AIBL

ASSOCIATION of INTERNATIONAL BUSINESS LAWYERS

ASSOCIATION de JURISTES d'AFFAIRES INTERNATIONAUX

WHY SHOULD YOUR ORGANISATION WORRY ABOUT DATA PROTECTION?

Friday, September 26, 2014
Luncheon, Hôtel Métropole, Geneva

Isabelle Hering
Attorney-at-law
Nyon

ETUDE HERING

WHO IS CONCERNED AND SHOULD WORRY?

- Natural persons
- Legal persons
  - Small, middle, big organisations

⇒ Whoever ***processes personal data***

- Reputation
- Competition
- Claims from data subjects
- Criminal prosecution

LEGAL FRAMEWORK

DATA PROCESSING BY NATURAL OR LEGAL PERSONS OR FEDERAL AUTHORITIES	DATA PROCESSING BY CANTONAL OR COMMUNAL AUTHORITIES
Swiss Federal Act on Data Protection (FADP) Applicable since July 1st, 1993 Revised in 1996 and 2010 http://www.admin.ch/ch/e/rs/c235_1.html =>protection of privacy of the data subjects **Ordinance to the Federal Act on Data Protection** =>details some provisions of the FADP [**Other specific laws related to specific professions** (Ex.: banking law or social security laws)]	**Cantonal data protection acts** **ex.:** • Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD), Geneva • Loi sur la protection des données personnelles (LPRD), Vaud • Loi sur l'information, la protection des données et l'archivage (LIPDA), Valais
Practice from the Federal Data Protection and Information Commissioner (FDPIC) Recommendations, guides, advice, FAQ, contracts templates, and explanations http://www.edoeb.admin.ch/index.html?lang=en	**Practice from the Cantonal data protection commissioners**
EUROPEAN Law	

PROCESSING OF PERSONAL DATA/SENSITIVE DATA/PERSONALITY PROFILES

Art. 3 FADP

- **Personal data (open definition)**:
  - all information relating to an identified or identifiable person
- **Sensitive personal data (closed definition)**:
  - religious, ideological, political or trade union-related views or activities
  - health, the intimate sphere or the racial origin
  - social security measures
  - administrative or criminal proceedings and sanctions
- **Personality profile**:
  - a collection of data that permits an assessment of essential characteristics of the personality of a natural person

=>Sensitive data/Personality profile justify a different treatment, eg. :

-an explicit consent (art. 4 al. 5 LPD) (when requested)

-obligation to inform (art 14 al. 1 LPD)

-declaration of files by private individuals (art. 11 LPD)

- justification for disclosure to third parties (art. 12 al. 2 letter c LPD)

