Unofficial consolidated version
Updated to October 2017

30 NOVEMBER 1998

ACT GOVERNING THE [INTELLIGENCE AND SECURITY SERVICES]

(BOJ 18 December 1998)

Heading replaced under Article 2 of the Act of 30 March 2017 (BOJ 28 April 2017).

CHAPTER I
GENERAL PROVISIONS

Article 1

This Act governs a matter specified in Article 78 of the [Belgian] Constitution.

Article 2

[§ *1.*][1] This Act is applicable to State Security (the civilian intelligence and security service) and to the [General Intelligence and Security Service][3] (the military intelligence and security service), which are the two intelligence and security services of the Kingdom [of Belgium].

In the execution of their assignments these services are responsible for compliance with and contribute to the protection of individual rights and freedoms and to the democratic development of society.

[The intelligence collection methods used by the intelligence and security services covered by this Act][4] cannot be used with the intention of infringing or violating individual rights and freedoms.

Any use of a specific or exceptional intelligence collection method implies compliance with the principles of subsidiarity and proportionality.][1] [The evaluation of the principle of subsidiarity takes account of the risks that executing the intelligence assignment entails for the safety of the agents and third parties.][4]

[§ *2.* The intelligence and security services are not permitted to acquire, analyse or make use of data which are protected by either the professional secrecy of a lawyer or a doctor, or the confidentiality of journalistic sources.

Exceptionally, and where the service in question is in prior possession of serious evidence that the lawyer, doctor or journalist is or has been personally and actively involved in the creation or development of the potential [threat][3], as defined in Articles 7, 1. […][3] and 11, [or in the activities of foreign intelligence services within Belgian territory][4], these protected data […][4] can be acquired, analysed or used.][1]

[§ *3.* [Without prejudice to the Act of 11 December 1998 on classification and security clearances, certificates and advice, the Open Government Act of 11 April 1994 and the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, and at the request of any natural person with a personal and legal interest who falls under Belgian jurisdiction, the head of service shall notify that person in writing that he or she has been the subject of a method covered by Articles 18/12, 18/14 or 18/17, provided that:

1. a period of more than ten years has passed since the termination of the method;

2. the notice cannot cause any harm to an intelligence investigation;

3. the obligations referred to in Articles 13, paragraph 3 and 13/4, paragraph 2 are not affected;

4. the notice cannot cause any harm to Belgium's relationships with foreign States and international or supranational institutions.

If the request is inadmissible or the person involved has not been the subject of a method covered by Articles 18/12, 18/14 or 18/17, or if the conditions for the notice have not been fulfilled, the head of service shall notify the person that their request under this section cannot be granted.

If the request is admissible, the person involved has been the subject of a method covered by Articles 18/12, 18/14 or 18/17 and the conditions for the notice have been fulfilled, the head of service shall indicate what method has been used and on which statutory basis.

The head of the intelligence and security service in question shall notify the Standing Committee I of each request for information and the response given, and further provide a concise motivation. The application of this provision is the subject of the report of the Standing Committee I to the Chamber of Representatives as referred to in Article 35, § 2 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

By means of a Royal Decree adopted after deliberation in the Council of Ministers and based on the opinion of the National Security Council, the King shall lay down the further rules with which the request must comply.][2, 4]

[1]Supplemented under Article 2 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]nullified by the Constitutional Court on 22 September 2011, no. 145/2011, [3]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [4]replaced, supplemented, introduced and repealed under Article 4 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 3

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

[*1.* "National Security Council": the Council established within the Government that is tasked with the national security duties as determined by the King;][2, 5]

2. "agent": every member of the statutory or contractual personnel and every member of the Armed forces who operates within one of the intelligence and security services referred to in Article 2;

[*3.* "intervention team member":

a) for State Security, the agent, as referred to in Articles 22-35, who is tasked with protecting the personnel, infrastructure and assets of State Security;

b) for the General Intelligence and Security Service, the agent, as referred to in Articles 22-35, who is tasked with protecting the personnel, infrastructure and assets of the General Intelligence and Security Service;][3, 5]

4. "[General Intelligence and Security Service][4]": the [General Intelligence and Security Service][4].

[*5.* "the Minister": for State Security, the Minister of Justice, and for the [General Intelligence and Security Service][4], the Minister of Defence;

6. "the Commission": the administrative commission charged with supervision of the specific and exceptional methods for the collection of intelligence by the intelligence and security services which is established under Article 43/1;

7. "the Standing Committee I": the Standing Intelligence Agencies Review Committee, as referred to in the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment;

8. "the head of service": firstly, the Administrator-General of State Security or, in his absence, the acting Administrator-General, and secondly, the Head of the [General Intelligence and Security Service][4] or, in his absence, the acting Head;

9. "the intelligence officer":

a) for State Security, the agent [...][5] who holds at least the rank of commissioner;

b) for the [General Intelligence and Security Service][4], the officer assigned to this service, as well as the civil servant who holds at least the rank of commissioner;

10. "communication": any transmission, broadcast, or reception of signs, signals, text, images, sounds or data of any nature, by wire, radio-electricity, optical signalling or another electromagnetic system; communication by telephone, mobile telephone, radio telephone, telex, fax or electronic data transmission via computer or computer network, or any other private communication;

11. "electronic communications networks": the electronic communications networks as defined in Article 2, 3. of the Act of 13 June 2005 on electronic communications;

[*11.(1)* "electronic communications service provider": any party which in any way provides or offers a service within Belgian territory that consists in transmitting signals via electronic communications networks, or that consists in allowing users to obtain, receive and distribute information via an electronic communications network;

12. "publicly accessible place": any place, public or private, which can be accessed by the public;

12.(1) "place that is inaccessible to the public and not hidden from view": any place that cannot be accessed by the public and that is visible to everyone from the public road without any equipment or artifice, except for the interior of buildings that are not accessible to the public;][5]

13. "post": postal services as defined in Article 131, 6., 7. and 11. of the Act of 21 March 1991 on the reform of certain economic public companies;

14. "technical [means][5]": a configuration of components which detects, transfers, activates the recording of and records signals, [other than:

a) a device that is used to take photographs;

b) a mobile device that is used to record moving images if taking photographs could not guarantee the discretion and safety of the agents, on condition that this use is preauthorised by the head of service or his delegate. Only images that are deemed relevant will be kept on record. The other images will be destroyed within one month of the recording date;][5]

15. "radicalisation process": a process whereby an individual or a group of individuals is influenced in such a manner that that individual or group of individuals is mentally shaped or prepared to commit terrorist acts;

16. "journalist": a journalist who is entitled to the title of professional journalist under the Act of 30 December 1963 on the recognition and the protection of the title of professional journalist;

17. "confidentiality of sources": the confidentiality described in the Act of 7 April 2005 on the protection of journalistic sources;

18. "Director of Operations of State Security": the agent of the field services of State Security, holding the grade of commissioner-general, appointed to head the field services of State Security.][1]

[*19.* "locked object": an object that must be opened with the help of a picklock or by forced entry;

20. "observation": the monitoring of one or more people, their presence or conduct, or of items, places or events;

21. "search": entering, inspecting and examining a place, as well as inspecting and examining an object.][5]

[1]Supplemented under Article 3 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]repealed under Article 4 of the Act of 6 December 2015 (BOJ 17 December 2015), [3]repealed under Article 17 of the Act of 21 April 2016 (BOJ 29 April 2016), [4]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [5]restored, repealed, replaced, introduced and supplemented under Article 5 of the Act of 30 March 2017 (BOJ 28 April 2017).

CHAPTER II
ORGANISATION AND ASSIGNMENTS

Section 1 – State Security

Article 4

State Security carries out the duties assigned to it by the Minister of Justice in accordance with the guidelines of the [National Security Council].

Replaced under Article 6 of the Act of 6 December 2015 (BOJ 17 December 2015).

Article 5

§ 1. State Security carries out the duties assigned to it under the authority of the Minister of Justice.

§ 2. The Minister of the Interior can nevertheless requests State Security to intervene in connection with the execution of assignments provided for [in Article 7, 1.], if these concern the maintenance of public order and the protection of persons.

In such a case the Minister of the Interior, without becoming involved in the organisation of the service, specifies the subject of the request and can make recommendations and give precise indications concerning the means to be employed and the financial resources to be allocated.

Should it prove impossible to act on such recommendations and indications because their execution would jeopardize the execution of other assignments, the Minister of the Interior shall be informed thereof at the earliest opportunity. This does not discharge State Security from the obligation to execute the request.

§ 3. The Minister of Justice is responsible for the organisation and the general management of State Security, especially with regards to expenditure, staff management and training, internal order and discipline, pay and expenses, and equipment.

Replaced under Article 18 of the Act of 21 April 2016 (BOJ 29 April 2016).

Article 6

§ 1. The Minister of the Interior is, in accordance with §§ 2, 3 and 4, involved in the organisation and management of State Security, whenever this organisation and management have a direct influence on the execution of assignments relating to the maintenance of public order and the protection of persons.

Should the Minister of Justice be unable to act on a request from the Minister of the Interior, then he shall inform him of the reasons for this.

§ 2. The co-signature of the Minister of the Interior is required for:

1. all government bills concerning State Security;

2. all draft statutory decrees concerning the general organisation of State Security.

§ 3. The assent from the Minister of the Interior is required for:

[…]

2. all draft royal decrees concerning the nomination and appointment of officials-general for State Security;

[…]

[…]

[…]

[…]

7. all draft statutory decrees concerning the specific duties of the official in charge of State Security;

The Minister of the Interior shall issue his opinion within the time period set by the Minister of Justice. This period may not be less than twenty working days. In the event of reasoned urgent necessity, this period can be reduced to five working days. If this time period elapses, the opinion shall be deemed to have been favourable. Reasons must be given if an opinion is unfavourable.

