Data Protection Officer** (origin Germany**)** for internal control

In parallel…, Earliest core steps…, Next

- **In // to those European instruments : MUCH INFLUENCE WORLD WIDE : 111 States DP law**

+ CoE: Lots of sector recommendations (to be looked at on its web site) prepared by the COE Convention committee, the Telecom one=> EU privacy directive, the police one also inspired EU instruments in that field.; others on current negotiation (health data, Big data..)

+ several important ECHR' s decisions against many States in particular in the Police field

+ EU : Adoption of Privacy directive, Lots of EU Working party of DPAs 'positions and recommendations adopted (on each new EC initiatives, on interpretation of core concepts or sector questions all to be seen) see on its web site

+ important European Court decisions see in particular those against States where DPA are not independent, against the "traffic telecom and internet data' retention directive", against Google search engine establishing the "right to be forgotten", against the "Safe Harbour" EC decision on data transfers to USA

- **Earliest international steps Snowden's revelations 2013 => a UN Special Rapporteur on Privacy: shall we have a world convention? In how many years?**

The Modernization of Convention 108, started in 2011, to be soon adopted, because

- Need to up dates taking on board EU addition good provisions
- And new concepts from the International conference of 2008 in Madrid

See next presentation

In parallel…, Earliest core steps…, Next

The EU general DP regulation and the EU DP directive for police activities which negotiation started in 2012, adopted 24 April 2016, to replace the Directive of 95 and EU other decisions (because of expansion of EU missions and powers) **cf. new IT, data processing in all aspects of life + to be directly applicable = a detailed law. Core new concepts**

- **Extended and more detailed definitions (such as personal data, pseudonymisation, profiling, consent, genetic and biometric data, personal data breach, main establishment…)**
- **More precise rules on applicable law, change of purpose (consent or law), where data subject being a minor,**
- **Extension of "sensitive data" to genetic and biometric data=> legal basis**
- **Extension of information to be given to data subject (third country/protection, retention period…) and Extension of the data subject rights to "portability right"**
- **Much less notification to DPA, only on cases presenting particularly risks fixed by DPA => More controller's internal measures:**
  - **DPO, data protection assessment, data protection "by design" and by default"**
- **introduction of certification scheme**
- **high administrative sanctions (maximum 4% Global revenue),**
- **WP art 29 => Board with power for decisions on sanctions when several MS are concerned**

NEXT

- Adoption of the modernized CoE Convention early 2017? see next presentation ,
- GDPR and Police directive to be enforced in 2018
- Among others COE recommendations : Big data… and WP art.29 on good practice to apply the new EU DP Texts
- Continuing other international, regional or common language DPA's networks (including in Asia and Africa), see in a next session
- UN Rapporteur on Privacy visiting countries currently,annual report,
- **the EU privacy directive to be up dated**, including on the difficult question the technical security means of hard Cryptography : will the keys be **in the hands of intermediaries or also in users' hands** ??? The latest solution favoured by all IT specialists, Enterprises, HR NGOs (because of hackers) but not by Governments …

.

THANK YOU