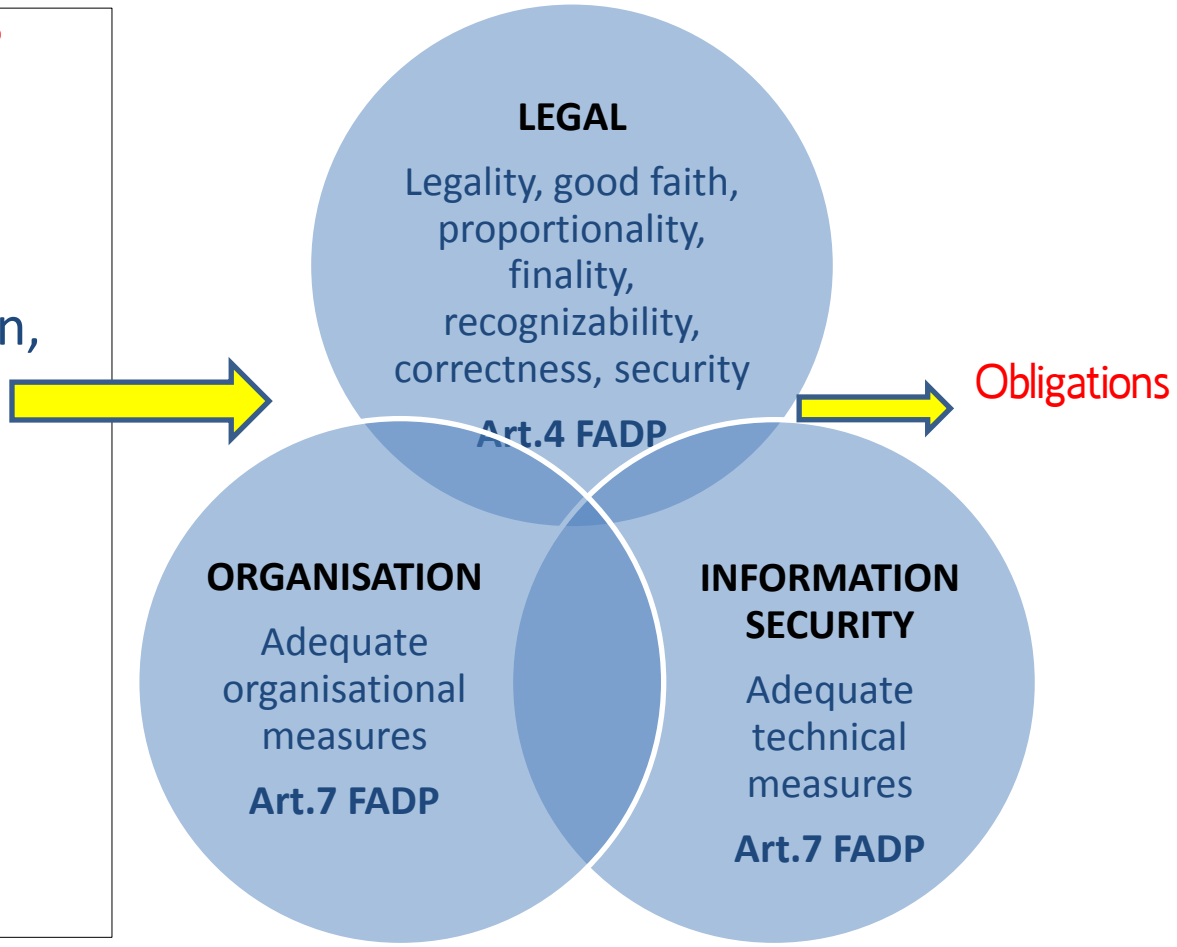
If above data are anonymised=> no FADP application

THE THREE CIRCLES APPROACH

DATA PROCESSING?

- Collection
- Communication/ Disclosure (access, transmission, publication)
- Storage
- Use
- Revision
- Archiving
- Destruction

Exceptions



FIRST CIRCLE: THE LEGAL PRINCIPLES

The processing of data by private (individual or legal) persons **must not unlawfully breach the privacy** of the data subject (art. 12 FADP)

Breaches (not exhaustive) if :
-processing in contravention of the legal principles

- Legality
- Good faith
- Proportionality
- Finality
- Recognizability
- Correctness
- Security

-against express wish of the data subject

-disclosure of sensitive personal data/personality profiles to third parties

***Unless* there exists a justification (consent, legal basis, overriding private or public interest)**

OBLIGATIONS

Obligations	**Exceptions**
Access right (information right) (Art. 8 FADP)	Derogations: legal basis, overriding interest of third parties, overriding interest of controller of data (art. 9 FADP)
Duty to inform the data subject in case of collection of sensitive data and personality profiles (Art. 14 FADP)	Derogations: data subject already informed, legal basis, overriding interests of third parties, overriding interests of controller of data (art. 14 al. 5 FADP)
Duty to register data files (art. 11 FADP)	Derogations: legal basis, exemptions of files by FC, nomination of a DPO, certification (art. 11 al. 5 FADP)

SECOND CIRCLE: ORGANISATIONAL MEASURES

Model 1 : The controller of data files declares his files directly to the FDPIC

⇒ Designation of the controller (s) of data files in charge to ensure the proper application of the FADP

⇒ Simple and online declaration on the FDPIC website

Model 2 : The controller of data files designates a data protection officer (DPO)

⇒ Principle of self-regulation applies to the data protection

⇒ The designation releases the company from the obligation to disclose its files to the FDPIC

⇒ DPO has FADP knowledge versus controller of data

⇒ For organisations where there is a lot of reported files, with several different controllers of data , difficulties to build an inventory of data files

Model 3 : The company implements a Data Protection Management System, based on an Information Security Management System. The certification of this system releases the controller of data of its obligation to declare its data files to the FDPIC

Other tasks part of the organisational measures:

Establish procedures for managing access , Contracts (clients employees, partners) , Internal charters / guidelines, Specifications (who does what) ,Training / awareness, risk management and compliance

