

IP / IT Law

➤ **Part 2: Information technology**

Title 2: The private data

- Chapter 1: Context of the private data
- Chapter 2: National Commission for Computers and Freedom (CNIL)
- Chapter 3: Rights of individuals concerned by the personal data collection
- Chapter 4: Obligations of the responsible collection of personal data

Chapter 1: Context of personal data

- **Necessity of a legislative intervention in the field of personal data**
- Difficult conciliation between the free movement of electronic information and the fundamental freedoms
- Difficult protection of the individual on the Internet
- Incomplete and inappropriate legislative solutions

❖ The legislative aims:

- The loyalty of the collection, identification of the recipient and the actual use of the data collected.
- The means implementation in order to control the illegal collection of personal data on the Internet and prevent the commercial prospecting unsolicited (*spam*).
- The differences reduction between the national laws on personal data.
- The appropriate protection of the user's private life.

❖ Personal data = particular possession

- **Everyone** has the right to respect for his private life when he /she communicates electronically.
- **Definition**: *“Any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more to specific factors as the physical physiological, mental, economic, cultural or social identity. “*
- **Are concerned**: Any treatment of personal data collected by any communication service available to the public.**

➤ **The regulation of personal data**

❖ **Main European and International sources**

European directives:

- Directive of October 24th, 1995 on the protection of the private data and the free movement of such data
- Directive of May 20th, 1997 on the consumers protection in the distance contracts

European regulation:

- European Commission Regulation of December 18, 2000

Others international agreements

❖ French law

- Act of **January 6, 1978** amended by the **L August 4, 2004** **

■ Aims of the law:

Regulate and control the development of information technologies.
Protects the individual and public freedoms.

■ Person concerned:

All companies which hold processing of personal data (*activity sector irrelevant*).

■ Data concerned:

Any elements identifying a person.

■ Private data definition

“ Any information relating to an natural person identified or can be identified, directly or indirectly, by the reference to an identification number or to one or more elements of its own ”.

■ Data processing definition

*“Any operations implementing these previous data regardless of the method used *”.*

■ Responsible of data processing definition

“The person, public authority, department or agency that implements these private data”. → Civil or criminal liability

■ Fundamental principles and enforcement of the law

- Protection of private data
- Transparency
- Right to oblivion and secrecy or confidentiality

→ Specific laws, criminal laws, cases law also consists of essential sources for the personal data protection.

Chapter 2: *“National Commission for Computer and Liberties”*

❖ Context

- Establishment of Internet user profiles which are immediately available;
- Implementation of many techniques in order to create these profiles: forms, directories, forums, cookies, script Common Gateway Interface (CGI), applet Java, ... etc.

→ **Difficulties:** the anonymity on the Internet and the control of networks.

→ **Solution:** Creation of an independent administrative authority by the law of 78: CNIL

❖ Missions and powers of the CNIL (4)

- To protect the private life and the individual or public liberties **(a)**
- To inform and advice the persons **(b)**
- To control the computer applications **(c)**
- Regulatory powers **(d)**

a) **The protection of the private life and the individual or public liberties**

- The CNIL ensures that the information used in the data processing are **adequate, relevant and not excessive** (*in relation to the purpose requiring the registration*).
- The CNIL ensures that the information relating to the racial origin, political opinions, religious or philosophical, trade union member ship, health, sex life, offenses and sentences are not stored (*except the limited cases provided by the law*).

→ **Protection of the human identity on the national territory ***

b) **Information and advice for the persons**

- The CNIL informs all persons concerned and all data controllers of their rights and obligations.
- Availability to the public a **list** of data processing that have been reported.
- The CNIL receives the complaints and petitions relating to the implementation of personal data processing, and must advise the authors of the follow-up.
- **Investigative powers** on the spot are provided.

c) **Control of computer applications**

The powers of the CNIL allows it to guarantee the respect of the law:

- Seizure of the CNIL and decision powers: complaint by a citizen, request for advice by the Committee or self-seizure power.
- Settlement disputes power: Amiable settlement of disputes privileged.
- Investigation powers: communication right of any relevant information, collect on evidence and can remove the confidentiality obligation of the computer engineers.

