BELGIAN ASSOCIATION OF DIGITAL TECHNOLOGY LEADERS

Beltug Position

Two years of the GDPR – An evaluation

By Privacy experts from companies from different sectors and public institutions

25 May 2020

Contents

About Beltug

With over 1800 members from 490+ companies, Beltug is the largest Belgian association of Digital Technology leaders. We aim to tackle the challenges of the connected organisation, covering topics such as software asset management, 5G, hybrid IT, cyber security, artificial intelligence, IoT, smart collaboration, privacy, blockchain, data governance, and many more.

We defend the interests of our members, develop positions, and support knowledge exchanges between our members. Each year, we organise more than 30 events for exchanging experiences. Beltug also represents the business ICT users at the European and international levels, in close cooperation with organisations in other countries.
www.beltug.be

Two years of the GDPR – An evaluation

1 Introduction

May 2018 was a turning point for personal data protection in the EU, as the GDPR became applicable throughout the EU and for everyone active on the EU territory. We now have two years of real, everyday experience behind us. At the EU level, the review process is ongoing. It is time to take stock, see what has improved, and consider where further improvements would be welcome. In the following sections you will find a list of each. It is not our intention to write in favour of or against the GDPR. Rather, we are trying to assess the current state of GDPR adoption two years after the implementation date of 25 May 2018.

In the Beltug Privacy Council privacy experts from 55+ organisations for different sectors and public institutions exchange knowledge, experience and ideas.

2 The positive effects of the GDPR

In this section, we look at the improvements the GDPR brought, compared to the prior situation under the Data Protection Directive 95/46/EC.

2.1 Extended scope

The broader material and territorial scope of the GDPR ensures that all actors present on the EU territory, are subject to the same rules. In the past, the territorial scope allowed such actors to dispute – at length – the applicability of (then) national data protection rules, hampering effective data protection.

The GDPR has also brought a level playing field between the public and private sectors. Both are now expressly held to the same rules, with the sole exception of law enforcement and EU institutions (which are subject to a specific set of rules derived from the GDPR, but which we will not discuss here).

2.2 Increased harmonisation

As a Regulation, the GPDR applies directly in all EU Member States. This makes it a more effective legal instrument than a Directive, which must be translated in national law, often causing delays in implementation and application. This also allows different national supervisory authorities to provide guidance built on the common legal base[1].

The GDPR has also set the standard for comparable legal initiatives outside the EU (e.g. California, Brazil). These initiatives tend to model themselves after the GDPR to provide an equivalent level of protection for personal data in order to facilitate data exchange with EU countries.

[1] Covid-19 lead to different regulators issuing guidance on how to deal with personal data.

2.3 Effective enforcement

As the Data Protection Directive did not include any specific sanctions, Member States had the freedom to determine their own approaches. As a result, the lack of sanctions in some countries enabled factual impunity for violations of data protection law. Belgium did not have a specific sanctions regime, meaning that both criminal and civil procedures had to follow standard judiciary routes. The high-profile case against Facebook is still ongoing, several years after its initiation. This perfectly illustrates why there has been little if any privacy-related case law in Belgium over the past 25 years.

The GDPR, on the contrary, contains administrative sanctions that can be applied by the national supervisory authority. Member States can allow for limited exceptions on the fines, but the alternative sanctions still remain. Rules can only have an impact if infringements can be sanctioned.

2.4 Reformed supervisory authorities

The GDPR reformed the national data protection authorities. Given a new role and additional powers, they are now supervisory authorities. This also meant reviewing their organisation and internal processes. At the time of the Directive, some authorities were mere advisory bodies with limited impact.

The national authorities can now act as true regulators. They can inspect data controllers' and data processors' activities. They can even conduct an on-premise or IT search, and issue administrative fines. These new powers often required recruiting additional staff to provide them with new knowledge and additional competences. Instead of a purely formalist legal approach, as could be expected from an advisory body, they have now acquired experience from the field that was previously not available to the supervisory authorities.

2.5 Increased data controller awareness

Most data controllers (companies, public authorities…) are more aware of how to handle personal data in line with GDPR requirements, and to act accordingly. There is a real change in actions, not just a perceived change. Many controllers have also reviewed their business processes to align them with GDPR requirements.

