Unofficial translation

3 DECEMBER 2017. - Act establishing the Data Protection Authority (Publication: 10-01-2018 - Entry into force: 25-05-2018) - **Revision on 28-05-2018.**

CHAPTER 1. - Introductory provision

Art. 1. This law regulates a matter referred to in Article 74 of the Constitution.

Art. 2. For the purposes of this Act, the following definitions shall apply:

1° "Data Protection Authority": the supervisory authority for the processing of personal data;
2° "Regulation 2016/679": Regulation 2016/679 of the European Parliament and the Council dated 27 April 2016 on the protection of natural individuals with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC;
3° "computer system": any system for the processing of data;
4° "inspector": statutory or contract official of the Data Protection Authority charged with identifying infringements of this law and the laws containing provisions in relation to the protection and processing of personal data.

CHAPTER 2. - The Data Protection Authority

Art. 3. A "Data Protection Authority" shall be established in the Chamber of Representatives.

It is the successor of the Commission for the protection of privacy (CPP).

It enjoys legal personality. Its head office shall be based in the administrative district of Brussels-Capital.

Art. 4. § 1. The Data Protection Authority shall be responsible for supervising compliance with the basic principles of the protection of personal data within the framework of this law and of the laws containing provisions on the protection of the processing of personal data.

Notwithstanding the powers of the Community or Regional Governments, of the Community and Regional Parliaments, of the United College and of the Joint Assembly referred to in Article 60 of the special law dated 12 January 1989 on the Brussels institutions, the Data Protection Authority shall perform these duties throughout the entire Kingdom, regardless of the national law applicable to the processing concerned.

§ 2. The supervision organised under this law does not concern the processing operations carried out by the courts and tribunals or by the Public Prosecution Service in the exercising of their judicial duties.

The King may designate other authorities insofar as they process personal data in the context of their judicial duties.

The competences, duties and powers as a supervisory authority provided for in Regulation 2016/79 are, with respect to the police services within the meaning of Article 2,2° of the law dated 7 December 1998 on the organisation of an integrated police service structured at two levels, exercised by the Monitoring Body on police information as referred to in Article 44/6, § 1 of the law dated 5 August 1992 on the police force.

§ 3. Each legally binding decision taken by the Data Protection Authority shall be dated, signed and substantiated and set out the legal remedy that can be availed of to appeal against the decision.

Art. 5. The Data Protection Authority shall perform its duties solely in the public interest.

The members of its bodies and staff shall not bear civil liability for their decisions, actions or conduct in the exercising of the statutory duties of the Data Protection Authority, except where provided for by law.

Art. 6. The Data Protection Authority shall have the authority to bring violations of the basic principles of the protection of personal data within the framework of this act and of the laws containing provisions on the protection of the processing of personal data to the notice of the judicial authorities and, where applicable, institute legal proceedings to ensure compliance with these basic principles.

Art. 7. The Data Protection Authority is composed of six bodies:

1° an executive committee;
2° general secretariat;
3° a front office;
4° a knowledge centre;
5° an inspections service;
6° a litigation chamber.

The Data Protection Authority may enlist the assistance of experts for the performance of its duties.

Art. 8. An independent advisory council shall be added to the Data Protection Authority.

Section 1. - The executive committee

Art. 9. The executive committee:

1° approves the annual accounts and decides on the annual budget, the annual report, the strategic plan and the management plan, including the annual priorities of the Data Protection Authority;
2° determines the evaluation indicators concerning the implementation of the annual report, the strategic plan and the management plan;
3° decides on the organisation and composition of the Data Protection Authority, including the internal mobility of the staff between the bodies;
4° decides on the identity document model referred to in Article 31(2).

The executive committee shall request the opinion of the advisory council with regard to the strategic plan and the evaluation indicators referred to in paragraph 1, 2° above and submit the strategic plan at the same time for at least two weeks for public consultation.

Art. 10. The executive committee shall monitor developments in the technical, commercial and other fields that impact on the protection of personal data.

The executive committee can seek advice from the advisory council to this end.

Art. 11. The executive committee shall draw up the internal rules of procedure for the Data Protection Authority within two months of the Authority's establishment.

This set of regulations shall set out the essential rules concerning the functioning of the bodies and the timeframes within which information, opinions and approvals referred to in Article 20(1) have to be delivered.

The executive committee shall submit the internal rules of procedure, as well as subsequent amendments to the rules, to the Chamber of Representatives for approval.

Art. 12. The executive committee is composed of the director of the general secretariat, the director of the knowledge centre, the director of the front office, the inspector-general and the chairman of the litigation chamber.

The members of the executive committee shall perform their duties on a full-time basis.

They shall make the following oath to the chairman of the Chamber of Representatives: "I swear loyalty to the King and obedience to the Constitution and the laws of the Belgian people."

Art. 13. § 1. The executive committee shall be chaired by the chairman of the Data Protection Authority.

If the chairman is indisposed, the executive committee shall be chaired by the oldest member of the executive committee present, with the exception of the chairman of the litigation chamber.

§ 2. The function of chairman of the Data Protection Authority shall be exercised alternately by the director of the general secretariat for the first three years of the term of office and by the director of the knowledge centre for the second half of the term of office.

§ 3. The chairman of the Data Protection Authority shall be assisted by the general secretariat in the performance of his duties.

Art. 14. The executive committee shall meet at the request of its members at least once per month.

Art. 15. The executive committee can only take decisions when a majority of its members are present.

The vote can be held electronically.

In the event of a lack of consensus, a decision shall be taken if a majority of the entire executive committee is present.

Art. 16. Minutes shall be taken of the executive committee's deliberations. The minutes shall be signed by the chairman.

The decisions of the executive committee referred to in Article 9, 1° and 4° shall be published on the website of the Data Protection Authority.

Art. 17. The chairman of the Data Protection Authority:

1° is responsible for cooperation and coordination between the different bodies of the Data Protection Authority;
2° prepares the annual budget, the annual accounts, the annual report, the strategic plan and the management plan, including the annual priorities of the Data Protection Authority;
3° manages the internal organisation and composition of the Data Protection Authority;
4° represents the Data Protection Authority.

The management plan shall include arrangements concerning the objectives for the Data Protection Authority and the resources required for this.

Art. 18. The chairman of the executive committee and, in his absence, the oldest member of the executive committee present, with the exception of the chairman of the litigation chamber, shall represent the Data Protection Authority in legal matters.

Section 2. - The general secretariat

Art. 19. The general secretariat has the following horizontal support functions:

1° manage questions relating to human resources, the budget and the IT of the Data Protection Authority;
2° manage any legal matter relating to the management and operation of the Data Protection Authority;
3° manage internal and external communication.

