Belgium used its implementation of the European Union General Data Protection Regulation legislation to expand the country’s Privacy Commission’s members to include at least six independent support agencies, including an “inspection body” and a “dispute resolution chamber,” the authors write.

Data Protection Litigation to Become a New Reality in Belgium

BY JAN DHONT, LAUREN CUYVERS, AND DAN FELZ

On Nov. 16, 2017, the Belgian Senate adopted an “Act on the Establishment of the Data Protection Authority.” Following Austria, Germany, and the U.K., Belgium became the fourth EU member state to pass a domestic statute implementing the General Data Protection Regulation 2016/679 (GDPR) before its effective date of May 25. The new Belgian Act sets forth the structure and legal organization of the data protection authority (DPA), which will supplant and serve as the successor to the current Belgian Privacy Commission. More importantly, the Act significantly broadens the DPA’s powers. The DPA's function will evolve from being predominantly advisory to truly corrective, and even potentially punitive. With the publication of the new Act in the Belgisch Staatsblad on Jan. 10, the final step in the legislative procedure is complete. The Act should enter into force on May 25 (simultaneously with the GDPR).

National Implementing Legislation Targeting DPA Powers

The Act was drafted in light of the GDPR, which entered into force on May 25, 2016, and will be enforceable in all EEA member states, including in Liechtenstein, Norway, and Iceland, starting May 25. As of that date, the current legislative data protection frameworks in the member states will no longer apply but will be replaced by the framework of the GDPR on the one hand and local legislation of the member states implementing the GDPR on the other. The GDPR requires and permits member states to adopt deviating or supplementing local laws in a number of areas, including the establishment of their local supervisory authority.

The Belgian Parliament took this opportunity to not only lay down the structure and organization of the new DPA, but also—for the first time—to clearly establish its competencies and its relation to other comparable supervisory agencies. In short, the Act expands the Privacy Commission’s members to include at least six independent support agencies (supplemented further by independent experts and a “reflection council”), the most remarkable being an “inspection body” and a “dispute resolution chamber.” These two agencies will each exercise true investigatory and corrective powers,
comparable to powers exercised by a public prosecutor in criminal investigations.

**A Solid Structure Inspired by Other Belgian Supervisory Authorities** The Act’s reform of the DPA’s structure is prompted by this significant increase in powers. The six newly instituted agencies are structured in light of this and include an executive committee, general secretariat, frontline service, knowledge center, inspection body, and dispute resolution chamber. The inspiration for this new DPA structure was found in—as the Act refers to it—“supervisory authorities with comparable powers” such as the Belgian Institute for Postal Services and Telecommunications and the Belgian Competition Authority, both of which have expansive competencies when it comes to investigations, administrative fines, and penalties.

**Inspection Body and Dispute Resolution Chamber** The most significant bodies introduced by the new Act are the inspection body (“inspectiedienst”) and the dispute resolution chamber (“geschillenkamer”). These two bodies truly transform Belgium’s prior advisory commission into a true enforcement agency with monitoring and corrective powers.

**Far-Reaching Powers of the Inspection Body** The powers granted to the inspection body are reminiscent of powers typically found in criminal investigations. They include the interrogation and written examination of individuals, on-site investigations, the consultation of information technology systems and copying of relevant data, the seizure or sealing of assets or IT systems, and summoning the identification of the subscriber or regular user from a telecoms operator. In addition, the rights granted to individuals subjected to an interrogation are reminiscent of the rights usually present in the case of criminal interrogations, notably the right to counsel, the right to obtain a free copy of interrogation transcripts, and the right to request performance of specific investigatory acts. The inspection body is also empowered to impose preliminary measures, such as a temporary suspension, restriction, or freezing of processing activities, leading to a potentially major impact on businesses subject to investigations by the inspection body.

The Act’s enforcement ambitions are further reflected by the scope investigations could potentially
grow to. Individuals and entities subject to investigation are under a legal duty of cooperation, which the Act’s Explanatory Memorandum compares to the duty of cooperation applicable to investigations by the Financial Services and Markets Authority (FSMA). Individuals and companies are required to hand over all information (save privileged information) that may serve to establish a data protection violation. The DPA bears a potentially light burden in justifying its opening of an investigation; more often than not, the DPA can exercise its powers “whenever it is deemed necessary,” with the DPA being free to interpret what is “necessary” in specific circumstances.

Sanctions Taken by the Dispute Resolution Chamber
The dispute resolution chamber is the final step in the DPA’s administrative procedure path, and it is the body empowered to impose sanctions. It is an administrative body competent to exercise the so-called “corrective powers” granted to supervisory authorities under the GDPR. Its specific structure and organization strongly resemble a judicial institution or body, or Article I courts within the U.S. The chamber’s most significant corrective powers exist in the issuing of warnings and reprimands, the ordering of compliance with data subjects’ individual rights requests, the temporary or definite freezing or restricting of processing activities (or a ban on the processing altogether), enjoining processing to be brought into compliance with data protection laws, imposing penalties and administrative fines of up to 20 million euros ($24.59 million) or 4 percent of worldwide turnover, suspending cross-border data transfers, revoking privacy certificates, and publishing its decisions on its website.