In addition, data controllers have a better handle on their business as a whole. A successful GDPR implementation requires data controllers to have an accurate and comprehensive view of their activities and specifically the personal data they treat. To make the GDPR implementation more profitable, some data controllers conducted an in-depth review of their entire business, to improve business efficiency overall. Some even used it to implement ISO 27000- and NIS-related measures on top of other business process and data management improvements, such as incorporating privacy by design.

2.6 Risk-based approach

Respecting the GDPR implies first of all assessing risks. It is not sufficient to start collecting consent or including information in the general terms and conditions. Different interests must also be balanced based on their respective importance. This does provide data controllers with more control over their business, as they have made their decisions in a more considered way.

A realistic balance, for example, has been struck between the interests of data controller and data subject in the area of the legal basis of consent and legitimate interest. It will be crucial to maintain the current balance to preserve the acquis of GDPR.

2.7 Data protection-related case law

There is now the option to contest the decision of a supervisory authority in regular courts but using a shortened judiciary procedure. As a result, the administrative sanctions enter the realm of the judiciary, potentially giving the sanctions an additional weight: a transformation from administrative practice to case law. This puts it at the same level as doctrine and legislation from a legal practitioner's point-of-view. At the time of writing, four appeals have been decided under the new legal process[2].

The possibility to appeal a decision also endows a factual accountability principle on behalf of the supervisory authorities. Supervisory authorities thus have an incentive to ensure a high level of quality in their decisions. The more decisions that pass scrutiny by the courts, the higher the impact and standing of the supervisory authority's decisions.

2.8 Data protection as competitive advantage

Data protection has become a sales argument for some companies. GDPR compliance can also become a deal-breaker or -maker for both EU and non-EU companies. During the Covid-19 pandemic, certain solutions were banned by both government (departments) and private companies, due to insufficient security both from a technical and a data protection perspective.

Data protection issues are at times the canary in the coalmine. Not incorporating data protection properly in the development process, usually makes it a weak link. And a chain is only as strong as its weakest link. By incorporating data protection properly in development, you will obtain a more resilient end product.

[2] https://www.gegevensbeschermingsautoriteit.be/arresten-marktenhof; https://www.autoriteprotectiondonnees.be/decisions-de-la-cour-des-marches

2.9 Data protection as mainstream discussion topic

When we look at GDPR two years on, we cannot ignore the Covid-19 crisis, which has given rise to questions on the legitimacy of tracking individuals. There have been two predominant views. One is that the GDPR has the right provisions and allows for such collection insofar as processing is necessary, proportionate and fair. Another viewpoint holds that allowing tracking will demean the privacy laws. Regardless of your own perspective, even in time of pandemic, GDPR has been one of the most talked about laws in both the niche as well as mainstream press. Few people would have imagined data protection as an elementary factor in such discussions a decade ago.

3 Room for further improvement

In this section, we consider aspects of GDPR where we feel additional improvements would be welcome.

3.1 Administration & formalities

GDPR documentation and transparency obligations require a significant amount of work and generate a considerable number of documents. But does this actually advance personal data protection? The GDPR allows for a risk-based approach, but the administrative burden stifles this to some extent. Why is extensive documentation needed if there is proven to be little or no impact of data processing on a data subject? And is it truly necessary to separate a privacy policy and cookie notice on a website?

Notification of data breaches also leads to lots of debate and frustration. People still struggle to determine whether notification is required; there is no practical guidance or standard practice in this respect. Many also consider the 72hr notification term to be impractical. 'Three working days' (or maybe even five?) would have been a more realistic notification period.

3.2 Member State options

The GDPR leaves room for Member State options, resulting in differences between Members States' legislation that the Regulation was supposed to eliminate.

HR and scientific data are usually subject to Member State law. Hence, there are no uniform rules throughout the EU, which is an issue for:

- Outsourcing
- Secondments
- IT-tools for employee assessments
- …

Related processes, however, are quite similar throughout the different countries. Belgium has some laws and collective labour agreements, where GDPR is not really helpful. Belgium has not updated laws as a result of GDPR. An EU-wide approach is thus extremely difficult for pan-EU companies, due to these many national differences. The GDPR coherence mechanism does not mitigate the effects of Member State options.