§ 4. The King shall decide matters concerning the organisation and management of State Security, other than as specified in §§ 2 and 3, and which have a direct influence on the execution of assignments relating to the maintenance of public order and the protection of persons, and for which the Minister of Justice requests an opinion from or notifies the Minister of the Interior, as well as additional rules in this respect.

Repealed under Article 19 of the Act of 21 April 2016 (BOJ 29 April 2016).

Article 7

The duties of State Security are:

1. collecting, analysing and processing intelligence related to any activity which threatens or could threaten the internal security of the State and the maintenance of democratic and constitutional order, the external security of the State and international relations, the scientific and economic potential, as defined by the [National Security Council][1], or any other fundamental interest of the country, as defined by the King on the motion of the [National Security Council][1];

2. the execution of security investigations entrusted to it in accordance with the guidelines of the [National Security Council][1].

[…][3]

[*3./1* collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory;][2]

4. the execution of all other assignments entrusted to it pursuant to the law.

[1]Replaced under Article 6 of the Act of 6 December 2015 (BOJ 17 December 2015), [2]introduced under Article 2 of the Act of 29 January 2016 (BOJ 24 February 2016) and [3]repealed under Article 20 of the Act of 21 April 2016 (BOJ 29 April 2016).

Article 8

For the application of Article 7 the following definitions shall apply:

1. "activity which threatens or could threaten": any individual or collective activity conducted in the country or from abroad which could be related to espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations, including the distribution of propaganda, the encouragement or direct or indirect support, inter alia by

providing financial, technical or logistical resources, the provision of [information][2] on possible targets, the development of structures and capabilities and the realisation of the intended purposes.

For the application of the preceding paragraph the following definitions shall apply:

a) espionage: seeking or providing [information which is not accessible to the public][2] and the maintenance of secret relationships which could prepare for or facilitate these activities;

b) terrorism: the use of force against persons or material interests for ideological or political reasons with the aim of achieving its objectives by means of terror, intimidation or threats [. This also includes the radicalisation process][2];

c) extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless of whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions or other basic aspects of the constitutional state[; This also includes the radicalisation process][2];

d) proliferation: trade or transactions concerning materials, products, goods or know-how which could contribute to the production or development of non-conventional or very advanced weapons systems. This refers among others to the development of nuclear, chemical and biological weapons programmes and the transmission systems associated with them, as well as the persons, structures or countries involved;

e) harmful sectarian organisation: any group with a philosophical or religious character or one which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society or violates human dignity;

f) criminal organisation: any structured association of more than two people lasting over time, aiming to carry out criminal acts and offences by mutual agreement, in order to directly or indirectly acquire material benefits, where use is made of intimidation, threats, violence, trickery or corruption, or where commercial or other structures are used to conceal or facilitate the commission of crimes. This means the forms and structures of criminal organisations which have a substantial relationship to the activities referred to in Article 8, 1., a) to e) and g), or which could have a destabilising impact on a political or socio-economic level;

g) interference: an attempt to use illegal, fraudulent or clandestine means to influence decision-making processes;

2. "the internal security of the State and the maintenance of democratic and constitutional order":

a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental freedoms;

b) the safety and the physical and moral protection of persons and the safety and protection of goods;

3. "the external security of the State and international relations": the protection of the inviolability of the national territory, the sovereignty and independence of the State, the interests of the countries with which Belgium pursues common objectives, and the international and other relationships which Belgium maintains with other States and international or supranational institutions;

4. "the scientific or economic potential": the protection of the key elements of the scientific or economic potential;

[...][1]

[1]Repealed under Article 21 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]replaced and introduced under Article 6 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 9

At the request of State Security the [General Intelligence and Security Service][2] shall cooperate with State Security in the collection of intelligence whenever military personnel are involved in the activities specified in Article 7, 1. [and 3./1][1].

[1]Supplemented under Article 3 of the Act of 29 January 2016 (BOJ 24 February 2016) and [2]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Section 2 - [The General Intelligence and Security Service]

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 10

§ 1. The [General Intelligence and Security Service][2] carries out the assignments entrusted to it by the Minister of Defence in accordance with the guidelines of the [National Security Council][1].

§ 2. The [General Intelligence and Security Service][2] carries out the duties assigned to it under the authority of the Minister of Defence.

§ 3. The Minister of Defence is responsible for the organisation and the general management of the [General Intelligence and Security Service][2], especially with regard to expenditure, staff management and training, internal order and discipline, pay and expenses, and equipment.

[1]Replaced under Article 6 of the Act of 6 December 2015 (BOJ 17 December 2015) and [2]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 11

[*§ 1.* The duties of the General Intelligence and Security Service are:

1. collecting, analysing and processing intelligence relating to the factors that affect or could affect national and international security to the extent that the Armed Forces are or could be involved in providing intelligence support to their current or any future operations, as well as the intelligence relating to any activity that threatens or could threaten:

a) the inviolability of the national territory or the population,

b) the military defence plans,

c) the scientific and economic potential relating to the players, being both natural and legal persons, which are active in the economic and industrial sectors related to defence and included on a list approved by the National Security Council on a motion of the Minister of Justice and the Minister of Defence,

d) the execution of the assignments of the Armed forces,

e) the safety and security of Belgian nationals abroad,

f) any other fundamental interest of the country, as defined by the King on the motion of the National Security Council;

and immediately informing the competent Ministers thereof and advising the government, at its request, on the description of its internal and foreign policy in relation to security and defence;][6]

2. maintaining military security for personnel who come under the Minister of Defence, military installations, weapons [and weapon systems][6], munitions, equipment, plans, texts, documents, computer and communications systems or other military objects [and, in the context of cyber attacks on [weapon systems][6], military computer and communications systems or systems managed by the Minister of Defence, neutralising the attack and identifying its perpetrators, without prejudice to the right to respond immediately with its own cyber attack in accordance with the provisions of the law on armed conflicts][1];
3. protecting the secrecy related, in accordance with Belgium's international commitments or in order to ensure the inviolability of the national territory and the execution of the assignments of the Armed forces, to military installations, weapons, munitions, equipment, to plans, texts, documents or other military objects, to military intelligence and communications, and to military computer and communications systems or systems managed by the Minister of Defence;

4. executing security investigations entrusted to it in accordance with the guidelines of the [National Security Council][3].

[5. collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory.][4]

§ 2. For the application of § 1 the following definitions shall apply:

1. "activity which threatens or could threaten the inviolability of the national territory [or the population][6]": any expression of the intent to use military means to capture, occupy or attack the entire territory or a part of it as well as the airspace above that territory or the territorial waters, or to jeopardise the protection or the continued existence [of the entire population or a part of it][6], the national heritage or the economic potential of the country;

2. "activity which threatens or could threaten military defence plans": any expression of the intent to obtain unauthorized access to plans concerning the military defence of the national territory, the airspace above that territory or the territorial waters and the vital interests of the State, or concerning common military defence in the context of an alliance or international or supranational cooperation;

[2./1 "activity which threatens or could threaten the scientific and economic potential relating to the players, being both natural and legal persons, which are active in the economic and industrial sectors related to defence and included on a list approved by [the National Security Council][2] on a motion of the Minister of Justice and the Minister of Defence": any expression of the intent to jeopardise key elements of the scientific and economic potential of these players;][1]

3. "activity which threatens or could threaten the execution of the assignments of the Armed forces": any expression of the intent to neutralise, hinder, sabotage, jeopardize or prevent the preparation, mobilisation and use of the Belgian Armed forces, of allied Armed forces or of inter-allied defence organisations for missions, actions or operations in a national context or in the context of an alliance or an international or supranational cooperation agreement;

4. "activity which threatens or could threaten the safety of Belgian nationals abroad": any expression of the intent to collectively endanger the life or physical integrity of Belgians abroad and their family members [...][6].

§ 3. At the request of the [General Intelligence and Security Service][5], State Security shall cooperate in the collection of intelligence whenever persons not answerable to the Minister of Defence and with no connection to enterprises who execute contracts related to military matters concluded with the said Minister, with international military organisations or with third countries, or who are participating in a public tender procedure offered by these latter, are involved in activities [specified in section 1, 1., 2., 3. and 5.][4].

The measures for the protection of industrial property are only taken when the Minister of Defence, third countries or organisations to which Belgium is linked under treaty or contract request such action.

[1]Introduced and supplemented under Article 4 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 5 of the Act of 6 December 2015 (BOJ 17 December 2015), [3]replaced under Article 6 of the Act of 6 December 2015 (BOJ 17 December 2015), [4]supplemented and replaced under Article 4 of the Act of 29 January 2016 (BOJ 24 February 2016), [5]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [6]replaced, introduced and repealed under Article 7 of the Act of 30 March 2017 (BOJ 28 April 2017).

[CHAPTER III
EXECUTION OF THE INTELLIGENCE AND SECURITY ASSIGNMENTS]

Heading replaced under Article 8 of the Act of 30 March 2017 (BOJ 28 April 2017).

[…]

Heading repealed under Article 9 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 1] - General provisions

Heading renumbered under Article 10 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 12

The intelligence and security services may only use coercive measures in order to fulfil their assignments under the conditions set out in law.

Article 13

[The intelligence and security services may][3] seek, collect, receive and process [information][2] and personal data liable to be of value in the execution of their assignments and keep records thereof, more specifically as regards the events, groups and persons who are of importance for the execution of their assignments.

The intelligence included in these records must be related to the purposes of the data set and shall remain limited to the requirements thereof.

[The intelligence and security services shall ensure the security of the data that relates to their sources and of the information and personal data that these sources yield.][1, 2]

[The agents of the intelligence and security services have access to the information, intelligence and personal data collected and processed by their service, insofar as this is useful for the performance of their duties or execution of their assignment.][2]

[1]Supplemented under Article 5 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced and supplemented under Article 12 of the Act of 29 May 2016 (BOJ 18 July 2016) and [3]replaced under Article 11 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 2 - Protection and support measures]

Heading introduced under Article 12 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 13/1

[…][2]

[Agents may not commit criminal offenses.

