General Data Protection Regulation: Are you ready ?

Regulatory Update: General Data Protection Regulation

The European parliament, commission and counsel have reached an agreement on the General Data Protection Regulation (GDPR) text. This will replace the Data Protection Directive from 1995 and aims at protecting the EU citizen's personal data in the current digital world whilst harmonizing the legislation for the processing of personal data across the whole EU.

An agreement on the General Data Protection Regulation (GDPR) text was finally reached on the 15th of December 2015 – three years after its proposal in 2012 - by the European parliament, commission and counsel. The GDPR will replace the Data Protection Directive from 1995 and aims at protecting the EU citizen's personal data in the current digital world whilst harmonizing the legislation for the processing of personal data across the entire EU. It is foreseen that the Regulation will be formally adopted by spring of 2016, with an implementation period of 2 years, so entering into force in spring of 2018.

With the release of the agreed upon text, it is clear that a number of obligations are completely new, and many have significantly changed compared to the Directive of 1995, such as:

- requirements for getting consent,
- administrative fines,
- Privacy Impact Assessments (PIA),
- Privacy by Design & Default (PbD),
- data breach reporting,
- data transfer outside of the EU,
- the mandatory Data Protection Officer (DPO), and
- the right to be forgotten/erased.

Take a closer look at a number of high impact changes and new obligations of the GDPR:

1. Consent (changed)

The aspect of consent is not new, yet the requirements have been tightened significantly in the new GDPR. When requesting consent from your client for the processing of their personal data, it should be done in an unambiguous manner, through a statement or a clear affirmative action.

The box below indicates what is considered to be acceptable (+) and not acceptable (-) as an unambiguous consent (note this list is non-exhaustive).

+	-
Ticking a box (opt-in)	Silence
Placing a signature	Pre-ticket boxes (opt-out)
Explicit affirmative action	Inactivity

Things to think about:

- Using opt-out mechanisms are no longer sufficient as a sign of consent from the client. Organizations will have to change their consent settings on all of their platforms, paper and digital, - where required – in order to become compliant.
- Organizations will need to make sure that the consent mechanism is closely linked to their processing activity in order to prevent illegal (unlawful) processing. Processing personal data without valid consent is considered to be illegal.

2. New responsibilities for Data Processors (new)

One of the most impactful new additions – for data processors - is the responsibility that falls jointly upon the data controller and the data processor: the implementation of organizational and technical measures for the protection of the processed personal data.

Whereas, under the Directive of 1995, this responsibility would lie entirely with the data controller, the data processor will now also need to implement safeguards in order to be compliant with the GDPR.

Things to think about:

- Data processors will need to assess whether the existing measures are sufficient in terms of the purpose and extent of processing, the amount of data collected, the period of data storage, and the accessibility of the data. (Privacy by Default)
- A processing agreement will remain the basis for establishing the purpose and extent of the data processing activities between the data controller and processor, where the explicit identification of security measures is possible (and desirable).

3. Data Breach reporting (new)

Data breaches should be reported to the supervisory authority (in Belgium this is the Commission for the Protection of Privacy, CPP) within 72 hours after becoming aware of the breach.

Reporting on personal data breaches will depend on a number of things:

1. Does the organization know where all its personal data is located? Where personal data can be breached?
2. Does the organization have the capabilities of detecting when a breach has occurred? Do you know if you have been breached?
3. Do you have the necessary processes and procedures in place to swiftly respond to the data breach? How much time does it take to deal with such a breach? Will 72 hours be enough?

Things to think about:

- Responding to data breaches will require a well thought-through flow of actions from a range of different people and reporting will be one of those actions. Defining the actions and testing (dry-run) them in advance will only improve the response time once confronted with an actual data breach.
- Data breaches, no matter which size or impact, will need to be logged and documented in order to retroactively demonstrate compliance to the GDPR.

4. Mandatory Data Protection Officer (new)

The mandatory Data Protection Officer, has been one of the most talked about requirements in the GDPR. With the release of the agreed upon text it has been decided that each data controller or processor processing personal data "at large scale", regardless whether the personal data is sensitive or not, needs to appoint a Data Protection Officer (DPO).

This role can be filled in by an internal employee or an external contractor as long as the individual is appointed based on their professional qualities and expert knowledge of the data protection legislation and practices. How this expert knowledge should be interpreted is not yet clearly defined.

Things to think about:

- The DPO will fill an independent position with a lot of (possible) influence on the business. It's important that assigning this position is not taken lightly. The DPO should understand the company's business as well as have expert knowledge on the data privacy requirements and regulations, in order to provide adequate advise to the organization and correctly represent the company toward the Data Privacy Authority (Privacy Commission).

> "Belgian companies will only have two years to become compliant with the new regulation by pushing through operational and organizational reformswhere necessary."

5. Fines up to 20M EUR or 4% of global annual turnover (new)

With the adoption of the GDPR, administrative fines can be imposed for non-compliance with the regulation.

- Non-compliance with the obligations as a data controller or a data processor could result in a fine up to 10M EUR or 2% of the annual global turnover (whichever is higher).
- Non-compliance with the basic principles for processing (such as consent), the data subject's (client) rights or the approved data transfer mechanisms, could result in a fine up to 20M EUR or 4% of annual global turnover (whichever is higher).

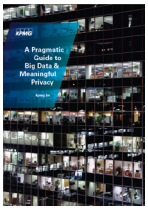
Even though so called monster fines will be possible, we do not expect to see them in the next couple of years. Large organizations that process large amounts of personal data should, however, be aware that they might be one of the first to hear the data protection authority knocking on their door to check on their compliance with the GDPR.

Things to think about:

- Fines will be imposed in case of non-compliance, so first focus on bringing the organization into compliance with the regulation and second, make sure the organization can prove its compliance through the necessary records (e.g. Privacy Impact Assessments, data breach records, consent, etc.).

Belgian companies will have a two year timeframe to become compliant with the new regulation by pushing through operational and organizational reforms where necessary.

Also view our other publications.



A Pragmatic Guide to Big Data & Meaningful Privacy

Unknown Threat in Belgium

Contact

Benny Bogaerts
Director
Information Protection Services

E: bbogaerts@kpmg.com

Kara Segers
Senior Expert
Data Privacy & - Protection

E: ksegers@kpmg.com