Art. 20. § 1. The general secretariat also has the following duties:

1° monitor the social, economic and technological developments that have an impact on the protection of personal data;
2° draw up the list of processing operations that require a data protection impact assessment;
3° give advice as part of a data protection impact assessment to a controller responsible for the processing as part of the consultation by the controller responsible for the processing conducted by the Data Protection Authority;
4° approve codes of conduct;
5° promote the introduction of certification mechanisms and approve certification criteria;
6° draw up and publish the criteria for the accreditation of a body for the supervision of codes of conduct on the basis of Article 41 of Regulation 2016/679 and of a certification body on the basis of Article 43 of Regulation 2016/679;
7° ensure the accreditation of a body for the supervision of codes of conduct on the basis of Article 41 of Regulation 2016/679;
8° approve the standard contractual clauses and the binding corporate rules.

§ 2. The duties set out in paragraph 1, 4° to 8°, shall be performed in accordance with current European and international regulations.

Art. 21. The general secretariat shall be headed by the director of the general secretariat.

Section 3. – The front office

Art. 22. § 1. The front office

1° receives the complaints and submissions sent to the Data Protection Authority;
2° can initiate a mediation procedure;
3° promotes data protection among the public, with a specific focus on minors;
4° promotes awareness among controllers and processors with regard to their obligations;
5° provides the data subject with information regarding the exercising of their rights.

§ 2. The front office shall be headed by the director of front office

Section 4. - The knowledge centre

Art. 23. § 1. The knowledge centre shall issue, either on its own initiative or at the request of the Government, of the Legislative Chambers, of the Community or Regional Governments, of the Community or Regional Parliaments, of the United College or of the Joint Assembly referred to in Article 60 of the special law dated 12 January 1989 on the Brussels institutions:

1° opinions concerning any matter relating to the processing of personal data;
2° recommendations relating to social, economical and technological developments that can impact on the processing of personal data.

§ 2. The knowledge centre shall take account, in its opinions and recommendations, of the necessary technical and organisational security measures.

Art. 24. The knowledge centre shall be composed of six members and the director of the knowledge centre.

The knowledge centre shall hold plenary meetings on the initiative of the director.

The knowledge centre shall be assisted by a secretariat in the performance of its duties.

Art. 25. The knowledge centre can only take decisions when a majority of its members are present.

The vote can be held electronically.

The decisions are adopted by a majority of votes.

In the event of a tied vote, the director shall have the casting vote.

Art. 26. § 1. Each request for opinion shall be submitted to the Data Protection Authority by registered mail or via an online form provided on the website of the Data Protection Authority.

Unless determined otherwise by law, the knowledge centre shall issue advice within sixty days of the necessary information having been communicated to the Data Protection Authority. Where the opinion of the Data Protection Authority is required under any law, decree or ordinance, the director of the knowledge centre can reduce the period of sixty days to fifty days in specially justified urgent cases.

§ 2. In cases where the opinion of the Data Protection Authority is required under any law, decree or ordinance, this requirement may be bypassed if the opinion has not been given within the periods referred in section 1, paragraph 2.

Art. 27. § 1. The opinions shall be provided in writing, giving the reasons for the same.

They shall be communicated to the concerned authority..

The government member responsible for the protection of privacy and the Chamber of Representatives shall receive an electronic copy of each opinion and recommendation.

§ 2. In cases where the opinion of the Data Protection Authority is required under any law, decree or ordinance, the opinion must be published in the Belgian Official Journal together with the relevant regulatory provision.

The opinions and recommendations shall be published on the website of the Data Protection Authority.

Section 5. - The inspection service

Art. 28. The inspection service is the investigating body of the Data Protection Authority.

Art. 29. The inspection service shall be headed by the inspector-general and be composed of inspectors.

The inspection service shall be assisted by a secretariat in the performance of its duties.

In the event of absence or being indisposed, the inspector-general shall be replaced by the inspector with the longest service or, in the case of equal seniority, the eldest.

Art. 30. § 1. The inspectors shall make the following oath to the inspector-general: "I swear loyalty to the King and obedience to the Constitution and the laws of the Belgian people."

§ 2. The function profiles and required areas of competence of the inspectors shall be set out in the internal rules of procedure of the Data Protection Authority.

Art. 31. The inspector-general and the inspectors shall be in possession of the proof of identity of their office when performing their duties, and must present it immediately on request.

The executive committee shall determine the model for the proof of identity.

Section 6. - The litigation chamber

Art. 32. The litigation is the administrative disputes body of the Data Protection Authority.

Art. 33. § 1. The litigation chamber is composed of a chairman and six members including:

1° two members with thorough knowledge of the protection of personal data;
2° two members with thorough knowledge of administrative dispute procedures;
3° two members with thorough knowledge of information security and information and communication technology.

The chairman of the dispute chamber shall have a thorough knowledge of administrative dispute procedures.

The chairman or one of the members of the litigation chamber shall sit alone unless the chairman of the litigation chamber decides to sit with three members in accordance with the provisions of the internal rules of procedure.

§ 2. The internal rules of procedure shall also provide details regarding the composition of the litigation chamber when sitting, as well as its working methods.

Art. 34. In performing its duties, the dispute chamber shall be assisted by a secretariat, which will also ensure the Registry's duties.

Section 7. - The advisory council

Art. 35. The board shall, on its own initiative or at the request of the executive committee or the knowledge centre, provide non-binding opinions to the Data Protection Authority concerning any matter relating to the protection of personal data.

The Chamber of Representatives shall determine the composition of the deliberation advisory and designate its members.

The members of the advisory council shall not be part of the Data Protection Authority.

CHAPTER 3. - Appointment of the members of the executive committee, the members of the knowledge centre and the members of the litigation chamber

Section 1. - General terms of appointment

Art. 36. § 1. The members of the executive committee, the members of the knowledge centre and the members of the litigation chamber shall be appointed on the basis of their skills and experience in the field of the protection of personal data, their independence and their moral authority.

§ 2. The members of the executive committee must hold a diploma that grants them access to a level A position.

The members of the executive committee must have a working knowledge of the second national language and English. At least one member of the executive committee must also have a working knowledge of German.

§ 3. The profiles of all members of the executive committee and the members of the litigation chamber must together make it possible for the Data Protection Authority to meet the legal, economic, ethical and technological challenges of the growth of the digital society.

Art. 37. The members of the executive committee, the members of the knowledge centre and the members of the litigation chamber shall be appointed for a renewable term of office of six years.