THIRD CIRCLE: INFORMATION SECURITY MEASURES

- Information security measures in order to ensure:
  - The **C**onfidentiality of data: access only to authorised persons
  - The **I**ntegrity of data : protection of accuracy and completeness of data
  - The **A**vailability of data: ensure that users have access at a given place and time
- Measures on Data Access: security of buildings and machines (against flows, fire, electricity, air conditioning), identification and authentication, logs and rights management, remote access control (mobiles, PC protection, logs)
- Measures related to Data Transfer: network security, email security (encryption, signature), logs on transfer of data
- Measures against : accidental, environmental and deliberate threats

=> Reducing the risks to an acceptable level

CROSSBORDER TRANSFER OF DATA

Art. 6 FADP: *Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the* ***absence of legislation that guarantees adequate protection.***

=>List of countries with adequate/inadequate protection
http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr

In the absence of such protection, data may only be disclosed abroad **if**

- Sufficient safeguards are put in place: contractual clauses or rules (*auto regulation*)
- Consent of the data subject
- Processing abroad directly connected with conclusion or performance of a contract of which the data subject is a party,
- An overriding public interest can justify the disclosure of personal data abroad
- Protection of the life or physical integrity of the data subject
- The data subject has made the data generally accessible and has not expressly prohibited its processing
- Existence of directives or charters for transfers within the same company or between legal persons that are under the same management (*auto regulation*)

=>The FDPIC must be informed in cases of auto regulation

NEW EUROPEAN LAW

ONE CONTINENT= ONE LAW=> THE EXISTING DIRECTIVE (95/46/CE) WILL BE TRANSFORMED INTO A REGULATION, DIRECTLY APPLICABLE IN THE EU TERRITORY

SAME RULES FOR ALL COMPANIES: WIDE TERRITORIAL APPLICATION (ART. 3): application of the regulation

- to data processing by a controller or a processor **established in the union**, whether the processing takes place in the Union or not .
- to the processing of personal data of data subjects in the Union by a controller or processor **not established in the Union** where the procession activities are related to the offering of goods or services in the union

=> NON EUROPEAN COMPANIES WILL HAVE TO STICK TO EU DATA PROTECTION LAW IF THEY OPERATE ON THE EUROPEAN MARKET

RIGHT TO ERASURE (ART 17) (right to be forgotten) right to obtain from the controller

- erasure of personal data relating to data subject
- abstention from further dissemination of such data,
- **from third parties the erasure of any links to, or copy or replication of, that data** where one of the following grounds applies:
  - the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
  - the data subject withdraws consent on which the processing is based
  - when the storage period consented to has expired, and where there is no other legal ground for the processing of the data

=>This applies to companies not established in the EU with servers in the US but who are offering services to European consumers…

NEW EUROPEAN LAW

OBLIGATION TO DESIGNATE A DATA PROTECTION OFFICER (ART. 35):

- […] the processing is carried out by **a legal person and relates to more than 5000 data subjects in any consecutive 12-month period;**
- […] **the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), data on children or employees in large scale filing systems.**

EFFECTIVE SANCTIONS: ADMINISTRATIVE FINES (ART. 79)

- *a warning in writing in cases of first and non-intentional non-compliance;*
- *regular periodic data protection audits;*
- *fine up to **100 million EUR or up to 5% of the annual worldwide turnover** in case of an enterprise, whichever is higher.*

Text adopted by the European Parliament on March 12, 2014: IN ORDER TO BECOME LAW, THE TEXT HAS TO BE ADOPTED BY THE COUNCIL OF MINISTERS

It is now awaiting Council 1st reading position

http://www.europarl.europa.eu/oeil/popups/summary.do?id=1342337&t=d&l=fr
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=FR&reference=P7-TA-2014-0212

AVAILABLE COURSES

- FER Genève: Workshop in French, June 9th 2015, 1 day

  «*Approche globale de la protection des données et de la sécurité de l'information en entreprise*»

- HEIG-VD Yverdon: certificate in French, January and March 2015, 6 days

  «*Le conseiller à la protection des données en entreprise*»

- University of Geneva: INFOSEC DAS/MAS in French, 1 ½ year program
  =>one specific module related to data protection

  «*Sécurité de l'information*»

CONTACT

THANK YOU FOR YOUR ATTENTION!

ETUDE HERING
Isabelle Hering
Reverdil 4
1260 Nyon
+ 41 22 361 85 81 (tel. and fax)
+ 41 76 394 80 80 (mobile)
www.heringavocats.com
ihering@heringavocats.com