Issue 01 / February 2018

VICTOR

LUXEMBOURG'S YOUNG BUSINESS LEADERS' AWESOME MAGAZINE

fjd fédération des jeunes dirigeants d'entreprise de luxembourg

VOYAGE D'ÉTUDE FJD 2017

IRAN – TÉHÉRAN ET ISPAHAN

40 ANS FJD

UN ANNIVERSAIRE... PAS COMME LES AUTRES

COMPANY SNAPSHOTS

TALKWALKER
ADY'S HYGIÈNE
KNEIP COMMUNICATIONS

„OP E PATT MAM..."
FINANZMINISTER
PIERRE GRAMEGNA

OFFENE WORTE BEI GUTEM WEIN

JOSCHKA FISCHER ZU GAST
BEI DEN JUNGEN UNTERNEHMERN LUXEMBURG (FJD)

OHNE ANGST IN DIE ZUKUNFT

PHILIPPE SCHMIT
Partner
Arendt & Medernach

FJD TOOLBOX

GENERAL DATA PROTECTION REGULATION

We have all heard a lot about the "GDPR" over the last months and we are likely to hear even more about it in the coming weeks. So what exactly is the GDPR and how will it impact our business?

With the deadline for the enforcement of the GDPR fast approaching, I have summarised the main takeaways in a short legal fact sheet:

What does "GDPR" stand for?

"*GDPR*" is an acronym which stands for the European General Data Protection Regulation, a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the EU. The GDPR's reach extends even beyond the EU's borders as it also impacts the exportation of personal data outside the EU.

Why is the "GDPR" currently such a hot topic?

The major objective of the GDPR is to give control over their personal data back to citizens and residents and to simplify the regulatory environment for international business by unifying the related regulation within the EU. The rapid development of information and communication technologies has given rise to new concerns with regard to the processing of personal data and the protection of privacy in a global environment. As a result, in the light of ever-growing concern for preserving protection of EU citizens' personal data, the European Commission has initiated a rather substantial reform to adapt European rules to the issues raised by the globalisation of communications and the development of technologies. This reform has led to the adoption of the GDPR amongst others.

In spite of its direct effects (N.B. the GDPR is a regulation which therefore directly applies to all EU Member States and in principle does not need to be implemented via a national bill, which is the case with European directives), the GDPR nevertheless gives the EU Member States a certain flexibility to apply additional local provisions. In Luxembourg a draft bill was issued on 12 September 2017 in this context. The current Luxembourgish legal framework regarding the protection of personal data mainly relies on the amended law of 2 August 2002 concerning the protection of individuals with regard to the processing of personal data. Such legal framework will therefore undergo some substantial changes based on the GDPR and the aforementioned draft bill in the coming months.

The GDPR will apply as of 25 May 2018. As a result, there are less than 4 months left in order to become GDPR-compliant… in other words, the clock is ticking at a serious pace!

Should I really care or are lawyers just roughing things up?

Due to the vast scope of the GDPR any business processing personal data (i.e. virtually any business) will be directly and inevitably impacted by the GDPR.

The regulation applies if the "*controller*" (an entity which determines the

purposes and means of the processing of personal data) or "*processor*" (an organisation that processes data on behalf of controllers, e.g. cloud service providers) or the data subject (i.e. the person concerned) is based in the EU.

The regulation also applies to organisations based outside the EU if they collect or process personal data of EU residents.

The GDPR defines "*personal data*" as *"any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

The European Commission emphasises the fact that "*personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address".*

It is therefore reasonable to say that any type of business is likely to be impacted by the GDPR in a more or less substantial manner.

Which points must be checked in order to verify compliance with the GDPR?

Basically, GDPR-compliance is assessed according to a two-fold analysis consisting of inventory and valuation of data processing:

Inventory and description

- Listing of the data processing of a company: Inventory and description of the data processing undertaken by a company, e.g. with respect to employees, surveillance (video, telephone monitoring, badges, etc.) and specific processing involved by the activities of a company.
- Listing of the processors used by a company: Inventory and description of the processors utilised by a company for the data processing controlled by it (e.g. payroll outsourcing, management of employees, etc.).

  List of the contracts between the company and the processors along with an analysis as to whether the data protection clauses in question are compliant with the GDPR (including the identification of possible addenda to such contracts in order to achieve compliance).

Valuation of the compliance of the data processing

In a (small) nutshell, it is necessary to verify for each data processing the following points if one wishes to assess compliance with the GDPR:

- Is the data processing lawful and legitimate?

"...each business employing employees needs to verify whether it is GDPR-compliant and if not take the necessary measures to become compliant by May 2018."

- Is the data processing fair?
- Have the data subjects been informed about the processing of their data in accordance with thew requirements of the GDPR?
- Have appropriate data processing agreements been entered into with any processors?
- Is the data transferred abroad? If so, to which entities acting in which capacity? Does the relevant country offer an adequate level of protection?

I have employees in my company, is there a specific impact?

As a local employer you necessarily qualify as a controller, e.g. within the framework of handling your employees' payroll (even if the latter is outsourced to a third party service provider!).

As a consequence, each business employing employees needs to verify whether it is GDPR-compliant and if not take the necessary measures to become compliant by May 2018.

In a nutshell, this means amongst others that:

- persons handling personal data in your company should receive dedicated training
- data protection should become part of your company's internal policies
- data protection-related provisions contained in your template employment agreements should be reviewed in order to make sure that they are GDPR-compliant
- you should verify whether you are under the obligation to appoint a data protection officer
- you should keep track of data processing by tracing related activities in a dedicated register

What??? An additional register needs to be implemented? So even more formalities on the horizon...

Yes, indeed. Unfortunately you can add one additional register for each entity concerned which is located in the EU to an already lengthy list of mandatory registers.