In derogation of the first paragraph, agents tasked with implementing intelligence collection methods, as well as the members of the intervention team who, for the purpose of their duties, commit infringements, breaches of the traffic regulations or theft for use that are strictly necessary for the successful execution of the method or to ensure their own safety or that of other persons, shall not be subject to penalties.

Without prejudice to the second paragraph, agents who, while implementing the methods specified in Article 18/2, with the prior written consent of the Commission given within four days of receipt of the written request from the head of service, commit criminal offense which are strictly necessary for the successful execution of the method or to ensure their own safety or that of other persons, shall not be subject to penalties. If the matter is urgent, the head of service shall request the prior verbal consent of the chairman of the Commission. The chairman of the Commission shall confirm this verbal consent in writing as soon as possible. The Commission or the chairman shall notify the Standing Committee I of their consent.

In derogation of the third paragraph, if the strict necessity of committing a criminal offense to ensure the safety of agents or other persons was not foreseeable, and it was likewise not possible to obtain the prior consent of the Commission or of the chairman in case of an urgent procedure, the head of service shall notify the Commission as soon as possible that a criminal offense has been committed. If the Commission, after evaluating, decides that the criminal offense was strictly necessary and unforeseeable, the agent shall not be subject to penalties. The Commission shall notify the Standing Committee I of this consent.][2]

The criminal offenses covered [by the second to fourth paragraphs][2] must be proportionate to the purpose of the intelligence assignment and may in no case harm the physical integrity of persons.

[…][2]

The members of the Commission who grant authority for the commission of criminal offenses as specified in [the third and fourth paragraph][2] shall not be subject to penalties.][1]

[1]Introduced under Article 6 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced, introduced and repealed under Article 13 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 13/2

For security reasons relating to their own personal protection or the protection of third parties, agents may use a name that does not belong to them, as well as a fictitious identity and capacity, in accordance with further rules to be determined by the King.

The measure referred to in the first paragraph may not be used autonomously for intelligence collection.

Any active use of a fictitious identity must be temporary and targeted, and be mentioned in a list that is submitted monthly to the Standing Committee I.

The intelligence and security services may produce, arrange for the production of and use false documents for the purpose of creating and using a false name or a fictitious identity and capacity.

Every creation of official documents to prove a fictitious identity or capacity shall be authorised by the head of service and communicated to the Standing Committee I.

The intelligence and security services may request the cooperation of civil servants and agents of the public services for the purpose of executing the measures referred to in this article.][1, 2]

[1]Introduced under Article 7 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 14 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 13/3

§ *1*. The intelligence and security services may incorporate legal persons, in accordance with further rules to be determined by the King. These further rules may deviate from the legal provisions which are applicable in the event of the dissolution and settlement of a legal person.

§ *2*. The intelligence and security services may use legal persons in support of their assignments.

Without prejudice to the first paragraph, the further rules for using a legal person for intelligence collection are laid down in Article 18/13.

§ *3*. The intelligence and security services may produce, arrange for the production of and use false documents for the purpose of applying sections 1 and 2.

§ *4*. Every incorporation of a legal person shall be authorised by the head of service and communicated to the Standing Committee I.

Any use of a legal person other than in the case envisaged in Article 18/13 shall be mentioned in a list that is submitted monthly to the Standing Committee I.

§ *5*. The intelligence and security services may request the cooperation of civil servants and agents of the public services for the purpose of executing this article.][1, 2]

[1]Article 18/13, first paragraph, introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2] renumbered and replaced under Article 15 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 13/4.

The intelligence and security services may request the cooperation of third parties.

The services shall ensure the security of the data relating to the third parties that are cooperating or have cooperated with them.

The second, third and fifth paragraphs of Article 13/1 apply to third persons who have provided necessary and direct help and assistance in the execution of a method.]

Introduced under Article 16 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 3 - Overlap with a criminal investigation or judicial inquiry]

Heading introduced under Article 17 of the Act of 30 March 2017 (BOJ 28 April 2017).

[[Article 13/5][2]

The intelligence and security services shall ensure that they do not conduct investigations that deliberately affect the [assignments of the competent magistrate][2] or that could hinder the proper progress of criminal investigations or judicial inquiries.

When an intelligence and security service opens an investigation which could affect a criminal investigation or judicial inquiry, this service, if it is using the intelligence collection methods specified in Article 18/2, may not obstruct this criminal investigation or judicial inquiry.

The intelligence and security service shall notify the Commission of this. Without prejudice to the agreements concluded with the judicial authorities, the Commission, in consultation with […][2] the competent magistrate and the head of the service involved [or the agent that he authorises for that purpose][2], shall decide whether and under which further rules the intelligence and security service may continue the investigation. The Commission shall notify the Standing Committee I of its decision. The intelligence and security service shall execute its assignment in accordance with the decision of the Commission. The Commission shall supervise compliance with its decision.][1]

[1]Introduced under Article 7 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]renumbered, introduced, replaced and repealed under Article 18 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 4 - Intelligence collection methods]

Heading introduced under Article 19 of the Act of 30 March 2017 (BOJ 28 April 2017).

Subsection [1][2] - [Ordinary intelligence collection methods][1]

[1]Heading replaced under Article 8 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]renumbered under Article 20 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 14

[…][2] [The judicial authorities][2], civil servants and agents of the public services[, including those of the police services,][1] [may][2], of their own accord, [pass information that is useful for the execution of its assignments][2] to the intelligence and security service in question.

[At the request of an intelligence and security service, the judicial authorities, civil servants and agents of the public services, including those of the police services, shall pass [information that is useful for the execution of its assignments][2] to the intelligence and security service in question. When judicial authorities, civil servants and agents of the public services, including those of the police services, are of the opinion that the sharing of the information covered by the second paragraph is liable to hinder an ongoing criminal investigation or judicial inquiry, or the collection of intelligence under [the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash][3], or jeopardise the physical integrity of a person, they may refuse the request within five working days after its submission giving the reasons for this in writing.

[With due regard to the relevant legislation the intelligence and security services, may, in accordance with further general rules determined by the King, gain access to databases held by the public sector which are of use in the execution of their assignments.][1]

[1]Introduced, replaced and supplemented under Article 9 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced, introduced and repealed under Article 21 of the Act of 30 March 2017 (BOJ 28 April 2017) and replaced under Article 150 of the Act of 18 September 2017 (BOJ 6 October 2017).

Article 15

The rules for the communication of information appearing in the population register and the aliens register as well as in the waiting list for aliens are established in a Royal Decree deliberated in the Council of Ministers.

[Article 16

Without prejudice to Article 2, § 2, persons and organisations belonging to the private sector may, of their own accord, pass information and personal data to the intelligence and security services that are useful for the execution of their assignments.[1]

Without prejudice to Article 2, § 2, the intelligence and security services may, in the interest of executing their assignments, collect information and personal data from persons and organisations belonging to the private sector.][1, 2]

[1]Partially replaced under Article 10 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]fully replaced under Article 22 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 16/1

§ *1.* In the interest of executing their assignments, the intelligence and security services may observe the following without the help of technical resources:

1. publicly accessible places;

2. persons and items located there;

3. events that occur there.

§ *2.* In the interest of executing their assignments, the intelligence and security services may do the following without the help of technical resources:

1. search publicly accessible places;

2. search the content of unlocked objects that are located there and not guarded by the owner.][1, 2]

[1]Introduced under Article 11 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 23 of the Act of 30 March 2017 (BOJ 28 April 2017).

[**Article 16/2**

[§ 1][2] In the interest of executing their assignments, the intelligence and security services may request the cooperation of an electronic communications network operator or an electronic communications service provider to proceed with:

1. identifying the subscriber or the usual user of an electronic communications service or the electronic communication device used;

2. identifying the electronic communications services and devices to which a specific person is subscribed or which are normally used by a specific person.

The request shall be made in writing by the head of service or his delegate. If the matter is urgent, the head of service or his delegate may verbally requisition this data. This verbal request will be confirmed by a written request within twenty-four hours.

Every electronic communications network operator and every electronic communications service provider whose cooperation is requested shall submit the requested data to the head of service or his delegate within a period and in accordance with further rules to be set by Royal Decree issued on the motion of the Minister of Justice, the Minister of Defence and the Minister competent for electronic communications.

Subject to compliance with the principles of proportionality and subsidiarity, and subject to registration of the consultation of the data, the head of service or his delegate may also obtain the aforementioned data via access to the customer files of the operator or service provider. On a motion of the Minister of Justice, the Minister of Defence and the Minister competent for

electronic communications, the King shall decide under which technical conditions this access is possible.

[§ *2* For the purpose of executing their assignments, the intelligence and security services may request a bank or financial institution to cooperate in identifying the end user of the prepaid card referred to in Article 127 of the Act of 13 June 2005 on electronic communications, based on the reference of an electronic bank transaction that relates to the prepaid card and that is communicated in advance by an operator or provider pursuant to section 1.

The request shall be made in writing by the head of service or his delegate. If the matter is urgent, the head of service or his delegate may verbally requisition this data. This verbal request will be confirmed by a written request within twenty-four hours.

Every bank or financial institution whose cooperation is requested shall immediately provide the requested data to the head of service or his delegate.

The identification data that the intelligence and security services receive while executing the methods referred to in this section is limited to the identification data referred to in section 1.][2]

[§ *3*][2] Anyone who refuses to provide the requested data or grant the requested access shall be subject to a fine of between twenty-six euros and ten thousand euros.

