The GDPR is now applicable: What are your new obligations?

11 October 2018

mnks
A DIFFERENT LAW FIRM

Agenda

1. Definitions of key notions
2. Sanctions
3. “Accountability” principle
4. Consent mechanism
5. Liability of data processors
6. Data subjects’ rights
7. International data transfers
8. Data breach notification

1. Definitions of key notions

- **Personal data**

Name, first name, email address (professional and personal), picture, video, passport copy, location data, banking details, signature, evaluation sheet, salary, person of contact, tax returns data, etc.

⇒ Concerns only individuals

⇒ Data relating to (i) employees, (ii) your clients as individuals, (iii) persons of contact, directors, economic beneficiary, etc. in relation to your clients as legal persons and to your subcontractors, (iv) any individual who is your contact

- **Data processing**

Any action performed with the data: collect, retention, transfer, copy, etc.

- **Data controller**

The entity that decides which data must be collected, why, for how long, etc.

- **Data processor**

The entity that processes personal data on behalf and under the instructions of the data controller (e.g. provider of payroll services).

⇒ An entity can act both as data controller and as data processor

2. Sanctions

Administrative sanctions

Increased sanctions - administrative fines of up to EUR 20.000.000 or 4% of the annual worldwide turnover.

Approach from the CNPD

- Focus on companies considered “at risk”;
- Performance of an audit when a complaint is received;
- Accompany rather than issue sanctions if the company can show good faith;
- Source of risk: 1. employees
  2. clients

3. “Accountability” principle (1/2)

No more prior notifications

But …

Accountability

- Detailed data processing records in-house;
- Protection of data by design (“privacy by design”);
- Protection of data by default (“privacy by default”);
- Appointment of a DPO ?
- Implementation of organizational and technical measures

3. “Accountability” principle (2/2)

- Examples of security measures to follow:
- Clean desk policy every evening
- Lock cabinets containing documents and do not leave the key out in plain sight
- Use as little paper as possible - keep a paper version only when you have a legal obligation to do so
- Be careful before sending an email outside the company and containing personal data
- Use an EDMS (electronic document management system) / sharepoint: supervise the retention of electronic documents
- Classify your emails as well as possible
- Keep only the necessary documents and data
- Don't create shared folders all the time / Manage access

4. Consent mechanism

- Principle: In general consent is not necessary to collect and store personal data (prior information)
- Prior consent of data subjects can be mandatory:
  - When you process sensitive data;
  - When you transfer personal data outside the EEA and no other legal basis is available;
  - When you send commercial communications to contacts that are not clients (opt-in)
- Consent must be informed and explicit and data subjects may be able to withdraw it at any time

5. Liability of data processors

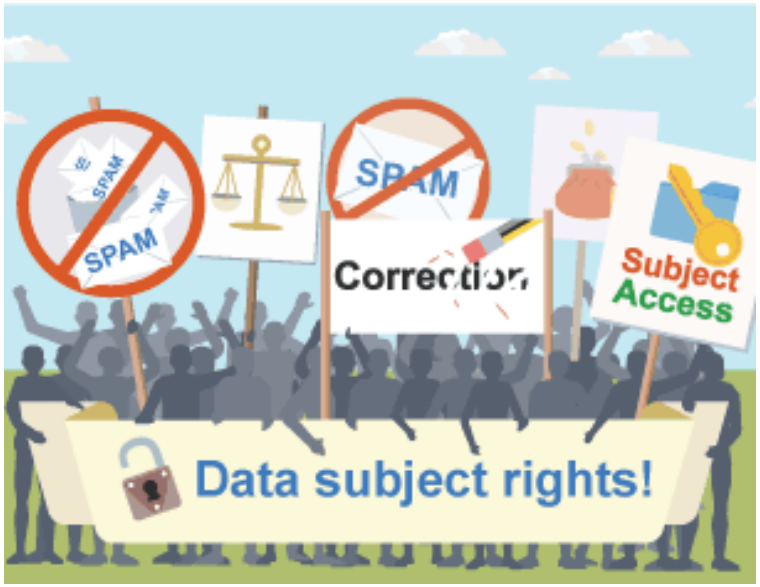
Directive 95/76/EC

- No direct obligations imposed on data processors

Regulation

- Applicable to data processors
- New obligations of data processors
  - Mandatory clauses in the contract between data controller and data processor
  - Maintain a data record
  - Implementation of technical and organizational measures
  - Data breach notification
  - Appointment of a DPO
- New liabilities
  - Contractual liability towards data controller
  - Liability towards data subjects
  - Sanctions under the GDPR

6. Reinforced data subjects' rights



- Right to information
- Right to access data
- Right of rectification of inaccurate or incomplete information
- Right to object to and to seek restriction of the processing

- Right to obtain erasure of data (right to be forgotten)
- Right to data portability
- Right not to be subject to a decision based solely on automated processing (profiling)

7. International data transfers

- **Data transfers outside the EEA are prohibited in principle**

- **Exceptions :**

- Transfers to countries ensuring an adequate level of protection;
- Transfers based on model contractual clauses of the European Commission;
- Transfers based on binding corporate rules (subject to a prior authorization from the CNPD);
- Transfers based on prior consent;
- Approved code of conduct;
- Approved certification mechanism.

8. Data breach notification

Personal data breach: *A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Notification to the data controller (Art 31)

- Without undue delay
- After becoming aware of a breach

Notification to the data protection authority (Art 33)

- Without undue delay – if possible within 72 hours
- Delay permitted if "reasoned justification"
- Exempt if unlikely to result in a risk to the rights and freedoms of data subjects

Notification to Data subjects (Art 34)

- Without undue delay
- If likely to result in a risk to the rights and freedoms of data subjects
- 3 cases of exemptions:

a. Encrypted data
b. No high risk
c. Notification would require disproportionate effort

Thank you!

Contact

Audrey Rustichelli

Head of *Technologies & IP*
T: +352 26 48 42 35 98
rustichelli@mnks.com