

## Proceedings Before the Inspectorate



**Ms. Heidi Waem**  
Senior Associate



**Ms. Louisa Vandepitte**  
Associate

[heidi.waem@nautadutilh.com](mailto:heidi.waem@nautadutilh.com) [louisa.vandepitte@nautadutilh.com](mailto:louisa.vandepitte@nautadutilh.com)

On 10 January 2018, the Act creating the Data Protection Authority (the "Act") was published in the Belgian State Gazette. This newsletter provides information about proceedings before the Inspectorate, the investigative branch of the Data Protection Authority (the "Authority") which has a wide range of powers to investigate complaints. The procedural provisions of the Act will enter into force on 25 May 2018.

### Referral to the Inspectorate

Matters can be referred to the Inspectorate:

1. when the Executive Committee finds that there are serious indications of the existence of a practice capable of giving rise to a violation of fundamental personal data protection principles;
2. when, further to the filing of a complaint, the Dispute Resolution Body finds that examination by the Inspectorate is necessary;
3. by the Dispute Resolution Body further to a request for additional investigation;
4. at the request of the Executive Committee, in order to cooperate with the data protection authority of another state;
5. at the request of the Executive Committee if the matter is referred to the Data Protection Authority by a court or administrative body;
6. on its own initiative when the Inspectorate finds that there are serious indications of the existence of a practice capable of giving rise to a violation of fundamental personal data protection principles.

## **Investigative Powers**

The Inspectorate has a wide range of powers, similar to those of other regulatory bodies such as the Competition Authority. Where necessary, the Inspectorate may call upon the assistance of the police. The Inspectorate may also carry out joint operations together with the data protection authorities of other states. The various powers are detailed below.

### *Preliminary Measures*

The Inspectorate may order a controller or processor to temporarily suspend, limit or freeze data processing activity, if this is necessary to avoid serious and immediate harm that would be difficult to repair. The parties involved can ask to be heard prior to execution of the measures or object to the measures within five (5) days after the execution thereof.

The Inspectorate's decision must be substantiated and specify the duration of the preliminary measures, which may not exceed a period of three (3) months (renewable once).

The parties may appeal the Inspectorate's decision to the Dispute Resolution Body within 30 days from notification of the decision by registered letter with an acknowledgment of receipt. It should be noted that appeal does not suspend the preliminary measures.

### *Gathering of Information*

In order to verify compliance with data protection legislation, the Inspectorate may proceed with any investigation, monitoring or hearing and gather any information it deems useful. As indicated below, the Inspectorate must obtain the examining magistrate's authorisation for certain actions.

### *Identification of Persons*

The Inspectorate may verify the identity of any person present at premises where an inspection is being conducted, as well as that of any other person it deems necessary to identify.

The inspector general may, by means of a substantiated written decision, verify the identity of any user of electronic communication services or electronic means of communication. If identification is not possible, the inspector general can request the cooperation of the relevant telecom operator and any person located on the Belgian territory that transmits signals via electronic communication networks or enables users to obtain, receive or distribute information through such networks.

### *Hearings*

The Inspectorate can conduct hearings if required to do so for purposes of an investigation. The person being questioned must be provided with the following information at the start of the hearing:

- (a) the fact that his or her statements can be used as evidence in court;
- (b) the fact that he or she has the right to the assistance of a lawyer;
- (c) the fact that he or she has the right to request the questions in writing, in the exact wording used;
- (d) the fact that he or she has the right to request investigative measures; and
- (e) the fact that he or she has the right to receive a copy of the hearing transcript free of charge.

Any person being questioned can request to include by reference certain documentation in the transcript. The transcript shall mention the time the hearing started and ended as well as any interruptions. It shall also mention the identity of any persons participating in the hearing.

At the end of the hearing, the person being questioned shall be asked to read the transcript and to amend or supplement the statements set out therein, if necessary.

#### *Written Inquiries*

The Inspectorate can request in writing all information it deems necessary or useful. The requested information must be provided within the time limit set by the Inspectorate, and the Inspectorate can request additional information at any time. The person from whom the information is requested can submit additional information and explanations, if necessary.

#### *On-Site Inspections*

The Inspectorate can conduct on-site inspections at the premises of a data controller or processor, if it has reasons to suspect that data protection legislation is being violated. If the Inspectorate requires access to the premises of persons bound by a duty of professional secrecy, the written consent of the person concerned or an authorisation from the examining magistrate is required.

The Inspectorate can conduct on-site inspections at residential locations with the occupant's prior consent or an authorisation from the examining magistrate.

Inspections at residential premises without the occupant's consent must be carried out between 5.00 am and 9.00 pm by two inspectors.

### *Consulting and Copying IT Systems and the Data They Contain*

If the Inspectorate has reasons to believe that data protection legislation is being violated, it may consult any IT systems and the data they contain, provided it has obtained the prior consent of the data controller or processor being investigated or an authorisation from the examining magistrate.

This also holds true where the data are stored in another member state and are publicly accessible in Belgium by electronic means or through the consent of persons legally authorised to use the computer system under investigation.

In addition, the Inspectorate may copy any IT systems and the data they contain. If it is not possible to make copies in a readable, legible format, the Inspectorate may seize the IT system and data.

If the data are in a foreign language, the Inspectorate can request a translation into an official language of Belgium (Dutch, French or German).

If the Inspectorate has obtained the prior consent of the person concerned or an authorisation from the examining magistrate, it may (with the assistance of an expert) verify the security measures of IT systems.

The Inspectorate shall at all times take appropriate measures to safeguard the integrity of the data it accesses.

### *Seizure or Sealing of Assets and IT Systems*

The Inspectorate can seize or place under seal any asset, document or IT system, for up to 72 hours. The Inspectorate can only seize or seal assets or IT systems for investigative or evidentiary purposes or if there is a risk that the violation will otherwise continue or a new violation will be committed.

After 72 hours have passed, the Inspectorate may, with the prior authorisation of the examining magistrate, seize or seal any asset, document or IT system that contributed to the violation. The seized or sealed assets and IT systems shall be listed in a register.

The controller or processor concerned may appeal the Inspectorate's decision to the Dispute Resolution Body by registered letter with an acknowledgment of receipt within 30 days after being

notified thereof.

### **Close of the Investigation**

Once the investigation is finished, a report shall be drawn up and added to the file. The inspector general can decide to submit the file to the Dispute Resolution Body, the data protection authority of another state or to the public prosecution service if the matter constitutes a criminal offense. The Inspectorate can also decide to close the case with no further action.

### **Conclusion**

Whereas the Privacy Commission had limited enforcement powers, the Data Protection Authority is entrusted with a wide range of powers to enforce data protection legislation. These powers are comparable to those of other regulatory bodies such as the Competition Authority.

Data controllers and processors should be prepared for investigation by the Data Protection Authority. It is, therefore, recommended to put in place a so-called dawn raid procedure in order to be ready when the Data Protection Authority knocks on your door.