The register imposed by the GDPR must at least have the following content:

- Name of the processing, reference, date of creation of the processing dates of up-dates of the processing
- Name, address, country, telephone number and e-mail address of the controller, processor and joint controller
- Purposes of the processing
- Security measures (organisational and technical),
- Categories of data and categories of sensitive data and the date of cancellation of this data
- Categories of data subjects
- Recipients in the EU: name, address, country, reasons for the transfers, if the recipient is a processor or a third party
- Recipients outside EU: name, address, country, adequate level of protection or not, guarantees (standard contractual clauses or other), reasons for the transfers, if the recipient is a processor or a third party

Any other similar surprises?

One of the major innovations of the GDPR is the obligation for some companies to appoint a Data Protection Officer ("*DPO*"). The GDPR requires the designation of a DPO in a few specific cases:

- Where the processing is carried out by a public authority or body
- Where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale ▸

STUNNING GDPR FACTS FOR B2B

1 B2B marketers use personal data and therefore the GDPR will apply to them too.

2 Corporate email addresses and other contact details are personal data.

3 The GDPR definition of personal data is broad and includes cookies and IP addresses.

4 The GDPR does not state that organisations need to obtain an opt-in consent for their marketing.

5 The GDPR lays out 6 legal grounds for processing personal data. All are equally valid.

6 B2B marketers will be able to make use of the legitimate interest legal ground for their marketing activity in most instances.

7 Legitimate interest is a subjective legal ground so an organisation must justify its activity and consider the privacy risks for data subjects.

8 Consent is black and white. It is a yes or a no. However, it is a robust standard which may be hard to achieve. If it is, legitimate interest might be the better choice.

THE REASONING BEHIND THE GDPR

Increased responsibilities for companies concerned

Reinforcement of existing rights
- enhancement of consent
- consolidation of information rights

Creation of new rights
- accountability
- right to oblivion
- easier access to personal data
- right to portability
- information right in case of unauthorised access to personal data

Hardening of sanctions

- Where the core activities of the controller or the processor consist of processing on a large scale of special categories of data (these include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)
- Personal data relating to criminal convictions and offences

Unless it is obvious that an organisation is not required to designate a DPO, it is recommended that controllers and processors document the internal analysis carried out to determine whether or not a DPO is to be appointed, in order to be able to demonstrate that the relevant factors have been taken into account properly. It may be required by the CNPD (*Commission Nationale pour la Protection des Données*) and should be updated when necessary, for example if the controllers or the processors undertake new activities or provide new services. Nothing prevents an organisation, which is not legally required to designate a DPO and does not wish to designate a DPO on a voluntary basis, from nevertheless employing staff or outside consultants with tasks relating to the protection of personal data.

Sounds like a rather unclear matter... how can I know whether my business is compliant?

Companies concerned are well advised to undergo a verification of their current process regarding personal data, e.g. with the assistance of specialised lawyers, in order to verify if and which measures must be implemented in order to comply with the GDPR when it enters into effect.

It is likely that a "*bull run*" may be witnessed in early 2018 by all companies not having undergone such checks in due time...

I therefore highly recommend starting a due diligence of your data processing as soon as possible in order to determine which steps need to be taken to make your business GDPR-compliant.

Will I actually go to jail if my business is not GDPR-compliant?

Please rest assured, based on the current developments you will most likely not become a long-term resident of the *Centre Pénitentiaire de Luxembourg* in Schrassig for failing to comply with the GDPR. Surprisingly the aforementioned draft bill does not foresee criminal sanctions in case of non-compliance for the time being (at least at the time this article has been written), contrary to the currently applicable law of 2 August 2002 which foresees criminal sanctions

in such scenario. The CNPD however recently issued an opinion on the draft bill, recommending that criminal sanctions be re-introduced within the new law, at least for the most serious violations of the GDPR principles. It thus remains to be seen whether the final version of the new law will foresee such sanctions.

The GDPR will also extend the currently foreseen financial sanctions in case of non-compliance. For example, heavy fines may be imposed upon non-compliant companies (between 2% and 4% of the global turnover of the company concerned, or up to EUR 10 m and EUR 20 m, whichever the highest). Extensive administrative sanctions have also been foreseen.

As from a practical perspective the CNPD will be in charge of ensuring proper application of the aforementioned provisions and will therefore be in charge of investigating complaints. The CNPD will therefore be in a position, amongst others, to temporarily suspend data processing and to order the deletion or destruction of data, and/or prohibit further processing and report breaches to the public prosecutor.

Anything else worth bearing in mind?

Even if major data protection principles will not change substantially, the current status of local implementation work demonstrates the Luxembourg government's intention to reinforce the protection of personal data and to extend the mission of the CNPD by providing it with dissuasive means to sanction any infringements of the GDPR and the future Luxembourg data protection law.

It is thus highly recommended that companies processing personal data adopt, before the entry into force of the GDPR in May 2018, specific measures to comply with the new obligations arising from it and to show accountability in this respect.

« Companies concerned are well advised to undergo a verification of their current process regarding personal data ».

HOW TO... BECOME GDPR-COMPLIANT IN 7 STEPS

1 Create a role for a DPO if necessary.

2 Implement the GDPR at board level, with direct responsibilities lying for example with the CIO, CISO and Data Protection Officer (if any).

3 Adopt risk management tools and implement security and privacy protocols into the operations of the organisation (for example, develop a data privacy framework).

4 Be concise and clear about data that is collected, what it is, where and how it is stored, how it is accessed and where it goes.

5 Be confident that data held can be securely deleted when requested.

6 Carry out regular and compulsory impact assessments.

7 Ensure your IT infrastructure is set up to minimise the risk of a data leak or security breach. As part of the GDPR regulation you are required to report a data. breach to the CNPD within 72 hours.