→ **A priori or a posteriori control**

- The obstruction to the CNIL:
 - Offense which is punished by **1 year** of imprisonment and **15 000 € fine**.
- The acts constituting the offense are:
 - The **opposition** to the practice of on the spot inspections;
 - The **refusal** to provide the useful information and documents or the concealment or disappearance;
 - The communication of information **non-compliance** with the content of the registrations.

❖ Decision of the CNIL (3 possibilities)

- To close the case without further action;
- To order a warning procedure;
- Seizure the public prosecutor's department and so it transmits the information at its disposal.

In case of emergency: It can order an temporary interruption of the implementation of data processing, the lock of certain data and/ or the information of the Prime Minister.

- **Regulatory powers of the CNIL**

- Establishment of standards in compliance with the protection of the private life and liberties.
- Types of standards: simplified standards, regulation types, rules of procedure of the CNIL.

❖ The functioning of the CNIL

→ **Independent administrative authority**

→ Composition:

- 17 members appointed for 5 years (*or for the duration of their mandate*);
- Renewal Mandate once time but without exceeded 10 years;
- 1 president appointed by the commission and 2 vice-presidents;
- All members of the CNIL are subject to the **professional secret**.

Chapter 3: Rights of individuals concerned by the personal data collection

6 rights are provided for the data subjects in relation to the private data processed:

- Right of a prior information
- Right of access and right of curiosity
- Right of communication
- Right of rectification
- Right of objection
- Right of oblivion

❖ Right of a prior information

■ Principle: The files should not be created without the knowledge of people.

→ The data must necessarily be collected from concerned persons.

→ Several types of data collections:

- Direct collection of data **(a)**
- Indirect collection of data **(b)**
- Collection of health data **(c)**

a) **Direct collection of private data**

- Whatever the responsible for the collection or the storage system information, the person must be informed of:
- the identity of the controller and the aim pursued by the data processing;
 - Compulsory or optional characters of answers;
 - Consequences for the person concerned of a failure to respond
 - Individuals or entities recipients of the data;
 - The existence of a right of access, rectification, opposition and a right to oblivion.
- → Requirements reduced in case of “anonymization process”*

b) Indirect collection of private data

- **Principle**: The Directive provides for a general obligation to inform the persons identified whatever the way, direct or indirect, to collect the data.
- **Exception**: The obligation to provide the prior information is not required when the collection aim is the establishment of statistics, historical or scientific research.

c) Collection of health data

- **Specific regime**: the files should not be created without the knowledge of patients and the controller of files should indicate what he plans to make with the information collected.
- **Exception**: Certain information may not be provided if:
 - For legitimate reasons, the doctor appreciates consciousness, the patient is left in ignorance of diagnosis or serious prognosis;
 - In case of difficulty of finding the person concerned (*death or physical impossibility*).

❖ Right of access and right of curiosity

- **Principle**: everyone has a right to access the information which concern him/her and can obtain their communication (*request directly to the controller or in case of unknown controller to the CNIL*).
- **Persons concerned**: Exclusively to the natural persons whose the name appear in the file.
- **Field concerned**: the sector is irrelevant and the right applies whatever the preservation process, manual or automated processing.
- An indirect access right also provided in certain cases (*ex: public safety*).
- **Right of curiosity** : Everyone has the power to request any organization if it has information about him.

❖ Right of communication

- Right which extends naturally the right of access .
- The holder of the access right can obtain, in an accessible form, the personal data that concern it.

❖ Right of rectification

- The right of rectification is a complement or an outcome, the right of access.
- Everyone can obtain the correction of errors:
 - When they are **inaccurate, incomplete, ambiguous or outdated**
 - **If their collection, use, disclosure or storage are prohibited.**

❖ Right of objection

- Person concerned: Any person has the right to oppose, for legitimate reasons, that the personal data relating to him being processed.
- Are concerned: All the personal data whatever the way of collecting, recording or conservation, manual or automated processing files.