Art. 38. At the time of their appointment and during their term of office, the members of the executive committee, members of the knowledge centre and members of the litigation chamber must meet the following requirements:

1° be a citizen of a Member State of the European Union;
2° enjoy the relevant civil and political rights;
3° not be a member of the European Parliament or of the Legislative Chambers, or of a Community or Regional Parliament;
4° not be a member of a Federal Government, or of a Community or Regional Government;

5° not exercise a function in the minister's policy unit;
6° not be a proxy of a public function.

Section 2. - Appointment procedure

Art. 39. The members of the executive committee, the members of the knowledge centre and the members of the litigation chamber shall be appointed by the Chamber of Representatives.

The vacancies for the mandates of the members of the executive committee, the members of the knowledge centre and the members of the litigation chamber shall be published in the Belgian Official Journal no later than six months prior to the expiry date of the term of office and, for their first composition, no later than one month after this article has entered into force. The publication shall be in the form of a call for applicants, together with a description of the number of vacant positions, the terms of appointment, the duties of the bodies being established, and details of the rules governing the submission of applications.

Art. 40. § 1. The executive committee shall include an equal number of Dutch- and French-speaking members, except for the chairman of the litigation chamber.

The director of the general secretariat and the director of the knowledge centre may not belong to the same language group.

The knowledge centre shall have an equal number of Dutch- and French-speaking members.

The six members of the litigation chamber shall include an equal number of each language group and at least one member must have a working knowledge of German.

§ 2. A maximum of two-thirds of the members of the knowledge centre shall be of the same gender.

Art. 41. Should a position as member of the executive committee, member of the knowledge centre or member of the litigation chamber become vacant for any reason, a replacement shall be appointed for the remaining period of the term of office.

A completely new appointment procedure shall be set up pursuant to Article 39 for the function becoming vacant, with the publication of the function in the Belgian Official Journal no later than one month after becoming vacant.

Art. 42. Should their term of office not be renewed, the members of the executive committee, the members of the knowledge centre and the members of the litigation chamber shall remain in their positions until the executive committee, knowledge centre or litigation chamber has met for the first time respectively in its new composition.

CHAPTER 4. - Independence and operation of the Data Protection Authority

Art. 43. The members of the executive committee and the members of the knowledge centre, the inspection service and the litigation chamber shall not receive any questions or enquiries within the limits of their powers or any instructions, either directly or indirectly.

Their presence shall be prohibited during deliberations or decisions on matters in relation to which they have a personal or direct interest, or with regard to which their blood relatives or relatives up to the third degree have a personal or direct interest.

Art. 44.§ 1. The members of the executive committee, the members of the knowledge centre and the members of the litigation chamber may not, during their terms of office, perform any other activity, whether remunerated or not, that is not compatible with their mandate.

An incompatible activity is an activity that can draw direct or indirect benefit from the decisions and positions that can be taken by the Data Protection Authority.

The Chamber of Representatives can authorise a member of the executive committee to perform an additional activity provided that this does not affect the performance of his/her full-time function or his/her independence and reputation.

§ 2. Before starting their term of office, the members referred to in paragraph 1 above shall complete and sign a declaration stating that they do not have any conflicts of interest. They shall maintain this declaration throughout the duration of their term of office.

The members of the executive committee may not, for a period of two years after the end of their term of office, perform any function that would directly or indirectly provide them with advantages arising from the exercise of their mandate.

§ 3. Leave for an assignment of general interest can be granted to a civil servant or magistrate to perform the function of a member of the executive committee. They shall receive their salary as a member of the executive committee during their term of office, while their salary as a civil servant or magistrate will be suspended.

Art. 45. § 1. The Chamber of Representatives can only relieve a member of the executive committee, a member of the knowledge centre or a member of the litigation chamber of his/her mandate if he/she has been guilty of gross misconduct or no longer meets the requirements for the performance of his/her duties. There is no appeal against such a decision.

A member of the executive committee, a member of the knowledge centre or a member of the litigation chamber cannot be relieved of his/her mandate for opinions he/she expresses when performing his/her functions.

§ 2. The mandate cannot be rescinded until the individual concerned has been heard with regard to the reasons alleged.

Prior to the hearing, the Chamber of Representatives shall compile a file containing all the documents relating to the reasons alleged.

The individual concerned shall be summoned no later than five days prior to the hearing by way of a registered letter containing at least the following:

1° the serious reasons alleged;
2° the fact that the termination of the mandate is being considered;
3° the place, date and time of the hearing;

4° the right of the individual concerned to enlist the assistance of a person of his/her choice;
5° the place where and period within which the file can be accessed;
6° the right to have witnesses called.

The individual concerned and the person assisting him/her shall be able to access the file from the date of the summons up to and including one day prior to the hearing.

Minutes shall be drawn up on the hearing.

Art. 46. § 1. The staff of the Data Protection Authority, the regulations and the staff recruitment method shall be determined by the Chamber of Representatives in response to a proposal by the Data Protection Authority.

The staff of the Data Protection Authority shall be subject to the legal and statutory provisions applying to staff members of the federal administrative civil service.

§ 2. The tenured staff members of the Data Protection Authority shall benefit from the system of retirement pensions applying to civil servants in the permanent employ of the federal administration of the State. These pensions shall be payable by the Treasury.

Art. 47. The Data Protection Authority shall, for the performance of its legal duties, have access to the data referred to in Article 3, Paragraph 1, 1° to 6°, 9°, 9° /1 and Paragraph 2 of the law dated 8 August 1983 establishing a National Register of Natural Individuals.

It may use the national register number for the purpose of performing its legal duties.

The inspectors of the Data Protection Authority shall, for the performance of their inspection duties, also have access to the data referred to in Article 6bis, § 1, 1° of the law dated 19 July 1991 on the population registers, identity cards, foreigners' cards and residence documents as well as on the amendment of the law dated 8 August 1983 establishing a National Register of Natural Individuals.

Art. 48. § 1. Unless legal exceptions, the members of the executive committee, the members of the knowledge centre, the members of the litigation chamber and the staff of the Data Protection Authority shall, during and after performance of their respective mandate and agreement, be obliged to preserve the confidential nature of the facts, actions and information coming to their knowledge by virtue of their function.

§ 2. The Data Protection Authority can conclude protocols concerning the confidentiality obligation with third-party bodies for the purpose of guaranteeing the exchange of data required for the performance of its duties and powers.

Art. 49. A grant shall be allocated from the national general expenditure budget for the operation of the Data Protection Authority.