[§ *4*][2] Both intelligence and security services shall keep a register of all requested identifications and of all identifications made through direct access. The Standing Committee I receives a monthly list of the identifications requested and of each access from [the intelligence and security service in question].[2]][1]

[1]Introduced under Article 222 of the Act of 5 February 2016 (BOJ 19 February 2016) and [2]introduced, amended and replaced under Article 3 of the Act of 1 September 2016 (BOJ 7 December 2016).

[**Article 16/3**

§ 1. In the interest of executing their assignments, and subject to adequate motivation, the intelligence and security services may decide to have access to passenger data as referred to in Article 27 of the Act of 25 December 2016 on passenger data processing.

§ 2. The decision referred to in *§ 1* is taken by a head of service and then forwarded in writing to the Passenger Information Unit referred to in Chapter 7 of the aforementioned Act. The decision, including the underlying motivation, is served upon the Standing Committee I.

The Standing Committee I prohibits the intelligence and security services from using data that was collected in circumstances that do not comply with the legal conditions.

The decision may concern a set of data relating to a specific intelligence investigation. In this case, the list of passenger data consultations is sent to the Standing Committee I once a month.]

Introduced under Article 51 of the Act of 25 December 2016 (BOJ 25 January 2017).– *Entry into force yet to be determined*

Article 17

[In the interest of executing their assignments, the intelligence and security services may][2] always enter publicly accessible places and, with due regard for the sanctity of the home, visit hotel establishments and other establishments providing accommodation.

They may ask the owners, operators or agents of these establishments to produce the [registration data][1] of travellers.

[1]Replaced under Article 12 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 24 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18

[For the purpose of executing their assignments, the intelligence and security services may][3] call upon human sources [to collect intelligence on events, subjects, groups and natural or legal persons that are of importance for the execution of their assignments, in accordance with the guidelines of [the National Security Council][2].][1] […][1]

[1]Introduced and repealed under Article 13 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 6 of the Act of 6 December 2015 (BOJ 17 December 2015) and [3]replaced under Article 25 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Subsection [2][2] - Specific and exceptional intelligence collection methods][1]

[1]Heading introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]renumbered under Article 26 of the Act of 30 March 2017 (BOJ 28 April 2017).

[A. General provisions]

Heading introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010).

[Article 18/1

This subsection is applicable:

1. to State Security for the execution, [within or from the territory of the Kingdom][4], of the assignments referred to in [Articles 7, 1. and 3./1[…][3]][2], without prejudice to Article 18/9, § 1, 1.;

2. to the [General Intelligence and Security Service][3][, without prejudice to Article 18/9, § 1, 2.,][4] for the execution […][4] of the assignments referred to in [Articles 11, § 1, 1. to 3. and 5., and § 2][2], [except for the interception of communications originating or received abroad, as well as penetrating a computer system located abroad and recording fixed or moving images abroad, as referred to in Articles 44 to 44/5.][4]][1].

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 5 of the Act of 29 January 2016 (BOJ 24 February 2016), [3]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [4]replaced, introduced and repealed under Article 27 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/2

§ *1.* [The specific intelligence collection methods are listed in Articles 18/4 to 18/8.][3]

[…][2]

[§ *2.* The exceptional intelligence collection methods are listed in Articles 18/11 to 18/17.][3]

§ *3.* If one of the methods referred to in §§ 1 and 2 is applied to a lawyer, a doctor or a journalist, or to the premises or means of communication that they use for business purposes, or to their home or place of residence, this method may not be carried out until the president of, as appropriate, the Orde van de Vlaamse balies, the Ordre des barreaux francophone et germanophone, the Medical Association or the Association of Professional Journalists [or in the event of illness or indisposition of the President, his substitute][3], has been notified of this fact by the chairman of the Commission referred to in Article 3, 6. The Chairman of the Commission is required to provide the necessary information to the Chairman of the Association of which the lawyer, the doctor or the journalist is a member [or to the Chairman's substitute][3]. The Chairman in question [and his substitute are bound by confidentiality][3]. The

penalties set out in Article 458 of the Penal Code are applicable to breaches of this obligation of confidentiality.

If one of the methods referred to in §§ 1 and 2 is applied to a lawyer, a doctor or a journalist, or to the premises or means of communication that they use for business purposes, or to their home or place of residence, the chairman of the Commission shall check whether the information acquired by this method is directly related to [the potential threat][3], if it is protected by the professional duty of confidentiality of a lawyer or doctor or by the confidentiality of journalistic sources. [If no direct relationship has been demonstrated, the Commission prohibits the intelligence and security services from using this data.][3]

If an exceptional method referred to in § 2 is applied to a lawyer, a doctor or a journalist, the chairman of the Commission or a member of the Commission appointed by him [can][3] be present [...] while this method is employed. [The chairman takes into account the risk that his presence may have for the execution of the assignment, his own safety and the safety of agents and third parties.][3]][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced and introduced under Article 223 of the Act of 5 February 2016 (BOJ 19 February 2016) and [3]replaced and introduced under Article 28 of the Act of 30 March 2017 (BOJ 28 April 2017).

[B. Specific intelligence collection methods]

Heading introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010)

Article 18/3

[§ *1*. In consideration of a potential threat as referred to in Article 18/1, the specific intelligence collection methods referred to in Article 18/2, § 1 can be used if the ordinary intelligence collection methods are considered inadequate to collect the information required to carry out the intelligence assignment. The specific method must be chosen on the basis of the degree of gravity of the potential threat for which it is employed.

The specific method can only be employed after a reasoned written decision by the head of service and after notification of this decision to the Commission.

[*§ 2.* The head of service's decision states:

1. the nature of the specific method;

2. as relevant, the natural or legal persons, [de facto][4] associations or groups, items, places, events or information which are the object of the specific method;

3. the potential threat that justifies the specific method;

4. the actual circumstances that justify the specific method, the motivation relating to subsidiarity and proportionality, including the relationship between the provisions under 2. and 3.;

5. the period within which the specific method can be applied, counting from the moment when the Commission is notified of the decision;

6. the name of the intelligence officer(s) responsible for monitoring the application of the specific method;

7. where relevant, the technical device that is used in the application of the specific method [pursuant to Articles 18/4 or 18/5][3];

8. where relevant, the overlap with a criminal investigation or judicial inquiry;

[*9.* where relevant, the criminal offenses that are strictly necessary for the successful implementation of the method or to ensure the safety of the agents or third parties;

10. where relevant, the serious evidence which shows that the lawyer, the doctor or the journalist is or has been personally and actively involved in creating or developing the potential threat;

11. where relevant, the reasons that justify the extreme urgency;

12. if Article 18/8 is applied, the motivation for the length of the period for which data are to be collected;][3]][2]

[*13*. the date of the decision;

14. the head of service's signature.

The statements as referred to in the provisions under 1.-4., 7., 9., 10., 11. and 14. are prescribed under penalty of illegitimacy.][3]

[*§ 3.* If the matter is extremely urgent, the head of service may verbally authorise the specific method. This verbal decision is confirmed by a reasoned, written decision that includes the statements referred to in § 2, and must arrive at the Commission's headquarters on or before the first working day following the date of the decision.

The intelligence officer may request the cooperation of the persons referred to in Articles 18/6, 18/7 and 18/8 verbally or in writing. The nature of the method will be communicated to them. The intelligence officer must follow up a verbal request with a written confirmation as soon as possible.][3]

§ *4*. The specific method can only be extended or renewed by means of a new decision by the head of service which complies with the conditions given in § 1.][1]

[*§ 5.*][2] The specific methods may only be used with respect to a lawyer, doctor or journalist or the means of communication used by them for professional purposes, provided that the intelligence and security service has prior, serious evidence that the lawyer, doctor or journalist personally and actively participates or has participated in the creation or development of the potential threat and after the Commission, pursuant to Article 18/10, has given its assent on [the draft decision][3] of the head of service.

[*§ 6.*][2] The members of the Commission may at any time carry out checks on the legitimacy of the measures, including compliance with the principles of subsidiarity and proportionality.

To this end they can enter the places where the data relating to the specific method is received or stored by the intelligence and security services, appropriate any useful documents and hear the members of the service.

Data acquired in circumstances which do not comply with the legal provisions in force shall be stored under the supervision of the Commission in accordance with the rules and deadlines decided by the King, on receipt of an opinion of the Privacy Commission. The Commission forbids the intelligence and security services from using this data and shall suspend use of the method employed if it is still in progress.

The Commission shall on its own initiative immediately notify the Standing Committee I of its decision.

[*§ 7.*][2] The intelligence officer who is appointed [to monitor the application of the specific intelligence collection method][2] shall regularly update the head of service on the implementation of this method.

[§ *8*. The head of service shall terminate the specific method when the potential threat which justified it has passed, when the method no longer serves the purpose for which it was adopted, or when he establishes an illegitimacy. He shall notify the Commission of his decision as soon as possible.][2]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]amended, replaced and supplemented under Article 13 of the Act of 29 May 2016 (BOJ 18 July 2016) and [3]introduced, supplemented and replaced under Article 29 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/4

§ *1*. In the interest of executing their assignments, the intelligence and security services may observe the following with the help of technical resources:

1. publicly accessible places;

2. persons and items located there;

3. events that occur there;

and install a technical device there, operate it or remove it.

§ *2*. In the interest of executing their assignments, the intelligence and security services may observe the following with or without the help of technical resources:

1. places not accessible to the public but not hidden from view;

2. persons and items located there;

3. events that occur there;

without entering those places.][1, 2]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 30 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/5

In the interest of executing their assignments, the intelligence and security services may do the following:

1. search publicly accessible places with the help of technical resources;

2. search the content of locked or unlocked objects that are located there;

3. remove the locked or unlocked objects for a strictly limited period, if they cannot be examined on location for technical or safety reasons. These objects must be replaced as soon as possible, unless this would hinder the execution of the assignment.][1, 2]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 31 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/6

§ *1*. [In the interest of executing their assignments,][2] the intelligence and security services may consult the identification data of the sender or recipient of postal items, whether or not entrusted to a postal operator, and identification data of the holder of a P.O. box […][2]. When the cooperation of a postal operator is requested, the head of service shall address a written request to the operator. The nature of the decision shall be communicated to the postal operator from whom cooperation has been requested.

