

Checklist before the GDPR enters into force

Posted on Monday 26th of February 2018 in IP, IT & Media

Less than 4 months before the deadline of 25 May 2018 – date of entry into force of the new European regulation on the protection of personal data (Regulation 2016/679, known as the "GDPR") – the question arises about the level of your company's compliance with the GDPR requirements.

-Update on personal data processing-

Processing of personal data includes:

- collection, recording;
- organisation, structuring;
- storage, adaptation or alteration;
- retrieval, consultation, use;
- erasure or destruction.

Personal data are defined as *"any information relating to an identified or identifiable natural person, directly or indirectly"*.

Where are you on your GDPR journey?

Download our [checklist](#) of questions to assess the level of your compliance with the GDPR requirements.

WHERE ARE YOU ON YOUR GDPR JOURNEY? YOUR COMPLIANCE

Here is a [checklist](#) of questions to assess the level of your compliance with the GDPR requirements:

Stage 1: Making the action plan

- Has a **GDPR action and compliance plan** been developed?
- Does my company need to appoint a **personal data protection officer** (DPO)?
 - If yes, did I appoint one?
- Which entities/departments are involved in the compliance plan (inventory of business activities/procedures dealing with personal data)?

Stage 2: Audit of the treatment of existing data

8, rue Sainte-Zithe PO Box 690 L-2016 Luxembourg - T (+352) 297 298 1 - F (+352) 297 299 www.molitorlegal.lu

This newsletter only intends to provide our clients and friends with information on recent or forthcoming legal developments on a general basis and does not constitute a legal advice, which can only be provided on the basis of a personal relationship between MOLITOR Avocats à la Cour and our clients.

- Did I identify **the purposes and subjects of the processes and categories of personal data**?
- Is my company able to justify the **legal basis** of each processing of personal data?
- Did I define **retention periods** for personal data (and communicate them to data subjects)?
- Are all personal data collected necessary for the processing (proportionality)?

Stage 3: Identification of risky processes and special categories of data

- Does my company perform processes that could potentially impact the privacy of the persons concerned?
 - Did I define decision criteria for determining the need of a **privacy impact study**?
 - Did I define a privacy impact assessment method?
- Does my company perform processes that involve the **cross-referencing** of different categories of data or the **reuse** of data collected for another process?
- Does my company perform data **profiling** processes?
- Does my company transfer the processed data **outside the European Union**?
- Does my company use **subcontractors** who process personal data on behalf of my company (review of contracts with subcontractors and control of subcontractors' compliance with the GDPR requirements)?

Stage 4: Implementation of procedures

- Did I incorporate elements of RGPD compliance into my company's procedures?
- Does my company have some management mechanisms in place for the collection, registration, modification and revocation of the **consent** of data subjects (when the legal basis is consent)?
- Did I establish procedures in order to satisfy requests for the **exercise of rights under the GDPR** (rights to access, rectify, erase data, to restrict processing, right to oblivion, right to data portability)?
- Do data subjects benefit from clear and understandable information at the moment of data collection?
- Does my company have mechanisms for **archiving** and **deleting** personal data?
- Did I integrate the GDPR into my company's **HR training programme**?
- Did I involve my company's **IT department** in GDPR compliance?
 - Did we put in place data **security** measures (protected access, pseudonymisation, encryption, secure storage and transfer, purge and archiving rules, etc.)?
 - Has a process for **detecting**, handling and reporting personal **data breaches** been adopted?
- Does my company's **insurance** cover the risks (penalties, damages, incidents, etc.) related to the processing of personal data?

Stage 5: Documentation

- Did my company **document** its compliance with the GDPR?
- Is there an **exhaustive mapping** of personal data processed in my company's information system?
- Did I carry out an **impact analysis** of processes that could potentially impact the privacy of the persons concerned?
- Did I establish a **register of processing operations**?
- Did I establish a **register of data processing incidents**?

BE AWARE OF THE PENALTIES!

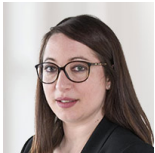
8, rue Sainte-Zithe PO Box 690 L-2016 Luxembourg - T (+352) 297 298 1 - F (+352) 297 299 www.molitorlegal.lu

This newsletter only intends to provide our clients and friends with information on recent or forthcoming legal developments on a general basis and does not constitute a legal advice, which can only be provided on the basis of a personal relationship between MOLITOR Avocats à la Cour and our clients.

High penalties apply for non-compliance with GDPR. Significant sanctions may be imposed for data breaches up to a maximum of either EUR 20 million or 4% of the company's annual worldwide turnover. In addition, data subjects may also claim damages for infringement of GDPR relating to the processing of their personal data.

We can support your company with the challenges GDPR brings. Contact us.

Your contact(s)



Virginie LIEBERMANN

Counsel

Avocat à la Cour, Member of Luxembourg Bar, 2008

virginie.liebermann@molitorlegal.lu