3.3 Dispersed instead of centralised supervision

Supervision is attributed to the national supervisory authorities. A coherence mechanism and a 'one-stop shop' are intended to mitigate negative effects of this attribution. But these are no replacement for a unified or harmonised supervision. Some national regulators are also overburdened because of the one-stop shop, Ireland being the prime example. The GAFAs have all based their main EU establishments in Ireland. This puts the entire burden for supervision of their EU activities on the Irish supervisory authority, resulting in a bottleneck. The GDPR does not have a mechanism to overcome bottlenecks caused by the one-stop-shop mechanism.

The EDPB is neither sufficiently equipped nor mandated to provide efficient and effective assistance to national authorities. The GDPR copied the EU competition sanction regime but left out the associated tiered supervision and enforcement mechanism. The enforcement approach by national supervisory authorities can also be improved.

3.4 Enforcement approach

Supervisory authorities should avoid being perceived as all bark but no bite. In this regard, they should be attentive to two aspects:

1. Sanctions they impose
2. Data protection frame of reference

The publication of the GDPR caused a lot of hubbub regarding the included sanction regime. Most people certainly recall the doomsday style of some communications. While no one, especially the supervisory authorities, wants those concerns to become reality, the GDPR will not reach full adoption without proper and adequate sanctions for infractions[3]. The GDPR foresees a range of both financial and operational sanctions. Simply announcing that sanctions will be issued, does not suffice, nor does issuing sanctions for minor offences or setting an example that isn't perceived as such. An effective response to infractions is key in this respect. So far, the GDPR still has to deliver on its promise.

Enforcement also requires clarity on the data protection frame of reference: what rules must data controller abide by? How can a data controller be assured his approach is judged on its merits? The GDPR is one element of this frame of reference. In addition, the European Data Protection Board and national supervisory authorities issue opinions on different aspects of the GDPR. But there is a big question mark hanging over the value of the opinions of the supervisory authorities and the EDPB. Some consider them as an annex to the GDPR, thus carrying similar weight. Others view these opinions as irrelevant, and only consider the GDPR and related national legislation. Recent case law could hint towards this second approach, but the relevant opinion predated the GDPR.

[3] NY Times, Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates: https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

The baseline should be that supervisory authorities' opinions provide data controllers with a clear frame of reference for their data processing operations, giving data controllers the freedom to make choices best in line with their activities. Or they clearly take the position that the controller can determine his own approach[4], subject to respect of the accountability principle.

And sometimes maybe all that is needed, is a nudge to get things moving in the right direction...

3.5 Data subject benefits

While the GDPR has brought benefits to the data subjects, the latter seem hardly aware of these, and see only the negatives, such as cookie consent banners and cookie walls. Only data subjects who have been involved in a GDPR implementation project appear to perceive the benefits. Thus far, the benefits for data subjects have failed to gain awareness.

This is a point on which supervisory authorities should indeed increase their efforts. Much effort has been dedicated to data controllers, but very little to the beneficiaries of the GDPR: the data subjects. A high-profile campaign is needed to reach all data subjects, with adequate and digestible information to get the public's attention. Once that has been achieved, subsequent communication efforts need to further the understanding of the importance and the benefits of the GDPR for the data subjects.

To reduce the perceived inconveniences of the GDPR, more attention should be paid to so-called 'dark patterns'[5]. These are methods used by data controllers to 'push' data subjects in the direction most beneficial to the data controller. These dark patterns are not limited to personal data protection, but are also used in commercial settings, negating other consumer rights. While many of these dark patterns appear to comply with the law, this is only in appearance.

3.6 Standards information deficit

Data controllers experience difficulties collecting information on the standards that are relevant for their compliance. While there are a multitude of relevant standards today, they are not labelled appropriately and are thus difficult – even impossible – to find.

Regarding data breach notification, the first question is usually "Do we need to notify?" They would welcome additional guidance in order to accurately assess when notification to the supervisory authority is in fact required.

Open data is another complex issue. The GDPR should have gone a bit further than just requiring 'adequate measures' to ensure personal data protection. Without further elaboration, the term 'adequate measures' lacks any substance. At the very least, a framework with relevant criteria to help identify what are 'adequate measures', would be valuable. Such an approach was taken for data protection impact assessments[6]. But we would still first require clarity on the personal data protection frame of reference.