[…][2]

§ *3*. A postal operator who refuses to cooperate under the terms of the present Article shall be subject to a fine of between twenty-six euro and [twenty thousand euro][2]][1].

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]repealed, introduced and replaced under Article 32 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/6/1

In the interest of executing their assignments, the intelligence and security services may requisition transport and travel data from any private transport or travel service provider. The head of service shall send a written request. The nature of the method is communicated to the service provider from which cooperation is requested.

A transport or travel service provider that refuses to provide information in its possession which is requested in accordance with this article shall be subject to a fine of between twenty-six euros and twenty thousand euros.]

Introduced under Article 33 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/7

§ *1.* [In the interest of executing the assignments,][3] the head of service may, by means of a written decision, proceed with or make arrangements for the following:

1. with the help of a technical device, identifying or localising the electronic communications services and devices to which a specific person is subscribed or which are normally used by a specific person;

2. requesting an electronic communications network operator or an electronic communications service provider to provide the data concerning the payment method, the identification of the payment instrument and the date of payment for the subscription or for the use of the electronic communications service. An intelligence and security service may also obtain the aforementioned data with the help of access to the operator's or service provider's customer files.][2]

[…][3]

§ *3.* Every operator of a communications network and every provider of a communications service from whom cooperation is requested to provide the data referred to in § 1 shall submit the requested data to the head of service within a period and in accordance with further rules to be set by Royal Decree issued on the motion of the Minister of Justice, the Minister of Defence and the Minister competent for electronic communications.

On a motion of the Minister of Justice, the Minister of Defence and the Minister competent for electronic communications, the King shall decide under which conditions the access referred to in § 1 is possible for the head of service.

Any person referred to in the first paragraph who refuses to provide the requested data shall be subject to a fine of between twenty-six euro and [twenty thousand euro][3].][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 224 of the Act of 5 February 2016 (BOJ 19 February 2016) and [3]replaced and repealed under Article 34 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/8

§ *1.* [In the interest of executing their assignments, the intelligence and security services may, when necessary, by requesting cooperation from an electronic communications network operator or an electronic communications service provider for that purpose, proceed with or make arrangements for:

1. tracing the call-associated data of electronic communication devices from which or to which electronic communications are being or have been sent;

2. tracing the origin or destination of electronic communications.][2]

In the cases noted in the first paragraph, for each electronic communication device of which the [call-associated data][2] are traced or of which the origin or destination of electronic communications is traced, the day, the time, the duration and if necessary the place of the electronic communication shall be reported and set out in a report.

The nature of the decision shall be communicated to the electronic communications network operator or the electronic communications service provider from whom cooperation has been requested.

§ *2.* [The following provisions apply to the application of the method referred to in § 1 on the data that is stored pursuant to Article 126 of the Act of 13 June 2005 on electronic communications:

1. for a potential threat that relates to an activity that may relate to criminal organisations or harmful sectarian organisations, the head of service, in his decision, can only requisition the data for a period of six months prior to the decision;

2. for a potential threat, other than those referred to in the provisions under 1. and 3., the head of service, in his decision, may only requisition the data for a period of nine months prior to the decision;

3. for a potential threat that relates to an activity that may relate to terrorism or extremism, the head of service, in his decision, may only requisition the data for a period of twelve months prior to the decision.][2]

§ *3.* Every operator of an electronic communications network and every provider of an electronic communications service from whom cooperation is requested to provide the data referred to in § 1, shall submit the requested data to the head of service within a period and in accordance with further rules to be set by Royal Decree issued on the motion of the Minister of Justice, the Minister of Defence and the Minister competent for electronic communications.

Any person referred to in the first paragraph who refuses to provide the technical assistance referred to in the present Article shall be subject to a fine of between twenty-six euro and [twenty thousand euro][3].][1]

[…][2, 3]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]amended and replaced under Article 14 of the Act of 29 May 2016 (BOJ 18 July 2016) and [3]replaced and repealed under Article 35 of the Act of 30 March 2017 (BOJ 28 April 2017).

[C. Exceptional intelligence collection methods]

Heading introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010).

[Article 18/9

§ *1.* The exceptional intelligence collection methods referred to in Article 18/2, § 2 can be employed:

[*1.* by State Security, if there is a serious potential threat to a fundamental interest of the country as referred to in Article 8, 2. to 4., and if this potential threat relates to an activity referred to in Article 8, 1. or relates to an activity of a foreign intelligence service;][3, 5]

[*2.* by the General Intelligence and Security Service, if there is a serious potential threat to a fundamental interest as referred to in Article 11, § 1, 1. to 3. and 5., with the exception of any other fundamental interest of the country as referred to in Article 11, § 1, 1. f).][3, 5]

§ *2*. Exceptionally and taking into consideration [a potential threat as referred to in section 1][5], the exceptional intelligence collection methods referred to in Article 18/2, § 2 can only be used if the ordinary and specific intelligence collection methods are considered inadequate to collect the information required to carry out the intelligence operation.

The head of service may only authorise the use of an exceptional method after the Commission has given its assent.

§ *3*. The exceptional method must be chosen on the basis of the degree of gravity of the potential [threat][4] […][5].

§ *4*. The exceptional methods can only be applied to a lawyer, a doctor or a journalist, or to the premises or means of communication that they use for business purposes, or to their home or place of residence, if the intelligence and security service has serious prior evidence that the lawyer, doctor or journalist in question is or has been personally and actively involved in the creation or development [of a serious potential threat as referred to in section 1.][5].][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 5 of the Act of 6 December 2015 (BOJ 17 December 2015), [3]supplemented under Article 6 of the Act of 29 January 2016 (BOJ 24 February 2016), [4]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [5]replaced and repealed under Article 36 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/10

§ *1*. The head of service subordinates the draft authority to the assent of the Commission, which investigates compliance with the legal provisions for the application of the exceptional intelligence collection method, and with the [principles of subsidiarity and proportionality][2] set out in Article 18/9 §§ 2 and 3, and checks the statements required under § 2.

In the absence of any legal provision to the contrary the period during which the exceptional intelligence collection method is used may not exceed two months, [counting from the time of the authorisation,][2] without prejudice to the option to extend the method in accordance with § 5.

The intelligence officer appointed to [monitor the application of the exceptional intelligence collection method][2] shall report regularly to the head of service, and he in turn shall inform the Commission about the execution of this method in accordance with the further rules and deadlines determined by the King.

The head of service shall terminate the exceptional method when the serious potential threat which justified it has passed, when the method no longer serves the purpose for which it was adopted, or when he establishes an illegitimacy. He shall notify the Commission of his decision as soon as possible.][2]

[§ 2. The head of service's draft authorisation states:

1. the nature of the exceptional method;

2. as relevant, the natural or legal persons, de facto associations or groups, items, places, events or information which are the object of the exceptional method;

3. the serious potential threat that justifies the exceptional intelligence collection method;

4. the actual circumstances that justify the exceptional method, the motivation relating to subsidiarity and proportionality, including the relationship between the provisions under 2. and 3.;

5. the period for which the exceptional intelligence collection method can be employed, counting from the time of the head of service's authorisation;

6. the name of the intelligence officer(s) responsible for monitoring the application of the exceptional method;

7. where relevant, the technical device that is used in the application of the exceptional method pursuant to Articles 18/11 or 18/12;

8. where relevant, the overlap with a criminal investigation or judicial inquiry;

9. where relevant, the criminal offenses that are strictly necessary for the successful execution of the method or to ensure the safety of the agents or third parties;

10. where relevant, the serious evidence which shows that the lawyer, the doctor or the journalist is or has been personally and actively involved in creating or developing the potential threat;

11. where relevant, the reasons that justify the extreme urgency;

12. the date of the authorisation;

13. the head of service's signature.

The statements referred to in the first paragraph are prescribed under penalty of illegitimacy.][2]

§ *3*. The Commission shall give its assent within four days after receipt of [the draft authorisation][2].

If the Commission issues a negative opinion, the exceptional intelligence collection method may not be employed by the service in question.

If the Commission does not issue an opinion within the deadline of four days [or it notifies the service involved that it cannot deliberate within that period in accordance with Article 43 § 1, paragraph 7][2], the service involved may apply to the competent Minister, who may then give authorisation to execute the intended method without further delay. The Minister shall inform the chairmen of the Commission and the Standing Committee I of his decision.

The head of service shall inform the Minister of his monitoring of the exceptional method authorised by presenting detailed reports on the progress of the method on a regular basis, as specified by the Minister in his authorisation.

The relevant Minister shall terminate the use of the exceptional method which he authorised [when the potential threat which justified it has passed][2] or when the method no longer serves the purpose for which it was adopted. He shall suspend the use of the method if he observes an illegitimacy. In that case the relevant Minister shall immediately notify the Commission, the head of service and the Standing Committee I of his reasoned decision to terminate or suspend the use of the exceptional method, as appropriate.

§ *4*. [In the event of extreme urgency and when any delay in the authorisation is liable to seriously jeopardise the interests referred to in Article 18/9, the head of service, after having received the verbal assent from the chairman of the Commission on the grounds of extreme urgency, may verbally authorise the exceptional intelligence collection method for no more than five days.

If the chairman of the Commission cannot be reached, the head of service may contact another member of the Commission.

The chairman, or the other contacted member, shall immediately inform the other members of the Commission of his verbal assent.

The intelligence officer may request the cooperation of the persons referred to in Articles 18/14, 18/15, 18/16 and 18/17 in writing. The nature of the method will be communicated to them. The head of service will be informed of this request as soon as possible.

