GDPR: Belgium sets up new Data Protection Authority

5 February 2018

INTRODUCTION AND SUMMARY

On 10 January, the Belgian Gazette published the Law of 3 December 2017 "setting up the authority for data protection" (the "Law").

The Law contains seven Chapters, divided into 114 Articles. It is the first legal text in Belgium applying various provisions of the EU's General Data Protection Regulation ("GDPR"). Under the GDPR, EEA Member States must provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR, in order to protect fundamental rights and freedoms of personal persons in relation to processing and to facilitate the free flow of personal data within the European Union. The Law therefore sets up a new "Data Protection Authority" ("DPA") in Belgium. With effect from 25 May 2018, it replaces the current body, the Commission for the Protection of Privacy ("Privacy Commission").

This briefing sets out a preliminary assessment of the Law. It then describes the main rules under the Law and how these relate to the GDPR, for example the DPA's powers to cooperate with other authorities and its power to impose fines prescribed by the GDPR itself.

PRELIMINARY ASSESSMENT OF THE LAW

Protection of personal data has become a major concern for corporate management – on a par with prevention of money laundering, bribery and corruption and anti-competitive behaviour – and so calls for a comparable regulatory and compliance approach.

Although not a "big player", Belgium is often at the forefront of developments in EU law, including in the protection of privacy. The DPA's predecessor, the Privacy Commission, has been active: its most recent annual report (2016) states that it dealt with nearly 4,500 cases in 2016, *i.e.* over 4,000 requests for information and for mediation, and 332 supervisory matters. It has also been one of several authorities across the EU which has sued Facebook – so far with mixed success due to thorny jurisdiction questions, which have also arisen in other disputes with Facebook and other social media providers.

The DPA will doubtless continue the Privacy Commission's advisory role, but the Law also grants extensive powers to the DPA: it remains to be seen whether the DPA will merely exhort rather than enforce. Much will depend on the composition of its Executive Committee (replacing the current team and described below). The DPA will need to press for sufficient budget to attract the personnel necessary to exercise its powers and to burnish its image as a truly independent authority (fines are not a source of financing, since, as noted below, fines are payable to the Treasury, not the DPA).

If the DPA does "show its teeth", the Law's extensive provisions on investigations by the DPA's Inspection Service, on preliminary measures by its Disputes Chamber and on the Chamber's proceedings on the merits will become familiar reading. The rights of the defence and other safeguards guaranteed in the Law will be put to the test. The ultimate sanction is, however, loss of reputation: no serious economic operator wants to face allegations – often highly publicised - that it has been negligent in its protection of the personal data of its customers.

THE DPA AND ITS OFFICIALS

Chapter 1 comprises introductory provisions, including definitions of: the DPA, clarifying that the Authority protects personal data in accordance with the scope of the GDPR itself; and the DPA's inspectors, *i.e.* a contractual or statutory official of the DPA responsible for identifying breaches of the Law and other laws containing provisions on processing of personal data.

THE DPA: DUTIES, POWERS, COMPOSITION, ETC.

Chapter 2 (Articles 3 to 32) sets up the DPA as successor to the Privacy Commission. The DPA has legal personality and its seat in Brussels. It is responsible for supervising compliance with the fundamental principles for protection of personal data under the Law and other data protection rules. Subject to the various competencies devolved under Belgium's federal system, the DPA carries out its duties throughout the Kingdom of Belgium. Its supervision does not, however, extend to processing by the courts and the public prosecutor. Separate provisions also apply to the police. The DPA's decisions must be dated, signed, and set out reasons; decisions must specify how they may be appealed.

The DPA carries out its duties exclusively for the general good: unless specifically provided by law, its executives and members of its staff are excluded from civil liability for their decisions, acts or behaviour when carrying out the statutory duties of the DPA. The DPA is empowered to bring breaches of fundamental principles of data protection to the attention of judicial authorities; it has capacity to bring proceedings to enforce these fundamental principles.

The DPA comprises six bodies:

- The Executive Committee: it approves the annual accounts and decides on the annual budget and report, strategic and management plans and priorities of the DPA, and, generally, overseas the DPA's work. It monitors developments affecting protection of personal data. The Law sets out the composition and meetings of the Committee, including the duties of its Chair, (the President of the DPA). The President is responsible for cooperation among, and coordination of, the various bodies of the DPA, preparing budgets, accounts and various strategic and other plans and priorities. The President represents the DPA vis-à-vis third parties.

