Point your toe and leap into your privacy program!

Learning from Belgium as you leap into your privacy program

It is now February 2020. With an extra day in this leap year, it is the perfect opportunity to "leap" into your privacy program! To help you, we'll take a look at the priorities that the Belgian Data Protection Authority (DPA) set in its draft Strategic Plan for period 2019-2025 in accordance with the Belgian DPA Act (Art. 9). A public consultation on the plan was opened until January 7, 2020. A final version of the plan should follow. The 50-page strategic plan contains a wealth of information about the organization of the DPA, but this summary only focuses on the (practical) priorities set by the DPA for the next six years. Depending on your business, some priorities may be more relevant to you than others. You can find the complete report on the DPA's website (in French and Dutch).

The DPA defines its mission as "guiding citizens, businesses, associations, and public authorities towards a digital world where everyone can truly enjoy their privacy." To that end, they have set six strategic objectives around data protection:

- Better data protection by building awareness
- Better data protection by enforcing the law
- Better data protection by identifying trends and responding to them
- Better data protection through collaboration
- Better data protection with the DPA as a leader and a reference center
- Better data protection with the DPA as an effective controller

The DPA will need more financial and human resources to implement its plan, and it sets its priorities for the next six years based on a risk approach (looking at the number of data subjects, the quantity of personal data, the type or sensitivity of the data, the data retention period, whether the data processing

is intrusive or not, the potential use of new technologies that must be regulated to avoid deviations, etc.).

The DPA will target its actions toward specific sectors, GDPR instruments, and social themes.

Targeted sectors:

- **Telecom and media companies:** These companies have access to many of their users' geolocation data, highly personal data, and identifiers. Moreover, since the sector is highly competitive, companies could be eager to use this data to obtain a competitive edge. Therefore, the DPA will closely watch how this data is used, if adequate security measures are taken, and how data is being reused by businesses and their partners.
- **Public authorities:** Public authorities have access to a vast array of personal data that can be very sensitive (citizens' earnings, assets, debts, and criminal convictions). For this reason, the DPA wants to guide and control public authorities; to ensure transparency (i.e., data must be accessed and used for the purposes for which it was collected or for compatible purposes); and to ensure that data subjects can exercise their rights. Data protection officers must perform their duties and tasks in an appropriate manner, and public authorities must lead by example. Click here to read about two fines imposed by the DPA in this regard.
- **Direct marketing (included data brokers):** The DPA wants to ensure that businesses have transparent, GDPR-compliant practices and that individuals maintain control over the actual use of their data. Users must, among other things, be notified beforehand when their data is used for profiling and be able to exercise their right to object. In this regard, the DPA issued a 78-page recommendation on direct marketing (in French) in January 2020.
- **Education**: The DPA is especially concerned about this sector since its data subjects are minors. Schools and their service providers are using digital technologies more and more, including pictures, e-learning tools, and data pertaining to students suffering from health issues, etc. They also transfer data to third parties.
- **Small and Medium Enterprises:** SMEs must be guided through guidelines and simple, easy-to-use tools since they typically do not designate a data protection officer to help them understand the concrete impact of privacy laws on their activities. Trade associations have an important role to play here, and the DPA intends to help them with information campaigns, document templates, and general recommendations.

Targeted GDPR instruments:

- **The data protection officer's (DPO's) role:** There is actually a lot of confusion and misunderstanding regarding the role of a DPO. The DPA emphasizes that a DPO must perform his or her duties and tasks in an independent manner, and that the DPA's inquiries will be aimed at identifying entities that have designated a DPO but do not allow him or her to act in accordance with the legal framework.
- **The lawfulness of processing – the controller's legitimate interest:** The DPA will have a closer look at data processing activities based on the data controller's legitimate interests in order to make sure this legal basis is not misused. The DPA wants to enforce penalties for violations of this GDPR principle.

- **Individuals' rights (access, rectification, transfer, etc.):** The DPA considers data subjects' rights to be a cornerstone of GDPR and believes it must act when individuals are not able to exercise their rights. It intends to enforce penalties against data controllers that have no system in place to respond to data subjects' requests to exercise their GDPR rights. Click here to read about the €2,000 fine imposed on a nonprofit association.

Targeted social themes:

- **Pictures and cameras:** Many individuals submit inquiries related to pictures and video clips that have been taken and broadcast. The DPA must update its website to post information on the technological developments so that incoming questions can be answered. It sees the illegal broadcast of pictures and videos as seriously undermining citizens' fundamental rights and freedoms.
- **Online data protection:** The data collected through cookies and enriched with other off-line data can be used to predict and/or impact our behaviors. The DPA emphasizes that data subjects must be notified of such data collection practices so that they can freely decide whether they consent or not to these practices. The DPA also considers it essential to take enforcement measures against entities that do not comply with these transparency rules and the legal basis for this type of data processing. It also prioritizes awareness campaigns and guidelines on data security. And last but not least, the DPA considers the data protection of young Internet users to be at stake since children are not aware of all of the associated dangers.

  Click here to read about the €15,000 fine that the DPA imposed on a website for its noncompliant cookie management and privacy policy. This decision offers a variety of key information for any foreign company doing business in Belgium. In a next issue, we'll look at the findings that led the DPA to impose this fine.

- **Sensitive data:** The use of so-called "sensitive data" (see GDPR, Art. 9(1)) is intrusive and must be highly regulated. The recent scandals involving the use of citizens' political trends to influence their votes show how important it is to review these practices. The use of biometric data for identification purposes also shows that individuals probably do not know these practices are forbidden. In this respect, the DPA will reinforce its position on the reuse of medical data.

Like the Belgian DPA, you might have a limited budget for your privacy program. I hope these key takeaways from the DPA's strategic plan will guide you as you set your own priorities for your privacy program if you're doing business in Belgium. For more inspiration, click here to watch the new data privacy and transparency promise given by IKEA to its customers, and let me know whether this user-centered approach might suggest a good long-term investment for your own organization.

Are you interested in solving the mystery of the above-mentioned €15,000 fine sooner than next month? Email me, and I might issue a special edition!

Enjoy your extra day this year! Point your toe, smile with confidence, and take a giant – or a modest – leap in your privacy program!