The head of service shall confirm the verbal authorisation in writing and give notice of this to the headquarters of the Commission, in accordance with the further rules determined by the King, no later than twenty-four hours after this authorisation has been granted. This written confirmation must contain the statements referred to in § 2.

Where relevant, the confirmation must state the reasons that justify upholding the application of the method after the five-day period, without exceeding the two months referred to in § 1, paragraph 2. In that case, the confirmation serves as the draft authorisation referred to in § 1.

If the need to uphold the method after the five-day period could not be foreseen, or in exceptional cases, the head of service may authorise its extension in accordance with the procedure under paragraph 1.][2]

If the chairman issues a [verbal][2] negative opinion, the exceptional intelligence collection method may not be employed by the service in question.

If in a case of extreme urgency the chairman does not issue an opinion immediately, the service involved may apply to the competent Minister, who may then give authorisation to execute the method in question. The Minister shall inform the chairmen of the Commission and the Standing Committee I of his decision.

The head of service shall inform the Minister of his monitoring of the exceptional method authorised by presenting detailed reports on the progress of the method on a regular basis, as specified by the Minister in his authorisation.

The relevant Minister shall terminate use of the exceptional method which he authorised [when the potential threat which justified it has passed][2] or when the method no longer serves the purpose for which it was adopted. He shall suspend use of the method if he observes an illegitimacy. In that case the relevant Minister shall immediately notify the Commission, the head of service and the Standing Committee I of his reasoned decision to terminate or suspend use of the method, as appropriate.

In any case, the exceptional method will be stopped within [five days][2] of the authorisation granted by the competent Minister [, except in the extension cases referred to in paragraphs 5 and 6][2].

§ *5*. The head of service may, following the prior assent of the Commission, authorise the extension of the use of the exceptional intelligence collection method for a new period that may not exceed […][2] two months [counting from the expiry of the current method][2], notwithstanding his duty to terminate the method as soon as [the potential threat which justified it has passed,][2] when the method no longer serves the purpose for which it was adopted, [or when][2] he observes an illegitimacy. In that case, the head of the service involved shall notify the Commission of his reasoned decision to terminate […][2] the method.

A second or subsequent extension of the exceptional intelligence collection method is only possible if there are special circumstances which necessitate the renewal of the use of this method. These special reasons shall be specified in the decision. If these special circumstances are not present, then the method is to be terminated.

The conditions defined in paragraphs 1 to 3 are applicable to the methods set out in this paragraph for the renewal of the exceptional intelligence collection method.

§ *6*. The members of the Commission may at any time carry out checks on the legitimacy of the exceptional intelligence collection methods, including compliance with the principles of subsidiarity and proportionality referred to in Article 18/9, §§ 2 and 3.

To this end they can enter the places where the data collected using the exceptional methods are received and stored, appropriate any useful documents and hear the members of the service.

The Commission shall terminate the exceptional intelligence collection method whenever it establishes that [the potential threat which justified it has passed][2] or whenever the exceptional method no longer serves the purpose for which it was adopted, or shall suspend the exceptional method in the case of illegitimacy.

Data acquired in circumstances which do not comply with the legal provisions in force shall be stored under the supervision of the Commission in accordance with the rules and deadlines

decided by the King, on receipt of an opinion of the Privacy Commission. The Commission forbids the intelligence and security services from using this data.

§ *7*. The Commission shall on its own initiative notify the Standing Committee I [of the draft authorisation referred to in § 2][2] of the intelligence and security service involved, of the assent referred to in § 3[, of the written confirmation of the verbal authorisation referred to in § 4][2], of any renewal of the exceptional intelligence collection method referred to in § 5, and of its decision, referred to in § 6, to terminate or where appropriate suspend the method and to forbid use of the data thus collected.][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), and [2]replaced, introduced and repealed under Article 37 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/11

§ *1*. In the interest of executing their assignments, the intelligence and security services may observe the following with or without the help of technical resources:

1. places not accessible to the public and hidden from view;

2. persons and items located there;][1]

3. events that occur there.

§ 2. In the interest of executing their assignments, the intelligence and security services may at any time, without the knowledge or consent of the owner or his rightsholder, enter places that are not accessible to the public, whether or not hidden from view, in order to:

1. carry out surveillance;

2. install a technical device there, operate it or remove it;

3. open a locked object to place a technical device in it;

4. remove an object in order to install a technical device in it, operate that object and return it.

The technical device or the object that has been removed must be returned or replaced as soon as possible after the surveillance, unless this would hinder the proper execution of the assignment.][1, 2]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 38 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/12

[In the interest of executing their assignments, the intelligence and security services may do the following at any time, without the knowledge or consent of the owner or his rightsholder:

1. search places that are not accessible to the public, with or without the help of technical resources;

2. search the content of locked or unlocked objects that are located there;

3. remove the locked or unlocked objects for a strictly limited period, if they cannot be examined on site for technical or safety reasons;

4. enter these places in order to replace the objects removed.

These objects must be replaced as soon as possible, unless this would hinder the execution of the assignment.][1, 2]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 39 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/13

[For the purpose of executing their assignments, the intelligence and security services may use a legal person, as referred to in Article 13/3, § 1, for collecting intelligence on events, items, groups and natural or legal persons that are of importance for the execution of their assignments.][2]

[...][2]

[The method is permitted for as long as is necessary for the purpose for which it is adopted.][2]

The intelligence and security service involved shall report to the Commission every two months on developments in the operation which required [...][2] calling upon a legal person. This report shall emphasise the elements which justify either the continuance or the termination of the exceptional method. […][2]][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced and repealed under Article 40 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/14

§ *1*. For the purpose of executing their assignments, the intelligence and security services may [...][2] [open][2] post [and inspect the contents][2], whether or not entrusted to a postal operator.

The postal operator referred to in the first paragraph shall be required to hand over the post to which the authorisation relates against receipt to an [...][2] agent of the service, on production of his identity card and a written demand from the head of service. This demand shall state, as appropriate, the nature of the assent of the Commission, the nature of the assent of the chairman of the Commission or the nature of the authorisation of the Minister in question.

§ *2*. The services shall ensure that, after inspection, a postal item handed over by a postal operator shall be returned to the postal operator for final delivery immediately.

§ *3*. A postal operator who refuses to cooperate under the terms of §§ 1 and 2 shall be subject to a fine of between twenty-six euro and [twenty thousand euro][2].

§ *4*. The State shall be liable under civil law to the postal operator for damage caused to post entrusted to it.][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]repealed and replaced under Article 41 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/15

§ *1*. For the successful execution of their assignments, the intelligence and security services may [requisition the following information][2]:

1. the list of bank accounts, safe-deposit boxes or financial instruments as referred to in Article 2, 1. of the Act of 2 August 2002 on supervision of the financial sector and financial services, of which the person targeted is the holder, nominee or beneficial owner, and, as relevant, all information concerning these;

2. the banking transactions which were carried out in a given period on one or more of these bank accounts or financial instruments, including the details of each originating or destination account;

3. data relating to the holders or nominees who have or had access to the safe-deposit boxes over a given period.

§ *2.* The bank or financial institution shall be required to provide the requested information immediately to an […][2] agent of the service, on production of his identity card and a written demand from the head of service. This demand shall state, as appropriate, the nature of the assent of the Commission, the nature of the assent of the chairman of the Commission or the nature of the authorisation of the Minister in question.

A bank or financial institution which refuses to cooperate under the terms of the present Article shall be subject to a fine of between twenty-six euro and [twenty thousand euro][2].][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]repealed and replaced under Article 42 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/16

§ *1.* Except as regards the computer systems of the judicial authorities and the administrative tribunals, the intelligence and security services may, for the successful execution of their assignments, […][2] whether or not making use of technical resources, false signals, false keys or false capacities:

1. gain access to a computer system;

2. neutralise any security it may have;

3. operate technical procedures on it in order to decipher and decode the data stored, processed or transmitted by the computer system;

4. copy the […][2] data stored, processed or transmitted by the computer system in any manner.

The method referred to in the first paragraph may only be employed on the computer systems of the governmental authorities with the prior consent of the relevant government authority.

The intrusion by the intelligence and security services into computer systems as referred to in the first paragraph may only have as its purpose the collection of relevant intelligence stored, processed or transmitted by that system, without causing any irreversible deletion or alteration of that data.

The intelligence and security services shall ensure that in the event of installation of technical resources as referred to in the first paragraph, 3., third parties will not be able to gain unauthorised access to these systems via the intervention of the intelligence and security services.

[*§ 2.* The intelligence and security services may at any time, without the knowledge or consent of the owner or his rightsholder, enter places that are not accessible to the public and gain access to locked or unlocked objects, in order to:

1. penetrate the computer systems;

2. install a technical device there, operate it or remove it;

3. remove the computer systems and subsequently return them.

The technical device or computer systems must be returned or replaced as soon as possible after being penetrated, unless this would hinder the proper execution of the assignment.][2]

§ *3.* The head of service may, by written decision, require persons whom he suspects of having particular knowledge of the computer system referred to in § 1, or of the services which enable the data that is stored, processed or transmitted by the computer system to be secured or encrypted, to provide information on the operation of that system and on how to gain access to the content of the computer system in an intelligible form [and to cooperate in the penetration of a computer system][2]. This demand shall state, as appropriate, the nature of the

assent of the Commission, the nature of the assent of the chairman of the Commission or the nature of the authorisation of the Minister in question.

§ *4*. Any person who refuses to provide the technical assistance as referred to in § 3 shall be subject to a fine of between twenty-six euro and [twenty thousand euro][2].

§ *5*. Should intrusion into a computer system result in that system becoming completely or partly inoperable, the State shall only be liable under civil law for the damage thus caused if this intrusion has no connection with the collection of intelligence as regards a serious threat to the physical integrity of one or more persons, including the terrorist offences referred to in Article 137 of the Penal Code.][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]repealed, replaced and introduced under Article 43 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/17

§ *1*. For the purpose of performing their assignments, the intelligence and security services may […][3] [intercept, listen to and record][3] communications.