The Data Protection Authority shall prepare a budget plan for its operations on an annual basis. Assisted by the Court of Auditors, the Chamber of Representatives shall examine the detailed budget proposals of the Data Protection Authority, approve them and monitor the implementation of its budget, as well as examine and approve the detailed accounts.

The Data Protection Authority shall enclose a strategic plan with its annual budget proposal, accompanied by the opinion of the advisory council and a management plan.

The Data Protection Authority shall apply a schedule for its budget and accounts that is comparable to the budget and accounts schedule of the Chamber of Representatives.

Art. 50. § 1. The members of the executive committee shall enjoy the same status as the councillors of the Court of Auditors. The salary scheme for the councillors of the Court of Auditors, contained in the law dated 21 March 1964 on the salaries of the members of the Court of Auditors, shall apply to the members of the executive committee. During his/her chairmanship of the Data Protection Authority, the executive member concerned shall receive remuneration equal to that of the chairman of the Court of Auditors.

With regard to pensions, the mandate of the members of the executive committee shall be counted as being equivalent to a permanent appointment. They shall benefit from the retirement pension scheme that applies to civil servants who are in the permanent employ of the federal administration of the State. These pensions shall be payable by the Treasury.

§ 2. Unless he/she resigns or is removed from office, the member of the executive committee shall, if his/her office is terminated or his/her mandate is not renewed, receive a flat-rate allowance for discharge equal to the gross monthly salary of one month per full year of the mandate served, up to a maximum of six months. Members of the executive committee who receive a professional income or a replacement income or a retirement pension shall be excluded from this measure. A survivor's pension or payment of a guaranteed minimum by a public social welfare centre is not regarded as a replacement income.

§ 3. The external members of the knowledge centre and the dispute chamber shall be entitled to an attendance allowance amounting to €294.55 (index figure 1.67374). The amount is linked to the evolution of the consumer price index. They shall be entitled to reimbursements for travel and subsistence expenses in accordance with the provisions applying to federal civil servants.

Art. 51. The Data Protection Authority shall submit an annual report on its activities of the previous year to the Chamber of Representatives and the Government, drawn up, in particular, on the basis of the evaluation indicators referred to in Article 9 (1)(2°).

A list of the opinions and recommendations issued by the Data Protection Authority shall be annexed to the report. It shall be stated which opinions and recommendations were formulated on its own initiative.

The report shall be made public and be sent to the European Commission and the European Data Protection Board referred to in Regulation 2016/679.

CHAPTER 5. - Cooperation arrangements

Section 1. - Cooperation at national level

Art. 52. § 1. The Data Protection Authority shall perform its duties in a spirit of dialogue and consultation with all government actors and private actors involved in the policy of protection of the fundamental rights and freedoms of natural individuals in connection with the processing and free movement of personal data, as well as in the consumer protection policy.

The Data Protection Authority can be assisted by or act at the request of other authorities responsible for the observance of other legislation.

§ 2. The Data Protection Authority can conduct a broad public survey or consultation or a more targeted survey or consultation of the representatives of the sectors concerned.

Art. 53. § 1. The Data Protection Authority can set up committees or groups on matters falling within its area of competence or which form a part of the same. Insofar as this does not affect its independence, the Data Protection Authority can, on its own initiative or on request, form part of committees or groups dealing with matters that fall within its area of competence.

§ 2. The executive committee can delegate members of the bodies or staff of the Data Protection Authority to represent the Data Protection Authority in matters that fall within its area of competence in committees or groups that it is obliged to or chooses to take part in and, within the limits established by the executive committee, to take part in the decision-making or voting process in the committees or groups concerned. These delegated assignments can be reviewed or withdrawn by the executive committee at any time.

Art. 54. The chairman of the Data Protection Authority or, where appropriate, one of the other members of the executive committee may be heard by the competent commissions of the Chamber of Representatives, the Community or Regional Parliaments, the United College or the Joint Assembly referred to in Article 60 of the special law dated 12 January 1989 on the Brussels institutions, at their request or on their own initiative.

Section 2. - Cooperation at international level

Art. 55. § 1. The Data Protection Authority can cooperate with any authority or other data protection authority of another state by using the powers granted to it under Regulation 2016/679 or by national legislation.

§ 2. The cooperation can, among other things, relate to:

1° the introduction of pools of expertise;
2° the exchange of information;
3° mutual assistance in the area of control/monitoring measures;
4° sharing personal and financial resources.

The collaboration can, among other things, be fleshed out on the basis of cooperation agreements.

Art. 56. § 1. With a view to the application of international treaties, the Data Protection Authority shall be authorised to assign certain members of its bodies or staff the capacity of representatives at international authorities insofar as these authorities perform duties concerning matters that fall within the area of competence of the Data Protection Authority.

§ 2. The executive committee can grant certain members of the bodies or staff of the Data Protection Authority the competence to represent the Data Protection Authority in international committees or groups that it is obliged to or chooses to take part in and, within the limits established by the executive committee, to take part in the decision-making or

voting process in the committees or groups concerned. These delegated assignments can be reviewed or withdrawn by the executive committee at any time.

CHAPTER 6. - Procedural provisions

Art. 57. The Data Protection Authority shall use the language in which the procedure is conducted as required by the specific matter.

Section 1. - Referral and admissibility of a complaint or request

Art. 58. Anyone can submit a complaint or request to the Data Protection Authority in writing, dated and signed.

The Data Protection Authority shall establish a form for this purpose.

Art. 59. The submission of a complaint or request shall be free of charge.

Art. 60. The front office shall assess whether or not the complaint or request is admissible.

A complaint is admissible when:

- it has been drawn up in one of the national languages;
- it contains a description of the facts, as well as the indications required to identify the processing to which it relates;
- it falls within the area of competence of the Data Protection Authority.

A request is admissible when:

- it has been drawn up in one of the national languages;
- it falls within the area of competence of the Data Protection Authority.

The front office can invite the complainant or the requester to explain his/her complaint or request.

Art. 61. The decision concerning the admissibility of the complaint or request shall be notified to the complainant or requester.

If the front office decides that a complaint or request is inadmissible, the complainant or requester shall be informed accordingly by way of a reasoned decision.

Art. 62. § 1. The admissible complaints shall be forwarded to the litigation chamber by the front office.

§ 2. The admissible applications shall be dealt with by the front office.

If an amicable agreement is reached between the parties through the intervention of the front office, the front office shall draw up a report setting out the solution reached and its compliance with the legal principles concerning data protection.

An amicable agreement does not rule out the supervisory competence of the Data Protection Authority.