❖ Right to oblivion

- The duration of the personal data stored in computer memory **must be limited**.
- The law does not allow to conserve indefinitely information on individuals.
- Duration = time required for the purpose for which the data are collected and processed.

- **What is about the private correspondence ?**

- **Principle:** Any person has the right to respect the confidentiality.

- The secret of correspondences sent through electronic communications is guaranteed by the law.
- Are concerned: any communication mean (*letters, telephone, fax, email ...*)

2 kinds of communication :

- **Private communication:** when the message is exclusively intended for one or more distinctive physical or natural person(s).
- **Public communication:** when the message is for either the general public or to certain categories of public.

→ The operators and members of their staff are subject to the confidentiality.

- “Spamming practice”

2 characteristics:

- The number of messages sent
- The unsolicited nature

→ Effect of spams: The recipient is not notified of the personal data collection.

→ Recognition of the opt-in system:

“Direct marketing by a professional using private data is prohibited when a consumer who has not expressed its consent to receive such calls”.

Chapter 4: The controller obligations of private data collections

Plan:

I / Obligations of the files manager

II / Collection of traces on the internet

III / Sanctions provided by the law

I. Controllers obligations of the personal data files

Common objective: the practical implementation of individual rights.

→ **General duty of loyalty** : prohibition of the fraudulent and unlawful collection with an obligation to security, confidentiality or aim. **

→ Provisions in relation with this duty:

- The data is collected and processed fairly and lawfully;
 - They are collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
 - They are adequate, relevant and not excessive in relation to the purposes for which they were collected and their subsequent processed;
- They are accurate, complete, and if necessary, updated.

1) Submission of the file draft constitution to the CNIL

→ This is the first step: the controller file must interact with the CNIL.

→ 3 legal regimes:

- Simplified standards regime **(a)**
- CNIL authorization regime **(b)**
- Sensible data regime **(c)**

a) **Simplified standards regime**

- **Data concerned:** data processes without invasion of the privacy and individual liberties.
 - **Formality:** A simple declaration of compliance with these standards is required.
- Table of these simplified rules available on the website of the CNIL.
- After sending of these declaration, a **receipt** is issued and the registrant can implement its data processing.

b) **Authorization regime by the CNIL**

- **Data concerned**: personal data in relating to the private life and individual liberties (*list on the CNIL website*).
- **Formality**: Application of authorization by the CNIL is a compulsory.
- The CNIL must decide within **2months** from the application receipt (deadline extended one time if necessity).
- In addition: the **consent of the data subject** is required ! (*exceptions provided by the law*).
- ➔ In any event, the CNIL ensures a balance between the fundamental freedoms of the persons concerned and the legitimate interests of the file controller !

c) **Sensible data regime**

- **Data concerned**: the information on the racial, trade union membership, political and philosophical opinion, the religious or behaviors of persons, the health and sexual life.
- **Regime: Prohibition** of these data collection
 - Some exceptions are established by the law.
 - It exists others procedures which are much heavier provided by the law (*authorization by ministerial decrees*).

❖ Designation of a data processing corresponding

- This designation avoid the data processing controller with CNIL formalities.
- This corresponding is designated by the file controller but he must exercise **independently** his functions.
- Mission of the data corresponding:
 - To keep the list of data processing implemented by the company ;
 - To ensure in an independent manner the compliance with the personal data laws.

2) Other obligations of the data controller

- Very many obligations for the data controller which ensure the no infringement to the individual liberties.
- List of these obligations on the CNIL websites.

- Obligations related to the data collection:

Principle: Freedom to collect data except the sensible or prohibit data collections.

- Duty of loyalty
- Duty of information (*previous chapter*)
- Online collection of data (forms) → Specific provisions provided by the EU directive

- Obligations related to the security of data processing:
 - Security requirements and privacy law
 - Obligations related to the transfer of data**
 - Marketing of data processing
 - Obligations relating to the conservation and non-disclosure of data:
 - Transmission of personal data to foreign country
 - Prohibition to make a decision from profiles collected
- **

II) Collection of traces on the Internet

→ Different ways to collect traces on the Internet: the **recommendations** of the CNIL are important.