[§ 2. For this purpose, the intelligence and security services may at any time, without the knowledge or consent of the owner or his rightsholder, enter places accessible or inaccessible to the public, in order to:

1. install a technical device there, operate it or remove it;

2. open a locked object to place a technical device in it;

3. remove the object in order to install a technical device in it, operate that object and subsequently return it.

The technical device or the removed object must be returned or replaced as soon as possible after the interception, unless this would hinder the proper execution of the assignment.][3]

§ *3*. If intervention is required on an electronic communications network, the head of service will send a written request to the operator of the network or the provider of an electronic communications service, who will then be required to provide technical cooperation. This demand shall state, as appropriate, the nature of the assent of the Commission, the nature of the assent of the chairman of the Commission or the nature of the authorisation of the Minister in question.

Any person who refuses to provide the technical assistance as referred to in the first paragraph shall be subject to a fine of between twenty-six euro and [twenty thousand euro][3]. Further rules and deadlines for this technical cooperation shall be defined by the King, on a motion of the Minister of Justice, the Minister of Defence and the Minister competent for electronic communications.

§ *4*. A recording is kept of the communications collected on the basis of the exceptional method referred to in § 1. The object of the exceptional method and the days and hours at which it was employed shall be stated at the beginning and end of each recording relating to it.

Only those parts of the recording of communications considered relevant for the [General Intelligence and Security Service][2] by the head of service or, as appropriate, on his instruction by the Director of Operations or the person he has appointed for State Security, or by the officer or civil servant holding at least the grade of commissioner, may be transcribed.

Any note taken in the course of the implementation of the exceptional method by the persons appointed for the purpose which was not included in a report shall be destroyed by the persons referred to in the second paragraph or by the person appointed by them. This destruction shall be noted in the special register provided for in § 6.

§ *5*. The recordings and any transcription of a communication deemed relevant or any translation shall be stored in a secure location indicated by the head of service in accordance with the requirements of the Act of 11 December 1998 on classification and security clearances, certificates and advice.

§ *6*. A regularly updated special register shall contain an overview of each of the measures referred to in §§ 1 and 2.

The overview shall give the date and time at which the measure started and at which it ended.

[§ 7. Communication recordings are destroyed in accordance with the further rules to be determined by the King, under the supervision of the Commission and an agent designated by the head of service for this purpose, within a period of five years that commences on the date of the recording. The head of service may, with the prior written consent of the Commission, decide to extend the storage period if the recording is still needed for the purpose of an intelligence investigation or judicial procedure. The total storage period may not exceed ten years unless a recording is still needed for the purpose of a judicial procedure. The destruction shall be recorded in the special register referred to in section 6.

The transcriptions of communications that are deemed relevant and any translations are stored and destroyed in accordance with Article 21.][3]][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 3 of the Act and [3]repealed and replaced under Article 44 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Subsection 3. - Common provision for some intelligence collection methods]

Heading introduced under Article 45 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 18/18

The King shall set the rates for the cooperation of natural and legal persons in [the methods referred to in Article 16/2 and subsection 2][2], taking account of the actual cost of this cooperation.][1]

[1]Introduced under Article 14 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]replaced under Article 46 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 5] - Communication of data

Heading renumbered under Article 47 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 19

The intelligence and security services shall communicate the intelligence referred to in Article 13, second paragraph only to the relevant Ministers and the relevant judicial and administrative authorities, to the police services and to any competent bodies and persons in accordance with the objectives of their assignments and to bodies and persons who are the subject of a [threat] as referred to in Articles 7 and 11.

With due respect for individual privacy and to the extent it is required for public information or the public interest, the Administrator-General of State Security and the head of the [General Intelligence and Security Service], or the person appointed by each of them, may communicate information to the press.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 19/1

When the use of specific or exceptional methods brings to light serious evidence concerning the commission of a crime or offence or gives rise to reasonable suspicion concerning criminal offences yet to be committed or already committed but not yet brought to light, the relevant services shall immediately bring this to the attention of the Commission with a view to the application of Article 29 of the Penal Code. This Commission shall investigate the collected data regardless of the medium on which they were recorded.

If the Commission finds serious evidence that may lead to the commission of a crime or offence or has reasonable suspicion concerning criminal offences yet to be committed or already committed but not yet brought to light, the chairman shall draw up an unclassified report. This report must be sent immediately to the Public Prosecutor or to the Federal Prosecutor, after the head of service has been heard on the conditions for this transmission [and the content of the report][2].

[This report must state the serious evidence that could be used in court.][2]

This report may not serve as the sole or primary grounds for trying a person. The elements included in this report must predominantly be supported by other evidence.

The Public Prosecutor or the Federal Prosecutor shall inform the chairman of the Commission of the actions taken after the transmission of the report. The chairman of the Commission shall in turn inform the head of the service involved.][1]

[1]Introduced under Article 15 of the Act of 4 February 2010 (BOJ 10 March 2010) and [2]added and replaced under Article 48 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 6] - Cooperation between the services

Heading renumbered under Article 49 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 20

§ 1. The intelligence and security services, the police services and the administrative and judicial authorities must ensure that their mutual cooperation progresses as efficiently as possible. The intelligence and security services shall likewise ensure cooperation with foreign intelligence and security services.

§ 2. When they are approached for this purpose the intelligence and security services may, within the limits set out in a protocol approved by the Ministers involved, cooperate and in particular provide technical assistance to the judicial authorities and public administrations.

§ 3. [The National Security Council][1] determines the conditions under which intelligence can be shared, referred to in Article 19, first paragraph, and the conditions for the cooperation, referred to in § 1 of this Article.

[*§ 4.* For the assignments described in Article 7, 3./1 and Article 11, § 1, 5., [State Security][3] and the [General Intelligence and Security Service][3] shall enter into a cooperation agreement on the basis of guidelines obtained from the National Security Council][2]

[1]Replaced under Article 7 of the Act of 6 December 2015 (BOJ 17 December 2015), [2]supplemented under Article 7 of the Act of 29 January 2016 (BOJ 24 February 2016) and [3]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 7] - Storage and destruction of data

Renumbered under Article 50 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 21

Personal data processed in the context of the application of the present Act may be stored for a period which may not be longer than that necessary for the purposes for which it is stored, with the exception of data of a historical nature as recognised by the State Archives.

It is only destroyed after a fixed time after it was last processed.

The King, on receipt of an opinion of the Privacy Commission, sets the time limit during which personal data as referred to in the previous paragraph may be stored after it is last processed.

Without prejudice to the legal provisions concerning the State Archives, the King shall determine, on receipt of an opinion of the Privacy Commission, the procedure for its destruction.

[Article 21/1

§ *1*. The intelligence and security services are exempt from transferring their archive documents that are less than fifty years old, on condition that:

1. the long-term storage, authenticity, integrity, classification, accessibility and legibility of these archive documents are guaranteed in accordance with the conditions determined by the King;

2. the public can consult these archive documents under the same conditions as in the State Archive.

The storage of the archive documents is subject to the supervision of the general state archivist or his authorised representatives.

§ *2*. After the period referred to in § 1, the intelligence and security service involved shall evaluate whether it is possible to review the level of protection or declassify classified archive documents.

§ *3*. The intelligence and security services shall transfer their archive documents that are more than fifty years old to the State Archive, on condition that:

1. the State Archive stores and uses the classified archive documents in accordance with the Act of 11 December 1998 on classification and security clearances, certificates and advice;

2. foreign intelligence and security services have given their express consent for the State Archive to store documents that have originated from them;

3. the general state archivist or his authorised representatives find, after consulting with the archive manager of the intelligence and security service involved, that the importance of a unified collection does not preclude a transfer.

On a motion of the Minister of Justice, the Minister of Defence and the Minister of Science Policy, the King shall determine the further rules for archive management and the use of transferred classified archive documents.

§ *4*. Archive documents may be destroyed only after the written consent of the general state archivist or his authorised representatives has been given.]

Introduced under Article 51 of the Act of 30 March 2017 (BOJ 28 April 2017).

[…]

Heading repealed under Article 23 of the Act of 21 April 2016 (BOJ 29 April 2016).

[CHAPTER III/1
PROTECTION OF THE PERSONNEL, INFRASTRUCTURE AND ASSETS OF THE INTELLIGENCE AND SECURITY SERVICES]

Heading introduced under Article 52 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 1. General provision]

Heading introduced under Article 53 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 22

Within each intelligence and security service, an intervention team can be established with the assignment of protecting the personnel, infrastructure and assets of the service involved.

The agents tasked with this assignment are appointed respectively by the Minister of Justice, on a motion of the head of State Security, and by the Minister of Defence, on a motion of the head of the General Intelligence and Security Service.

The intervention team members are the only agents who are authorised to execute the assignment to protect the personnel, infrastructure and assets of their service, notwithstanding their other duties. They receive training for this purpose.

The intervention team members report on their interventions to the head of the service involved.

They may not make use of the powers assigned to them by this chapter in the execution of their other assignments.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 54 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 2. Executing the assignment to protect the personnel, infrastructure and assets of the intelligence and security services]

Heading introduced under Article 55 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 23

Intervention team members may always enter empty buildings, outbuildings and vehicles.

They may enter and search occupied buildings, outbuildings and vehicles, day and night, only if there is a serious and imminent danger to the life or physical integrity of a member of staff of the intelligence and security service involved, insofar as this member of staff is within a place that is not accessible to the public and the danger cannot be averted in any other way.