If an amicable agreement is not reached, the original request for mediation shall assume the form of a complaint that is then forwarded by the front office to the litigation chamber to be dealt with on its merits:

1° with the consent of the applicant; or
2° if the front office identifies serious indications of the existence of a practice that may occasion an infringement of the basic principles of the protection of personal data, within the context of this act and of the laws containing provisions concerning the processing of personal data.

Section 2. - Procedure for the inspection service

Sub-section 1. - Referral to the inspection service

Art. 63. Referral to the inspection service can occur:

1° if the executive committee identifies serious indications of the existence of a practice that may occasion an infringement of the basic principles of the protection of personal data, within the context of this act and of the laws containing provisions concerning the processing of personal data;
2° if the litigation chamber has decided in response to a complaint that an investigation by the inspection service is required;
3° by the litigation chamber in the context of a request to conduct an additional investigation;
4° at the request of the executive committee with the aim of cooperating with a data protection authority of another State;
5° at the request of the executive committee in the event of the Data Protection Authority being seized by a judicial authority or an administrative supervisory body;
6° on its own initiative if it identifies serious indications of the existence of a practice that may occasion an infringement of the basic principles of the protection of personal data, within the context of this act and of the laws containing provisions concerning the processing of personal data.

Sub-section 2. - Investigatory options of the inspection service

1. General provisions

Art. 64. § 1. The inspector-general and the inspectors shall exercise the powers referred to in this section with a view to supervision as set out in Article 4, § 1 of this act.

§ 2. In exercising the powers referred to in this section, the inspector-general and the inspectors shall ensure that the means used by them are appropriate and necessary.

§ 3. The investigation shall be confidential, subject to any legal exception, up to the time of the report being submitted to the litigation chamber by the inspector-general.

Art. 65. The inspector-general and the inspectors can request the assistance of the police in the performance of its duties by submitting a reasoned request.

2. Powers of the inspection service

Art. 66. § 1. For the purpose of examining the file, the inspector-general and the inspectors can, in accordance with the procedures set out in this law:

1° identify individuals;
2° question individuals;

3° conduct a written questionnaire;
4° conduct on-site investigations;
5° consult computer systems and copy the data they contain;
6° consult information electronically;
7° seize or seal goods or computer systems;
8° request the identification of the subscriber or the habitual user of an electronic communication service or of the electronic means of communication used.

§ 2. The individuals that are the subject of the investigation must provide their cooperation to this end.

Art. 67. § 1. The investigative measures may lead to an official report establishing an infringement. The official report shall have evidential value until the contrary is proven.

A report shall be drawn up on the investigative measures not leading to an official report.

§ 2. Another member of the inspection service of the Data Protection Authority or another inspection service or administrative supervisory body may use the material findings arising from the official reports while maintaining the evidential value.

Information forming part of an ongoing preliminary or judicial investigation may only be communicated and used subject to prior authorisation by the public prosecutor or the investigating judge.

Information concerning medical data of a personal nature may only be communicated and used with due regard for the principle of medical confidentiality.

§ 3. The facts established by other inspection services or administrative supervisory bodies can be used by the inspector-general and inspectors in their investigations and be included in the official reports drawn up by them as part of their assignment with the same evidential value.

Art. 68. Without prejudice to Article 44/1 of the law dated 5 August 1992 on the police force, all State services, including the public prosecutor's office and the registries of the courts and tribunals, the provinces, the municipalities, the associations to which they belong, the government institutions depending upon the same, shall be required to provide the inspector-general and the inspectors, at their request, with all information that the latter consider useful for monitoring compliance with the legislation for which they are responsible, as well as make any information carriers available in this regard and provide copies of the same in whatever form.

If this information forms part of an ongoing preliminary or judicial investigation, it shall only be provided subject to prior authorisation by the public prosecutor or the investigating judge.

Art. 69. Under the provisions of Article 62 of Regulation 2016/679, the inspection service can conduct investigations together with the involvement of staff members from data protection authorities of other States.

3. Interim measures

Art. 70. The inspector-general and the inspectors can order the temporary suspension, limitation or freezing of data processing operations that are the subject of an investigation if this is necessary to avoid serious, immediate and irreparable harm.

The parties concerned can be interviewed by the inspector-general or an inspector before an interim measure is implemented. If the parties concerned cannot be interviewed in advance, they may make their objections known in writing or verbally within a period of five days after the implementation of the relevant measure.

The decision made by the inspection service must be substantiated and shall determine the duration of the interim measure, which may last up to three months and can be extended once by a further period not exceeding three months.

Art. 71. The parties concerned may lodge an appeal against the measures referred to in Article 70 with the litigation chamber. The appeal shall not suspend the measure.

The appeal shall, on pain of nullity, be lodged by means of a reasoned and signed petition deposited with the secretariat of the litigation chamber within a period of thirty days following notification of the decision by registered mail with acknowledgement of receipt.

4. Obtaining information

Art. 72. Without prejudice to the provisions contained in this section, the inspector-general and the inspectors may conduct any investigation, checks or questioning, as well as obtain any information they consider necessary to ensure that the basic principles of the protection of personal data, in the context of this act and of the laws containing provisions concerning the processing of personal data overseen by them, are actually complied with.

5. Identification of individuals

Art. 73. § 1. The inspector-general and the inspectors may verify the identity of the individuals present on the site under supervision, as well as of any individual whose identification they deem it necessary to verify for the performance of their duties.

They may ask such individuals to present official identity documents.

They may furthermore identify these individuals on the basis of unofficial documents submitted voluntarily by such individuals if they cannot produce official identity documents, or where the inspectors have doubts regarding the authenticity of the same, or the identity of these individuals.

§ 2. The inspector-general can, by way of a reasoned, written decision based on the data in his/her possession, proceed to the identification of the subscriber or habitual user of an electronic communication service or the electronic means of communication used.

If the inspector-general cannot identify the person referred to in paragraph one above with the data in its possession, he/she may enlist the assistance of:

- the operator of an electronic communication network; and

- anyone who, within Belgium, in any way makes available or offers a service consisting of the conveyance of signals via electronic communication networks or enabling users to obtain,

receive or disseminate information via an electronic communication network. This also includes the provider of an electronic communication service.

The reasoning shall reflect the proportionality, while respecting privacy and subsidiarity with regard to any other investigative act.

6. Questioning

Art. 74. The inspector-general and the inspectors may, where necessary in the presence of witnesses, experts or the police, question anyone whom they deem necessary with regard to any fact or situation they consider useful for the performance of their duties.