- The General Secretariat: this Secretariat has "supporting horizontal tasks", *i.e.* management of human resources, budget, IT, legal questions, communications, etc. It also has executive tasks, including monitoring socio-economic and technological developments affecting protection of personal data, drawing up the list of processing activities requiring a "data protection impact assessment" and other tasks contemplated by the GDPR itself (opinions, approval and monitoring of codes of conduct, certification procedures, and approval of model contact clauses and binding corporate rules).

- The Frontline Service: this service receives complaints and requests, commences a mediation procedure and promotes awareness among the public, especially minors, of protection of personal data, and among controllers and processors of their duties. It keeps data subjects informed of their rights.

- The Knowledge Centre: this centre issues opinions and recommendations in relation to protection of personal data, taking into account necessary, technical and organisational safety measures. Additional provisions set out its composition and procedures. It receives requests for opinions by recorded delivery letter or using a form to be made available on the DPA's website. Subject to certain exceptions, the centre must give its opinion within 60 days (15 days in urgent matters). Its opinions are in writing and must set out reasons. Opinions and recommendations are published.

- The Inspection Service: this service is the investigative arm of the DPA. It is headed by an inspector general and is made up of inspectors (as defined above) and a secretariat. Internal rules will set out details of the profile and competences expected of inspectors. When carrying out their duties, the inspector general and inspectors must carry their DPA identity card and show it immediately on request.

- The Disputes Chamber: this is the body within the DPA responsible for administrative proceedings. The Law outlines the composition and specialisations of the Chamber's six

members and its President. Internal rules will set out requirements for this Chamber, including its working methods. The Chamber has a secretariat which also acts as a registrar for proceedings.

In addition to the DPA bodies listed above, an independent think-tank assists the DPA by providing non-binding opinions on data protection questions.

APPOINTMENT OF MEMBERS OF DPA BODIES

Chapter 3 (Articles 33 to 41) provides for the appointment of members of the Executive Committee, Knowledge Centre and Disputes Chamber, including general conditions for their appointment. By way of example, appointment is open to citizens of the EU, but not to persons who hold political appointments, such as a member of the European Parliament or as an official in a public function. The Chapter also sets out the procedure for appointment.

AN INDEPENDENT AUTHORITY

Chapter 4 (Articles 43 to 51) addresses the independent status and operations of the DPA. Members of the Executive Committee, the Knowledge Centre, the Inspection Service and the Disputes Chamber must not, directly or indirectly in the performance of their duties, accept requests or take instructions. They are subject to rules on conflicts of interest, incompatibilities and security of tenure. The organisation, status and recruitment of the staff of the DPA are to be set by Parliament on a proposal from the DPA. The Law is succinct regarding financing of the DPA: the general spending budget for the State will include provision for the ADP's operations. Separate provisions address the ADP's budget, accounts, including remuneration of officials, and reporting to Parliament and the government. Its reports will be public and notified to the European Commission and the European Data Protection Board.

The Law grants the DPA access to specified registers. In general, DPA members and personnel are subject both during and after their appointment to a duty of confidentiality in relation to facts, acts or information which come to their knowledge by reason of their duties. The DPA can also enter into confidentiality agreements with third parties.

NATIONAL AND INTERNATIONAL COOPERATION

Chapter 5 (Articles 52 to 56) comprises provisions on the DPA's cooperation with other entities. At the national level, the DPA fulfils its tasks "in a spirit of dialogue and cooperation" with all public and private sector entities interested in the protection of fundamental rights and freedoms of natural persons in relation to the processing and flow of personal data, and in the protection of consumers. It may be assisted by, or act on the request of, other public entities acting within their own statutory responsibilities. It may also launch its own public enquiries or consultations, and set up or participate in appropriate committees or groups, subject always to its duty of independence. Its Executive Committee may delegate powers to its bodies or officials to represent it within such committees or groups and to vote within them. The DPA's President or other members of the Executive Committee may be heard by specified parliamentary commissions.

Internationally, the DPA may cooperate with any body or other data protection authority of another State in accordance with powers under the GDPR or national rules, for example to set up expert groups, exchange information, provide mutual assistance for supervisory purposes and share knowledge and financial resources.

ADMINISTRATIVE PROCEEDINGS

Chapter 6 (Articles 57 to 108) regulates proceedings before the DPA. The language to be used by the DPA in proceedings must reflect the needs of the matter.