- Visible data:
 - Data collected by mail (*private correspondence*)
 - Data sent on the forums
 - Data in the directory
- Invisible data:
 - Log files or data connection
 - Cookies
 - Failures contained in a software

III) Sanctions

→ An important feature of sanctions is designated in order to protect the personal data.

- Administrative sanctions
- Civil and criminal penalties
- Sanctions related to the failure of the declaration to the CNIL
- Sanctions related to the non-compliance with the rights of data subjects
- Sanctions for data processing in the health research aim
- Sanctions related to the violation of the secrecy of correspondence
- Sanctions related to the non-compliance with the security

- Administrative sanctions:
 - Warning
 - Dissemination of the warning
 - Notice
 - Specific sanctions if the data controller fails to comply with the notice
 - Financial penalties
- In case of emergency: the CNIL may decide to interrupt temporary the implementation of the data processing and may inform the Prime Minister (*see previous slides*).

- Sanction related to the failure of declaration to the CNIL:
 - Criminal offense
 - The sanctions are incurred as the unlawful file is processed and up to 3 years after the end of its use.
 - Material breach = a conviction is always possible whatever the file controller has failed to make this declaration intentionally or not (*even in negligence*).
 - **Sanctions: 5 years** of imprisonment and a fine of **300 000 euros** + civil penalties (*damages payment*).

- Sanctions related to the non-compliance with rights of data subject:
 - Criminal penalties
 - Denunciation system of the CNIL **
 - **Sanctions**: 5 years of imprisonment and a fine of 300 000 euros

- Sanctions related to the violation of the correspondence secrecy:
 - **Sanction**: 1 year of imprisonment and a fine of 45 000 euros

- Sanctions related to the non-compliance with the security and confidentiality obligations
- Criminal penalties
- **Sanctions:** 5 years of imprisonment and a fine of 300 000 euros.
- **For the legal person** : the fine incurred is **quintupled** (1,5 million euros).

QCM

▶ **The personal data protects**

- ➔ The individual data
- ☐ The company data
- ☐ The company and individual data

▶ **The law who has instituted the personal data protection is ...**

- ☐ The European Directive of 1995
- ➔ The law of 1978
- ☐ The law of 2004

▶ **The authority for the personal data is ...**

- ☐ INPI
- ☐ European commission
- ➔ CNIL

▶ **The CNIL is ...**

- ➔ an administrative independent authority
- ☐ under the authority of the government
- ☐ under the authority of the Justice Minister

▶ **The right of a prior information means that...**

- ➔ the files should not be created without the knowledge of people
- ☐ the files should be created without the knowledge of people
- ☐ Nothing, this right does not exist

▶ **Among these sentences what is the answer:**

- ➔ The data subject have a right of a prior information and communication
- ☐ The data subject does not have a rectification , objection and access right.
- ➔ The data subject has a right of curiosity

▶ **The spamming practice is ...**

- ☐ A prohibit practice in the French law
- ☐ An allowed practice in the French law
- ➔ An allowed practice in the French law with a specific regime called “opt-in system”

▶ **Among the regime which ones are provided by the French law ?**

- ➔ simplified standards regime
- ➔ sensible data regime
- ☐ a single consent of the subjects data whatever the types of data
- ➔ Authorization regime

▶ **What is the legal requirement provided in case of a simplified standards regime ?**

- ☐ An authorization of the CNIL
- ☐ The consent of the data subject
- ➔ A declaration to the CNIL

▶ **What is the legal requirement provided in case of an authorization regime ?**

- O A declaration to the CNIL
- O An authorization of the CNIL and the consent of the subject data in all the situations
- An authorization of the CNIL and the consent of the subject data in certain cases

▶ **What is the legal requirement provided in case of a sensible data regime ?**

- O A declaration to the CNIL
- O An authorization of the CNIL
- A prohibition with some exceptions

▶ **Among the following sentences which are administrative sanctions ?**

- Warning and dissemination warning
- Notice
- Dissemination of the notice