The questioning shall take place in accordance with Article 31 of the law dated 15 June 1935 on the use of languages in the courts.

When questioning individuals, irrespective of their capacity, the rules set out in Article 75 must be respected at the very least.

Art. 75. § 1. At the start of the questioning, the individual being questioned is informed that:

1° his/her statements can be used as evidence in legal proceedings;
2° he/she can be assisted by an advisor;
3° he/she can ask for all questions put to him/her and all answers given by him/her to be noted in the wording used;
4° he/she can ask for investigative measures to be conducted;
5° he/she can receive a copy of the text of the questioning free of charge to be handed to him/her immediately on completion of the questioning or sent to him/her within the month.

§ 2. Each individual being questioned can use the documents in his/her possession and request that these documents be attached to the minutes of the interview.

The minutes shall state the time at which the interview commenced, was suspended and resumed, if applicable, and when it was terminated. It shall state the identity of those individuals taking part in the interview or any part of the same.

§ 3. At the end of the interview, the interviewer shall hand the interviewee the minutes of his/her interview for his/her reading. He/she shall be asked whether these statements need to be modified or completed.

7. Written interview

Art. 76. The inspector-general and the inspectors can request individuals to provide any useful information they deem necessary in writing.

The inspector-general and the inspectors shall determine the period within which a response to a request for information must be given and can request additional information at any time.

Art. 77. The individual being questioned shall have the right to clarify his/her response, with explanations and information.

8. On-site investigation

Art. 78. Where the inspector-general and the inspectors have reason to believe that an infringement of the basic principles of the protection of personal data in the context of this act and of the laws containing provisions concerning protection of the processing of personal data has been committed, they may enter the company, service or any other location concerned at any time to conduct an on-site investigation for the purpose of making material observations.

Except with the written consent from the individual concerned or authorisation by the investigating judge, the inspector-general and the inspectors shall not have access to the premises of a professional who is subject to professional confidentiality and for whom a legal regulation is provided for an on-site investigation and access to their professional premises in the absence of a representative of the professional body.

Art. 79. § 1. Where the inspector-general and the inspectors have reason to believe that an infringement of the basic principles of the protection of personal data in the context of this act and of the laws containing provisions concerning protection of the processing of personal data has been committed, they may enter occupied areas, provided they have the consent of the occupant or, failing this, provided prior authorisation has been given by the investigating judge.

§ 2. To obtain this authorisation, the inspector-general shall submit a reasoned request to the investigating judge responsible for the judicial district in which the party under investigation is located. This application shall contain at least the following information:

1° the identification of the occupied areas that are the subject of the visit;
2° the name of the inspector in charge of carrying out the visit of the occupied areas;
3° the legislation that is the subject of the inspection and in relation to which the inspectors are of the opinion that authorisation for a visit is necessary;
4° the alleged infringements that are the subject of the inspection;
5° all documents and information showing that the use of this means is necessary;
6° the proportionality in comparison to any other investigative act.

§ 3. The investigating judge shall reach a decision within a period of not more than forty-eight hours after receiving the application. This decision cannot be appealed against.

§ 4. Visits to the occupied areas without the consent of the occupant shall take place between 5 a.m. and 9 p.m. by at least two inspectors acting together.

Art. 80. The party being monitored shall be informed of the purpose of the investigation and the applicable legislation.

With the exception of the documents from which the identity of the party submitting a complaint can be inferred, all supporting documentation required to obtain authorisation for the visit must be annexed to the report referred to in Article 91, § 1.

The party being monitored can prepare a statement to be added to the official report.

9. Consultation of the computer system and copy of the data on the IT system

Art. 81. § 1. Where the inspector-general and the inspectors have reason to believe that an infringement of the basic principles of the protection of personal data in the context of this

act and of the laws containing provisions concerning protection of the processing of personal data has been committed, they may inspect any computer system and the data contained on the same, provided they have obtained the consent of the party being monitored or, failing this, provided that prior authorisation has been given by the investigating judge.

§ 2. The inspector-general and inspectors may request submission on the spot of the computer system as well as the data contained therein and which they require for their investigations and observations. They may also take extracts, duplicates or copies free of charge or require the same in a readable and understandable form as requested by them.

If it is not possible to make copies on the spot, the inspector-general and the inspectors may, against a receipt containing an inventory, seize the computer system and the data contained therein under the terms and conditions set out in Article 89.

§ 3. The party being monitored must allow the inspector-general and the inspectors access to the computer system and the data contained therein by electronic means.

The inspector-general and the inspectors shall be able to take extracts, duplicates or copies from the computer system and the data contained therein free of charge or require the same in a readable and understandable form as requested by them.

Art. 82. The return of the computer system shall be subject to the submission of an inventory of the relevant IT systems.

Art. 83. The authorisation referred to in Article 81, § 1 shall also apply when the storage location of these data is in another State and the data are publicly accessible in Belgium by electronic means or with the consent of those individuals authorised to use the computer system examined.

Art. 84. § 1. The monitored party availing itself of a computer system for the processing of personal data shall present, for examination on site, all information relating to the analyses, programs, management and operation of the system used.

§ 2. The inspector-general and the inspectors can request a translation into one of the national languages of the data that are required to be stored by virtue of a regulatory obligation and which were drawn up in a foreign language.

§ 3. The inspector-general and the inspectors may, by means of the computer system and with the assistance of the party being monitored, verify the reliability of the computerised data and operations by requesting the presentation of documents for examination which were drawn up, in particular, to convert the data placed on computer systems into a readable and understandable form.

Art. 85. The inspector-general and the inspectors shall take the appropriate measures to ensure the integrity of the data collected and of the equipment to which they have access.

Art. 86. The inspector-general and the inspectors may consult, inspect and make copies of all information that is accessible to the public by electronic means, either free of charge or for payment. They may not assume a credible fictitious identity or use fictitious documents for this purpose and may not enter into any personal interaction with any individual.

Art. 87. The inspector-general and the inspectors may test computer system security measures or have this done by experts with the prior consent of the party being investigated or, failing this, with prior authorisation from the investigating judge.

Art. 88. The investigative activities conducted in the implementation of this law may not lead to the application of Art. 550bis of the Criminal Code.

10. Seizure and sealing

Art. 89. § 1. The inspector-general and the inspectors can seal or seize objects, documents or computer systems for the duration of their assignment, but for no longer than seventy-two hours.

They shall have these powers whenever this is necessary for the purpose of detecting, investigating or providing evidence of infringements, or where there is a danger of the infringements continuing or new infringements being committed with these computer systems.