Articles 58 to 62 address admissibility of a complaint or an application. Any person may file a complaint or application with the DPA; it must be in writing, dated and signed. The DPA will also provide a suitable form. There is no charge for the filing. The Frontline Service checks whether the complaint or application is admissible (use of a national language, within the DPA's jurisdiction, whether additional information is required, etc.) and so informs the complainer or applicant; a refusal of admissibility must set out reasons. If admissible, the complaint is forwarded to the Disputes Chamber, whereas, with regard to applications, the Frontline Service processes these directly itself, including, subject to additional provisions, mediation. If mediation fails, the application is treated as a complaint: if, following analysis by the Frontline Service, it presents "solid evidence of a practice which may breach fundamental principles of protection of personal data", whether under the Law or other personal data legislation, it may be transferred to the Disputes Chamber for further review.

Articles 63 to 91 contain detailed rules on proceedings before the Inspection Service, including:

- Referral to the Service by designated persons (the Executive Committee, the Disputes Chamber, etc.) and on its own initiative (where based on solid evidence of a practice in potential breach).

- Investigation by the Service within the scope of the supervisory competences conferred on the DPA by the Law: such powers must be used "appropriately and as necessary"; the investigation is secret in principle until the Service reports to the Disputes Chamber. The Service may also call on the police for support.

- Competences of the Service: the inspector general and inspectors have power to: (i) identify and hear persons; (ii) launch written investigations; (iii) conduct on-site inspections; (iv) examine IT systems and copy data held on them; (v) access information electronically; (vi) seize or seal IT material and systems; and (vi) require identification of a usual subscriber or user of an electronic communications service of the means of electronic communications actually used. Persons subject to investigation must cooperate. The investigation may result in a breach report, which is conclusive until proven otherwise. A report is also required in the absence of breach. The Law organises how the contents of reports may be used, so, for example, use of personal medical data is subject to rules and medical secrecy, while other information may only be used on authorisation from the public prosecutor or an examining judge.

- Provisional measures to suspend, restrict or temporarily freeze processing of data: these are possible where an investigation discloses "a situation which may cause serious and immediate harm which will be difficult to repair". Such measures are subject to procedural safeguards (hearings, time limits and appeal to the Disputes Chamber).

- Information gathering: the inspector general and inspectors also enjoy general powers of investigation, supervision, hearing and information gathering in order to ensure proper compliance with rules on protection of personal data.

- Identification of persons: during an on-site inspection, the inspector general and inspectors have the power to request identification (including ID papers and other official or unofficial evidence of identity) of any person as required in order to carry out their duties. By means of a substantiated decision in writing, the inspector general may also identify a subscriber or user of an electronic communication service, including requiring assistance from a network provider and other designated persons. The decision must be proportionate taking into account respect for privacy and subsidiarity in relation to any other duty to investigate.

- Hearing: the inspector general and inspectors may organise hearings of any persons including in the presence of witnesses, experts and the police. Such hearings are subject to various safeguards and rights of the defence set out in the Law.

- Written investigation: the inspector general and inspectors have broad powers to seek information from any person and subject to deadlines which they specify.

- On-site inspections: if the inspector general and inspectors have reason to believe a rule on protection of personal data is being breached, they may enter an undertaking, service or any other location for the purposes of on-site inspection and reporting. The inspector general and inspectors may, however, only enter the premises of a person who is subject to professional secrecy (for example, a member of a Belgian Bar or of the medical profession) if: (i) the person concerned agrees; or (ii) an examining judge has granted an order; and (iii) a representative of the person's governing body is present. Similar provisions apply to entry into a private house. As for the above order, the inspector general must apply for it, in accordance with prescribed criteria and subject to other safeguards, such as entry during normal hours, notice of the purpose of the inspection and protection of the complainer.

- Consultation of IT systems and copies of data on IT systems: if the inspector general and inspectors have reason to believe a rule on the protection of personal data is being breached, they may consult IT systems and content held by the person concerned, either with that person's consent or, failing which, on an order from an examining judge. Such consultation includes on-site copies, extracts, etc. and, if this is not possible, IT systems may be seized. Consultation may also extend to the place of storage of data in another country where the data is publicly accessible in Belgium by electronic means or with the consent of duly authorised persons. Persons subject to such consultation must provide analytical, programming, management and operating data supporting the IT system. Translations may be required, as well as assistance and documentation in order to check the reliability of the data and processing. On their side, the inspector general and inspectors must take appropriate measures to ensure the integrity of data and material to which they have had access. More generally, when gaining access to, or copying, information which is electronically accessible to the public, with or without charge, they many not, however, "assume a credible [*sic*] false identity or use fictitious documents or interact personally with any person". They may test, directly or with the help of experts, security measures for information systems, subject to the consent of the person being checked, failing which on an examining judge's order. Finally, investigative measures are expressly excluded from hacking offenses as defined in the Criminal Code.