---

[4] *Dutch only*: Brussel 19 februari 2020 (rolnummer 2019/AR/1600): https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Arrest_190220.pdf
[5] https://www.darkpatterns.org/
[6] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

3.7 ePrivacy as Damocles' sword

Personal data protection in electronic communications is at present still subject to the ePrivacy Directive 2002/58/EC. The initial plan was to have a revised legal framework, an ePrivacy Regulation, that would become applicable along with the GDPR. The legislative process for both texts was started at the same time, but progress has stalled on ePrivacy. This has resulted in an incomplete framework, that to some extent also hampers proper GDPR implementation.

Currently, it is unclear where the discussions on ePrivacy will land, let alone when. The result is a significant gap in data protection legislation regarding electronic communications. The problematic ambiguity in turn creates opportunities for abuse. It also puts a big question mark over the legal compliance of any new online tool or application under development or being updated.

3.8 Role of the DPO

Data Protection Officer is a central role in GDPR implementation. While it has been described extensively in both GDPR and DPA guidance documents, DPOs are experiencing serious difficulties in fulfilling the role. This relates to the position in the organisation, the resources made available, etc. To what extent can a DPO rely on external expertise when executing tasks? There is also no frame of reference to properly assess the professional qualities of a DPO, which makes selection of a 'qualified' person a bit hit-and-miss. Even decisions by the supervisory authorities on this subject provide little to build on[7]. There is a recent decision regarding the independence of the DPO and conflicts of interest with other roles[8]. In many countries the role is rather new and is still suffering from growing pains.

One concrete illustration of the difficulties is the role of the DPO in a Data Protection Impact Assessment (DPIA). The DPO should be involved, but the exact role is not clear. Should he just assist in the process, should he guide the process, should he manage the process? The data controller is the responsible party for the DPIA, but in practice this responsibility tends to be shifted to or even assumed by the DPO. This contradicts the clear definition of the role in the GDPR: advisory and controlling, but not executing the DPIA itself. This is despite the fact that a DPIA is (in theory) simply a risk assessment using common risk assessment methodology but focussing specifically on data protection. Hence, a DPIA would ideally be part of the company's general risk management process.

[7] *Dutch only*: GBA 15/2020 15 april 2020 Klacht wegens de verwerking van de persoonsgegevens van huurders via de belastingaangifte door een gemeente
[8] *Dutch only*: GBA 18/2020, 28 april 2020 Risicobeoordeling door Y betreffende melding van gegevenslekken

3.9 Professional or academic data protection qualifications

How can you demonstrate, for example, that your DPO or your privacy officer is 'qualified', if there is no benchmark available[9]? The GDPR imposes different requirements on a DPO without further specification. This also complicates the situation for privacy professionals who wish to expand their knowledge.

To this day, there is still no benchmark for assessing data protection qualifications. There are many training programmes, and the International Association of Privacy Professionals has its certification scheme. But there appears to be no proper academic or professional qualification that can be obtained today by privacy professionals. According to supervisory authority opinions and the text of the GDPR, the certification schemes as foreseen by GDPR do not cover natural persons and thus exclude DPOs.

4 Conclusion

The GDPR is certainly a step forward in personal data protection. Many aspects had already been declared 'good practices' in the past, but by incorporation into the GDPR have obtained mandatory legal status. Data controllers have adapted to the new rules and changed their ways, but we are not there yet. This is partly because discussions continue on the application of the GDPR, partly because enforcement is lagging, and partly because the administrative burden is high. Moreover, data controllers are dealing with legacy issues. The stalled legislative process of the ePrivacy Regulation is a liability for current implementation, as these may have to reviewed in-depth in the near future.

Taking stock after two years, it seems clear that there is still quite a bit of improvement needed.

[9] *Dutch only*: GBA 15/2020 15 april 2020 Klacht wegens de verwerking van de persoonsgegevens van huurders via de belastingaangifte door een gemeente

Beltug vzw/asbl

Prins Boudewijnlaan 97 | B - 9100 Sint-Niklaas | +32 3 778 17 83

BE 0443-557-046 | RPR Gent, afdeling Dendermonde

www.beltug.be | info@beltug.be