The measures shall be recorded in an official report, with the individual who was the subject of the measures receiving a copy of this report without delay.

§ 2. After seventy-two hours, the inspector-general and the inspectors may, with prior authorisation from the investigating judge, seal or seize objects, documents or computer systems that are the subject of the infringement or which were used to commit the infringement.

The measures shall be recorded in an official report, with the individual who was the subject of the measures receiving a copy of the same without delay.

§ 3. The sealed or seized objects, documents or computer systems shall be inventoried in a register kept specially for this purpose.

Art. 90. The parties concerned may lodge an appeal against the measures referred to in Article 89 with the litigation chamber.

The appeal shall, on pain of nullity, be lodged by means of a reasoned, signed petition deposited with the secretariat of the litigation chamber within a period of thirty days following receipt of the official report by registered mail with acknowledgement of receipt.

Sub-section 3. - Conclusion of the investigation

Art. 91. § 1. When the inspector-general and the inspectors are of the view that their investigation is complete, they shall draw up their report and attach it to the file.

§ 2. The inspector-general can:

- submit the file to the chairman of the litigation chamber;
- submit the file to the public prosecutor if the facts may constitute a criminal offence;
- close the file;
- submit the file to a data protection authority of another State.

§ 3. When the inspector-general has sent the file to the public prosecutor, and the public prosecutor's office subsequently decides not to institute criminal proceedings or propose an

amicable settlement or mediation in criminal matters as referred to in Article 216ter of the Code of Criminal Procedure, or where the public prosecutor's office has not made a decision within a period of six months from the date on which the file was received, the Data Protection Authority shall decide whether the administrative procedure should be resumed.

Section 3. - Procedure for the litigation chamber

Sub-section 1. - Referral to the litigation chamber

Art. 92. The litigation chamber can be invoked:

1° by the front office, in accordance with Article 62, § 1, for dealing with a complaint;
2° by a party involved in lodging an appeal, in accordance with Articles 71 and 90, against measures taken by the inspection service;
3° by the inspection service after it has closed an investigation in accordance with Article 91 § 2.

Art. 93. In principle, the procedure for the litigation chamber shall be conducted in writing. However, the litigation chamber can also hear the parties involved.

Sub-section 2. - Procedure prior to the decision on the merits

Art. 94. Once invoked, the litigation chamber can:

1° ask the inspection service to conduct an investigation in accordance with Article 63, 2°;
2° request the inspectorate to carry out an additional investigation if the litigation chamber is invoked in accordance with Article 92, 3°;
3° address the complaint without having invoked the inspection service on its own initiative.

Art. 95. § 1. The litigation chamber shall decide on how it will monitor the case and shall be authorised:

1° to decide that the case is ready for processing on the merits;
2° to propose a settlement;
3° to dismiss the complaint;
4° to issue warnings;
5° to order that the requests made by the data subject with regard to exercising his/her rights are complied with;
6° to order that the individual concerned be notified of the security problem;
7° to refer the case to the public prosecutor's office in Brussels, which will inform it of how to proceed;
8° to decide on a case-by-case basis to publish its decisions on the website of the Data Protection Authority.

§ 2. In the cases referred to in § 1, 4° to 6°, it shall inform the parties concerned immediately by registered mail of:

1° the fact that a case is pending;
2° the content of the complaint, where appropriate excluding the documents from which the identity of the person submitting the complaint can be deduced;
3° the possibility to view and copy the case file at the secretariat of the litigation chamber,

where appropriate excluding the documents from which the identity of the person submitting the complaint can be deduced, as well as the days and times when such consultation is possible.

§ 3. If, after the application of § 1, 7°, the public prosecutor's office decides not to institute criminal proceedings or propose an amicable settlement or mediation in criminal matters as referred to in Article 216ter of the Code of Criminal Procedure, or where the public prosecutor's office has not made a decision within a period of six months from the date on which the case was received, the Data Protection Authority shall decide whether or not the administrative procedure should be resumed.

Art. 96. § 1. The request by the litigation chamber, referred to in Article 94, 1°, for an investigation to be conducted must be submitted to the inspector-general of the inspection service within thirty days of the complaint having been referred to the litigation chamber by the front office.

§ 2. The request by the litigation chamber, in accordance with Article 94, 2°, for an additional investigation to be conducted must be submitted to the inspector-general of the inspection service within thirty days of the case having been referred to the litigation chamber by the inspection service.

Art. 97. If the report by the inspector-general makes mention of findings establishing infringements of legislation other than those relating to the protection of personal data, the litigation chamber must then send a copy of those findings to the public prosecutor.

Sub-section 3. - Deliberation and decision on the merits

Art. 98. If the litigation chamber decides that the case is ready for processing on the merits, it shall immediately inform the parties concerned by registered mail of the provisions set out in Article 95, § 2, as well as of the option to:

1° accept all communication concerning the matter electronically;
2° submit their defences and request a hearing;
3° add all documents they deem useful to the case file.

Art. 99. The litigation chamber shall invite the parties to submit their defences.

Art. 100. § 1. The litigation chamber shall have the authority to:

1° dismiss a complaint;
2° order criminal proceedings;
3° order suspension of the judgement;
4° propose a settlement;
5° issue warnings and reprimands;
6° order that the requests made by the individual concerned with regard to exercising his/her rights are complied with;
7° order that the individual concerned be notified of the security problem;
8° order that the processing be frozen, limited or prohibited temporarily or permanently;
9° order that the processing be brought into line;
10° order the rectification, restriction or deletion of data and notification of the same to the

recipients of the data;
11° order withdrawal of recognition by certification bodies;
12° impose penalty payments;
13° impose administrative fines;
14° order the suspension of cross-border data flows to another state or an international institution;
15° refer the case to the public prosecutor's office in Brussels, which will inform it of how to proceed;
16° to decide on a case-by-case basis to publish its decisions on the website of the Data Protection Authority.

§ 2. If, after the application of § 1, 15°, the public prosecutor's office decides not to institute criminal proceedings or propose an amicable settlement or mediation in criminal matters as referred to in Article 216ter of the Code of Criminal Procedure, or where the public prosecutor's office has not made a decision within a period of six months from the date on which the case was received, the Data Protection Authority shall decide whether or not the administrative procedure should be resumed.

Art. 101. The litigation chamber can decide to impose an administrative penalty on the parties being investigated in accordance with the general provisions set out in Article 83 of Regulation 2016/679.

Art. 102. The decision to impose the administrative penalty must state the reasons for this and determine the amount of the penalty.

The administrative penalty must be paid within thirty days of the date of the registered mail with acknowledgement of receipt containing the decision to impose the administrative penalty.