Rules of Procedure The Act’s rules of procedure aim to enhance the effective protection for individual privacy rights, as well as regulating rights of defense and means of legal redress before the DPA and the regular civil courts. A procedure before the DPA is typically initiated by a request or complaint, but may also be initiated by the DPA on its own initiative in a number of situations. The rule for complaints and requests is that any individual, as well as associations and institutions, have legal standing to file. Here, Belgium seems to have taken advantage of the margin of manoeuvre the GDPR grants member states to permit representative bodies to autonomously bring actions directly against regulators, controllers, or processors—i.e., without an individual’s mandate. Beyond doctrinal considerations, allowing representative bodies to autonomously initiate data protection investigations/proceedings significantly increases the chance that companies will be faced with some form of data protection scrutiny. Unlike most individuals, professional representative bodies are less likely to be intimidated by administrative hurdles or long proceedings.

Frontline Service All complaints and requests are filed with the DPA’s frontline service, which will conduct preliminary triage and decide on the admissibility of complaints and requests. Admissible complaints are transferred to the dispute resolution chamber, which can lead to either an investigation by the inspection body or, if the chamber decides sufficient evidence is available, administrative proceedings before the chamber itself. Information or other requests to the DPA are handled by the frontline service itself, which provides the requestor with the necessary information. Alternatively, the frontline service may also decide to initiate mediation to try and find common ground between both parties. If no solution is found in mediation, requests are treated in the same way as complaints and will be transferred to the dispute resolution chamber.

Inspection Body
The “intermediary” chain in the procedure is the inspection body, which is responsible for conducting investigations to secure sufficient evidence for proceedings on the merits before the dispute resolution chamber. The inspection body is also competent to impose preliminary measures (with a maximum duration of six months) when this is necessary to prevent an irreparable harm to the rights of the individual.

In light of procedural options, it is important to note that the defendant, after having been confronted with a preliminary measure, may request to be heard, file written or oral objections, and—most importantly—file an appeal against the measure with the dispute resolution chamber. The appeal, however, does not suspend the challenged measure (unless the chamber so orders), which raises questions about the practical impact or use of this procedural move. To prevent this, we recommend parties specifically request measures to be suspended until a final decision has been obtained in appeal (i.e., that the decision is “niet uitvoerbaar bij voorraad”).

Dispute Resolution Chamber
The final chain in DPA procedure is the dispute resolution chamber, which will decide the case on the merits, meaning finding facts and imposing appropriate sanctions. In principle, proceedings before the dispute resolution chamber are written, though the chamber may decide to organize oral hearings. The procedure before the chamber can take two turns: either the chamber decides to request (additional) investigation from the inspection body, or it decides to follow a “summary procedure” in which it treats the complaint autonomously without consulting the inspection body. The latter option goes hand in hand with very limited notifications to parties involved in the proceedings—which may significantly reduce procedural options. If an investigation is requested, parties are generally offered a broad range of procedural safeguards, such as appropriate notifications, the filing of a defense strategy, the right to have all relevant exhibits attached to the file, and the right to be heard.

Administrative Sanctions Accumulation
In terms of potential fine accumulation when a business is found to violate several data protection law provisions, the Act makes a distinction based on the situation where several distinct acts lead to multiple violations and in cases where one and the same act infringes several data protection law provisions (for instance, due to a common core of fact able to be qualified as multiple violations). It is only in the latter case that only one fine applies: the highest administrative fine. In the former case, administrative fines will be added up, subject to a cap at the level of the “highest administrative fine times two.” This may have significant implications for businesses facing privacy litigation before the Belgian DPA for several potential infringements.

Appeal
As soon as the dispute resolution chamber renders a
decision, the parties may file an appeal within 30 days
with the Commercial Court of Appeal (“Marktenhof”),
which will deal with the case in accelerated proceed-
ings on the merits (“zoals in kort geding”) to allow for
timely judicial relief. This appeal procedure will in
principle not have suspensive effect, meaning the dis-
pute resolution chamber's decision will be executable
pending the appeal procedure. In light of this, it is
recommended parties involved in proceedings at the
level of the dispute resolution chamber are prepared
to execute an unfavorable decision if needed. In the
same way, a decision from the dispute resolution
chamber establishing a violation of data protection
law can serve as a basis for the individual plaintiff to
bring a damages claim before the competent civil
court.

BY JAN DHONT, LAUREN CUYVERS, AND DAN FELZ
To contact the editor responsible for this story: Bar-
bara Yuill at byuill@bloomberglaw.com