MOLITOR Avocats à la Cour
8, rue Sainte-Zithe
L-2016, Luxembourg
www.molitorlegal.lu
+352 297 298 1

**GDPR in Luxembourg**

**The General Data Protection Regulation** ("**GDPR**") will take direct effect in Luxembourg on 25 May 2018, but since it allows EU Member States latitude in specific areas, it will also be incorporated into Luxembourg law via different bills that are currently in the process of being adopted.

The main draft bill of law containing specific Luxembourg provisions is draft bill n°7184, currently named "*creating the Commission Nationale pour la Protection des Données and implementing of GDPR and modifying the Labour Code and the modified law of 25 March 2015 fixing the remuneration and promotion conditions of Luxembourg civil servants and* ***repealing the Data Protection Act of 2 August 2002"***.

To implement **Directive 2016/680**[1], the draft bill n°7168 on the protection of individuals with regard to the processing of personal data in criminal matters and on national security is also still under discussion.

Luxembourg governmental amendments have been recently issued and contain the following draft provisions (which are still subject to further amendments / completions[2]):

| Issue | Proposed Luxembourg specificities |
|---|---|
| **National Data Protection Authority** *(Article 58 of GDPR)* | The "*Commission Nationale pour la Protection des Données*" or "*CNPD*":<br>- a public body, having legal personality, financial and administrative autonomy;<br>- in charge of the verification of compliance with the provisions of GDPR and Luxembourg Data Protection Act and the sanctions;<br>- can **adopt regulations**, published on the Luxembourg Legal Gazette and its own website;<br>- provide **accreditation of certification bodies**. |
| | CNPD can **impose periodic penalty payments** on the controller or the |

[1] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[2] The Luxembourg Council of State "*Conseil d'Etat*" and the Council of the Luxembourg Bar "*Conseil de l'Ordre des Avocats*" have both issued advice on the current draft bill n°7184, respectively on 8 March and on 30 March 2018

| | |
|---|---|
| **Sanctions** *(Articles 83 and 84 of GDPR)* | processor of up to 5 per cent of the average daily turnover per day for failure to provide any requested information or to observe a corrective measure (administrative fines).<br><br>Any **obstruction** or interference with the CNPD's missions can be punished by **imprisonment from 8 days to 1 year and/or a fine from EUR 251 to EUR 125,000** (criminal penalty).<br><br>The CNPD may order the **publication of its decisions** in newspapers or in any other way, at the expense of the sanctioned person. |
| **Proceedings** | Proceedings before the CNPD are subject to the rules governing **non-contentious administrative procedure**.<br><br>An action can be introduced against the CNPD's decision before the Administrative Court.<br><br>The CNPD has the power to initiate or take part in civil legal proceedings in order to enforce the provisions of the GDPR. |
| **Specific processing** | |
| **Journalistic or academic, artistic or literary expression purposes** *(Article 85 of GDPR)* | **Processing** is not subject to:<br>- prohibiting the processing of special categories of personal data (racial origin, political opinions, etc.) under certain conditions;<br>- limiting the processing of judiciary personal data under certain conditions;<br>- the rules that apply to data transfer to third countries or international organizations;<br>- the obligation to provide the data subject with information, whether or not the personal data is collected from the data subject.<br><br>The right of access is postponed and limited to the extent that it cannot refer to the personal data of a source if this could lead to the identification of the source. |
| **Scientific or** | The rights of access, rectification, limitation and objection can be limited to |

| | |
|---|---|
| **historical research or statistical purposes** *(Article 89 of GDPR)* | the extent that those rights risk making the realization of specific purposes impossible, or seriously interfering with such, provided that certain appropriate measures are implemented and under certain other conditions. |
| **Health** *(Article 9 of GDPR)* | **Health services** can process **special categories of personal data** (racial origin, political opinions, etc.) where it is necessary for the purposes of:<br>- preventive medicine, medical diagnosis, care or treatment provision;<br>- health or scientific research (if the data controller fulfils certain conditions);<br>- health services management under certain conditions.<br><br>If the processing is lawful, such data can be communicated to third parties or used for research purposes. |
| **Monitoring at the workplace** *(Article 88 of GDPR)* | The supervision at the workplace may be implemented in compliance with the GDPR by the employer as a data controller.<br><br>A distinction may be made in respect of the purpose of the planned processing:<br>(i) **Processing made for**:<br>- **the compliance with health and safety provisions;**<br>- **monitoring on a temporary basis the production process or employees' performance** (when such processing is required to determine the employees' remuneration); or<br>- **implementing and monitoring a flexible-time arrangement.**<br>Prior to its implementation, such a processing may be subject to a co-decision process with staff representatives/concerned employees or the Luxembourg Labour Inspection ('ITM'). Failure to reach an agreement between the parties may lead to a CNPD preliminary opinion as to the compliance of the contemplated supervision measures. The CNPD has one month to issue its advice.<br><br>(ii) **Any other grounds for processing** (Article 6 of the GDPR) may be subject to the staff representative or the concerned employees requesting a preliminary opinion from the CNPD as to the compliance of the planned monitoring process. Such request will have a suspensive effect. The CNPD then has one month to provide its advice. |

| | |
|---|---|
| | **Prior Information** of the concerned employees and the staff delegation or the ITM remains mandatory as in the current regime. |

MOLITOR

# Checklist before the GDPR enters into force

Less than few days left 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*".

**Checklist: 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:

| The relevant questions | Level of implementation | |
|---|---|---|
| | ☑ Done | ❑ Planned on (date) |
| **Stage of compliance 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 of compliance 2: Audit of the treatment of existing data** | | |
| 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 of compliance 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**?<br>✓ 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 of compliance 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)?<br>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 GPDR into my company's **HR training programme**? | | |
| Did I involve my company's **IT department** in GDPR compliance?<br>✓ Did we put in place data **security** measures (protected access, pseudonymisation, encryption, secure storage and transfer, purge and archiving rules, etc.)?<br>✓ 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 of compliance 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!

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.