Art. 103. In the case of concurrent infringements, the amounts of the administrative penalties referred to in Article 83 of Regulation 2016/679 shall be combined, although the total amount may not exceed double the highest penalty applicable to the infringements committed.

If an offender has committed multiple infringements by means of one and the same action, only the heaviest administrative penalty for the various infringements shall apply.

Art. 104. No account may be taken of a decision in which an administrative penalty was imposed or the individual concerned was found guilty and which dates back to three years or more prior to the facts.

The three-year period shall commence as soon as the decision has become enforceable or when the court ruling in which the judgement was delivered in the appeal has the force of res judicata.

Art. 105. The period of limitation concerning the facts shall be five years after they were committed.

The period of limitation shall only be interrupted by acts of investigation or prosecution.

Such acts shall entail the commencement of a new period of the same duration, even with regard to the individuals not involved therein.

Art. 106. The period of limitation for the administrative penalties shall be five years from the date on which they should have been paid.

The period of limitation shall be suspended if an appeal is lodged against the decision of the dispute chamber to impose an administrative penalty.

Art. 107. The fines, penalties and transactions imposed under the provisions of this law shall be paid or collected for the benefit of the Treasury by the general administration for collection and enforcement.

Sub-section 4. - Notification and appeal procedure

Art. 108. § 1. The litigation chamber shall inform the parties of its decision and the option to appeal to the Market Court within a period of thirty days from the service of the notification.

Subject to the exceptions provided for by the law, or unless the litigation chamber orders otherwise by way of a special reasoned decision, the ruling shall be provisionally enforceable, notwithstanding the appeal.

The decision to delete the data in accordance with Article 100, § 1, 10° shall not be provisionally enforceable.

§ 2 An appeal can be lodged against the decisions of the litigation chamber on the basis of Articles 71 and 90 with the Market Court dealing with the matter in the interim proceedings in accordance with Articles 1035 to 1038, 1040 and 1041 of the Judicial Code.

CHAPTER 7. - Suspension, transitional and concluding provisions

Art. 109. Chapter VII and chapter VIIbis of the law dated 8 December 1992 on the protection of privacy with regard to the processing of personal data are repealed.

Art. 110. This act shall enter into force on 25 May 2018, with the exception of Chapter III, which will enter into force on the date this act is published in the Belgian Official Journal.

The King may, for any provision of the same, with the exception of Chapter III, determine a date of entry into force prior to the date stated in the first paragraph.

Art. 111. Without prejudice to the supervisory powers of the Commission for the protection of privacy, the authorisations granted by the sector committees of the Commission for the protection of privacy shall retain their legal validity before the entry into force of this act.

Once this law has entered into force, a general authorisation granted during the deliberations of a sectoral committee may only be obtained provided that the applicant sends a written, signed undertaking to the Data Protection Authority in which he/she confirms that he/she will adhere to the conditions of the relevant deliberation, notwithstanding the supervisory powers that the Data Protection Authority can exercise after receiving the undertaking.

Subject to other legal provisions, pending requests for authorisations from before the law entered into force shall be handled by the Data Protection Officer of the institutions involved in the exchange of data.

Art. 112. Chapter VI shall not apply to complaints or requests that are still pending with the Data Protection Authority at the time this law entered into force.

The complaints or applications referred to in the first paragraph shall be dealt with further by the Data Protection Authority, as the legal successor of the Commission for the protection of privacy, in accordance with the procedure applying before the law entered into force.

Art. 113. The statutory and contractual staff members recruited by the Commission for the protection of privacy shall be transferred to the Data Protection Authority on the date Article 109 enters into force, with such staff at least retaining their status and rights, their seniority, as well as their pay and allowances and other benefits granted to them in accordance with the relevant regulations or contract of employment.

Art. 114. § 1. The term of office of the members of the Commission for the protection of privacyshall end on the day on which the members of the executive committee take the oath referred to in the third paragraph of Article 12 and sign the declaration referred to in the first paragraph of Article 44, § 2 that no conflicts of interest exist.

During the period between 25 May 2018 and the date referred to in the first paragraph above, the members of the Commission for the protection of privacyshall exercise the duties and powers of the Data Protection Authority.

Up to the end of their term of office, the members of the Commission for the protection of privacyshall be remunerated and treated in statutory terms in accordance with the law dated 8 December 1992 on the protection of privacy with regard to the processing of personal data.

§ 2. The term of office of the external members of the sectoral committees of the federal government, the Crossroads Bank for Enterprises and the Statistical Supervisory Committee shall end on 25 May 2018.

§ 3. The term of office of the external members of the Sectoral Committee for Social Security and Health shall end on the day on which their term of office is terminated by law.

The Sectoral Committee for Social Security and Health shall meet during the period between 25 May 2018 and the day referred to in the first paragraph above as a body into which both sections are integrated, and shall perform the duties that are compatible with Regulation 2016/679.

The chairman of the Sectoral Committee for Social Security and Health shall be regarded as an external member during the period referred to in the second paragraph above and be treated as such.

The operating costs, the remuneration amounts paid out and reimbursements of expenses shall be borne by the Crossroads Bank for Social Security and the eHealth platform during the period referred to in the second paragraph above.

§ 4. The term of office of the external members of the Sectoral Committee for the National Register shall end on the day on which their term of office is terminated by law.

During the period between 25 May 2018 and the date referred to in the first paragraph above, the Sectoral Committee for the National Register shall perform the duties of the Sectoral Committees for the National Register and for the federal government that are compatible with Regulation 2016/679.

The chairman of the Sectoral Committee for the National Register shall be regarded as an external member during the period referred to in the second paragraph above and be treated as such.

The operating costs, the remuneration amounts paid out and reimbursements of expenses shall be borne by the Federal Public Service for Policy and Support during the period referred to in the second paragraph above.

The Federal Public Service for Policy and Support shall draw up the legal and technical opinions, where applicable in consultation with the Federal Public Service for the Interior.

Art. 115. The term of office of the chairman and vice-chairman of the Data Protection Commission shall be deemed equivalent to a permanent appointment with regard to pensions. They shall benefit from the pension scheme applying to civil servants of the general administration. These pensions shall be payable by the Treasury.

Art. 116. Pursuant to Article 51(3) and Article 68(4) of Regulation 2016/679 and in accordance with Article 41(4) of Directive (EU) 2016/680 of the European Parliament and the Council dated 27 April 2016 on the protection of natural individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, the Data Protection Authority shall be the joint representative of the Belgian supervisory authorities within the European Data Protection Board.