- Attachments and seals: the inspector general and inspectors may put seals on objects, documents or IT systems, or seize them, for the duration of their duties, subject to a limit of 72 hours. They may only do so for the purposes of information, or investigation or collection of evidence of breaches, or where a risk exists of such IT systems enabling continued breach or new breaches. These measures are recorded in a report which is provided to the person concerned. Seals and seizure may be selectively extended beyond 72 hours, subject to an examining judge's order and to a further report. Objects, documents and IT systems that have been sealed or seized are recorded in a specific register. Appeal against the above measures lies to the Disputes Chamber subject to a prescribed form and time period for such appeal.

- Closing an investigation: on determining that an investigation is complete, the inspector general and inspectors draw up a report for the matter. The inspector general may then: (i) forward the completed matter to the president of the Disputes Chamber or to the public prosecutor (when a criminal offense may have occurred); (ii) close the matter; or (iii) submit the matter to the data protection authority of another State. Additional provisions apply for potential offenses.

Articles 92 to 108 regulate proceedings before the Disputes Chamber. The following persons may refer matters to the Chamber: (i) the Frontline Service in relation to complaints; (ii) a person appealing against measures taken by the Inspection Service; and (iii) the Inspection Service following closure of an inquiry. Proceedings are in writing, but the Chamber can also hear the parties.

Before a decision on the merits, the Chamber may instruct the Inspection Service to investigate a matter, or to complete a previous investigation, or deal with a complaint directly. It enjoys discretion as to whether and how to proceed and so can: (i) order a matter to be reviewed on its merits; (ii) propose a settlement; (iii) close a matter; (iv) give warnings; (v) order compliance with the interested person's requests to exercise their rights; (vi) order interested persons to be informed of a security concern; (vii) transfer the matter to the public prosecutor; and (viii) on a case-by-case basis, publish its decisions on the DPA's website. The Chamber is also bound to inform parties of its instructions, and to comply with certain time limits and other safeguards.

In proceedings on the merits, interested parties are informed so that they can file pleadings, be heard and submit evidence. At this stage, the Chamber enjoys broadly the same powers as at the preliminary stage (see paragraph above). It can also order: (i) suspension, or temporary or definitive restriction or prohibition of processing; (ii) remedial measures; (iii) rectification, restriction or erasure of data, including appropriate notifications; (iv) withdrawal of authorisation of a certification body; (v) fines; (vi) suspension of international transfer; and (vii) filing of the matter with the public prosecutor. The Chamber may impose administrative fines in accordance with the general conditions set out in Article 83 of the GDPR (*i.e.* fines must be "effective, proportionate and dissuasive", applying the criteria set out in the Article and, for the most serious infringements, fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher). Any such decision must set out reasons as well as the amount of the fine. The fine is payable within 30 days. Aggregated fines are possible within limits.

Decisions imposing a fine or finding a person liable are extinguished five years after the facts in question. A five-year time-bar applies generally to punishable breaches and can only be interrupted by an investigation or prosecution. Fines are time-barred after five years, unless interrupted. Fines, including settlements, are paid to the Treasury (not the DPA). Finally, appeal, within 30 days of notification, against the decision of the Disputes Chamber, lies to the Market Court (this is a specialised chamber of the Brussels Court of Appeal). Unless specifically provided otherwise, the decision of the Disputes Chamber is enforceable, despite appeal. Proceedings before the Market Court are subject to relevant provisions of the Judicial Code.

FINAL PROVISIONS

Chapter 7 (Articles 109 to 114) comprises repeals, transitional and final provisions. Unless the King decides on an earlier date, the Law enters into force on 25 May 2018, except for Chapter 3 (appointments to the various bodies within the DPA), which is already in force. Additional provisions address current and pending authorisations, applications and complaints, transfer of personnel from the Privacy Commission to the DPA and expiry of related appointments on 24 May 2018.

CONTACT

If you have any questions concerning this briefing, please contact Philip Woolfson or Yves Melin (contact details below). This briefing should not be treated as a substitute for specific legal advice on individual situations.

Steptoe & Johnson LLP
Brussels office
489 Avenue Louise
B-1050 Brussels, Belgium
Tel: +32 (2) 626 0500
Fax: +32 (2) 626 0510
www.steptoe.com

Philip Woolfson
Partner, *Avocat* (Paris and Brussels, established in Brussels), CIPP/E
Tel: +32 (2) 626 0519
Mob: +32 475 68 12 16
Email: pwoolfson@steptoe.com

Yves Melin
Partner, *Avocat* (Brussels)
CIPP/E
Tel: +32 (2) 626 0512
Mob: +32 473 97 50 27
Email: ymelin@steptoe.com