They may search empty buildings, outbuildings and vehicles only in the cases referred to in paragraph 2][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 56 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 24

Intervention team members may perform a security search, in order to ascertain whether a person is carrying a weapon or any object that presents a danger to their lives or physical integrity or those of the members of staff of the intelligence and security service involved, or to the integrity of the infrastructure and assets of the service being protected, in the following cases:

1. when the intervention team member, on the basis of the behaviour of this person, material evidence or the circumstances, has reasonable grounds to believe that the person who is subject to an identity check, in the cases and under the conditions set out in Article 28, is carrying a weapon or dangerous object;

2. when a person is provisionally detained in accordance with Articles 27 and 28;

3. when the person has access to places where members of staff of the intelligence and security service involved are under threat.

The security inspection takes the form of patting down the body and the clothing of the person searched and a check of any luggage. It may not take any longer than is necessary and the person may not be held up for longer than one hour for this purpose.

In the case referred to under 3., the search is carried out on the orders and under the responsibility of the intervention team member who is responsible for the assignment; it is carried out by an intervention team member of the same sex as the person being searched.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 57 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 25

Intervention team members may proceed to searching a vehicle or any other means of transport, both in traffic and parked on a public road or in publicly accessible places, if the behaviour of the driver or the passengers, material evidence or circumstances of time or place give reasonable grounds to suspect that the vehicle or means of transport is being used, or could be used, to seriously endanger the life or physical integrity of a member of staff of the intelligence and security service involved or the integrity of the infrastructure and assets of the service being protected.

An inspection of a vehicle may never take longer than the time required by the circumstances justifying it. The vehicle may never be held up for a search for longer than one hour.

An inspection of a vehicle which is equipped permanently as a home and which at the moment of the inspection is actually used as a home, is treated in the same manner as a house search.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 58 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 26

Objects and animals that pose a danger to the life or physical integrity of a member of staff of the intelligence and security service involved or to the integrity of the infrastructure and assets

of the intelligence and security service involved, in a publicly accessible place, may be confiscated from the owner, possessor or holder by an intervention team member where required by the protection assignment. This administrative seizure is conducted in accordance with the guidelines and under the responsibility of the intervention team member who is responsible for the assignment.

The items seized are made available to a police officer so that they can be handled in accordance with Article 30 of the Act on the police function.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 59 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 27

In case of absolute necessity, intervention team members can detain a person for whom, on the basis of his behaviour, material evidence or circumstances, there are reasonable grounds to suspect that he is making preparations to commit an act or is committing an act that seriously endangers the life or physical integrity of an agent or third party or the integrity of the infrastructure and assets of the intelligence and security service under protection, with the aim of preventing him from committing such an act or to stop such an act.

In that case, the person is detained only for the time needed to turn him over to a police officer.

Detention by the intervention team member may not be for a longer period than required by the circumstances which justify it and may in no case exceed one hour. This period starts from when the person involved is no longer free to come and go as a consequence of the actions of an intervention team member.

The King shall lay down further rules for registering the detention and storing the related data.

If the detention is followed by administrative arrest in accordance with Articles 31 to 33 of the Act on the police function, the maximum duration of the administrative arrest is reduced by a corresponding period.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 60 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 28

§ *1.* Intervention team members may check the identity of any person if, on the basis of his behaviour, material evidence or circumstances of time or place, they have reasonable grounds to suspect that person is preparing to harm the life or physical integrity of a member of staff of the intelligence and security service involved or the integrity of the buildings of that service.

§ *2.* Identity documents that are handed over to the intervention team member may be retained only for the time required for the verification of identity and must then be returned immediately to the person concerned.

§ *3.* If the person referred to in the previous sections refuses to or is incapable of providing evidence of his identity, or if his identity is in doubt, he may be detained in order to be turned over to a police officer.

Detention by the intervention team member may not be for a longer period than required by the circumstances which justify it and may in no case exceed one hour. This period starts from when the person involved is no longer free to come and go as a consequence of the actions of an intervention team member.

If the detention is followed by administrative arrest in accordance with Articles 34, § 4 of the Act on the police function, the maximum duration of the administrative arrest is reduced by a corresponding period.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 61 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 29

Except in an emergency, intervention team members may not expose detained persons to public curiosity.

They may not subject these people or allow them to be subjected without their consent to questions from journalists or third parties outside the scope of the case, nor photograph them or allow them to be photographed except when photographs are taken for their identification.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 62 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 30

Intervention team members may, taking account of the associated risks, use force to achieve a legitimate aim that cannot be achieved in any other way.

Any use of force must be reasonable and proportionate to the objective.

A warning must be given before any use of force, unless this would make that use of force ineffective.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 63 of the Act of 30 March 2017 (BOJ 28 April 2017)

[Article 31

Without prejudice to Article 30 of this Act, Articles 70, 416 and 417 of the Penal Code and the applicable rules of international law, intervention team members may use firearms against people only in the following cases:

1. against armed persons or in the direction of vehicles carrying armed persons, in the event of a crime or on catching someone in the act of committing an offence in the sense of Article 41 of the Code of Criminal Procedure, where that crime or offence was committed with force, if it can reasonably be assumed that these persons are in possession of a firearm ready for use, and that they will use this weapon against people;

2. if, in case of absolute necessity, the intervention team members are unable to defend the persons, infrastructure or assets entrusted to their protection in any other manner.

The use of weapons as defined under 1. and 2. may occur only in accordance with the guidelines and following a warning in a loud voice or by any other means available, unless this would make such use ineffective.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 64 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 32

Except when circumstances do not permit it or if it would make the assignment ineffective, intervention team members, or at least one of them, shall, when taking action against a person or calling at a person's home, make their capacity clear by showing the legitimation card they hold.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 65 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 33

Should he be in danger during the execution of his assignment or if an agent of the intelligence and security service involved is in danger, any intervention team member may call upon persons present to provide help or assistance.

In the event of absolute necessity he may likewise call on any other capable person for help or assistance.

The help or assistance called for may not put the person who provides it into danger.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 66 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 34

The weapons that form part of the required equipment are determined in accordance with the Act of 8 June 2006 governing economic and individual activities with weapons.

Where relevant, the King shall determine the additional equipment that is necessary for the performance of intervention team members' duties.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 67 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Section 3. Civil liability and legal assistance relating to intervention team members in the performance of their duties][1, 2]

[1]Repealed under Article 23 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]introduced under Article 68 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 35

The system of civil liability and legal assistance, as set out in Articles 91 to 98 of the Act of 20 May 1994 on the legal status of Defence personnel, in the Act of 10 February 2003 on the liability of and for personnel of public legal persons, and in the Royal Decree of 16 March 2006 on legal assistance to personnel of certain public services and the indemnification of the property damage they suffer, applies to intervention team members who are entrusted with assignments to protect the agents, infrastructure and assets of the intelligence and security service involved.][1, 2]

[1]Repealed under Article 22 of the Act of 21 April 2016 (BOJ 29 April 2016) and [2]restored under Article 69 of the Act of 30 March 2017 (BOJ 28 April 2017).

CHAPTER IV
CONFIDENTIALITY

Article 36

§ 1. Without prejudice to Article 19 any agent and any person who, in any capacity whatsoever, provides assistance in the application of this Act, has an obligation of confidentiality concerning secrets entrusted to him in the course of his assignment or his cooperation.

§ 2. The obligation of confidentiality shall also apply after the agent has been discharged from his position or the person who cooperates with the services has ceased to do so.

Article 37

Agents who call on the cooperation of a person who does not belong to the services of State Security or the [General Intelligence and Security Service] have the obligation to inform that person expressly of their obligation of confidentiality.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 38

§ 1. Judicial house searches and seizures carried out in places where the members of the intelligence and security services are exercising their functions shall be conducted in the presence of [the head of the service involved]. [The head of service] shall immediately notify the competent Minister of the judicial house searches and seizures conducted.

§ 2. If [the head of service] is of the opinion that the seizure of classified information and items would constitute a threat to the execution of the assignments referred to in Articles 7 [...] and 11, §§ 1 and 2, or would risk exposing a natural person to danger, he shall immediately warn the chairman of the Standing Committee I and the competent Minister. These seized classified items shall be put in a sealed envelope, signed by [the head of service] and stored in a safe place by the investigating magistrate.

At the same time [the head of service] may, after notifying the competent Minister, apply to the indictment division for lifting of the seizure. The application for lifting of the seizure shall have a suspensive effect. The case shall be brought before the indictment division by lodging a declaration with the registry of the court of first instance. The indictment division shall rule within fifteen days of the declaration being lodged. [The head of service] and the investigating magistrate shall be heard.

In the context of this procedure the content of the seized classified items may only be revealed to the magistrates of the court and of the Public Prosecutor's Office sitting in the indictment division, the investigating magistrate and [the head of service].

Should the indictment division rule to lift the seizure on the grounds of a threat to the execution of the assignments referred to in Articles 7 [...] and 11, §§ 1 and 2, or on the grounds of the risk of exposing a natural person to danger, the classified items shall be returned to [the head of service] in a sealed envelope.

Should the indictment division conclude that the documents may be seized, the prosecutor-general shall nonetheless return the seized classified items to [the head of service] after the judicial procedure has run its course.

§ 3. If [the head of service] does not apply to the indictment division for lifting of the seizure under § 2, second paragraph within ten days, the requirement for storage in a sealed envelope, referred to in § 2, first paragraph, shall be lifted.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 39

§ 1. House searches and seizures in the places referred to in Article 38 which are carried out in the context of a parliamentary investigation shall be conducted in the presence of [the head of service].

§ 2. If [the head of service] is of the opinion that the seizure of classified information and items would constitute a threat to the execution of the assignments referred to in Articles 7 [...] and 11, §§ 1 and 2, or would risk exposing a natural person to danger, he shall immediately notify the chairman of the Standing Committee I. The seized classified items shall be placed in a sealed envelope, signed by [the head of service]. The magistrate leading the investigation shall immediately hand over the sealed envelope to the chairman of the Standing Committee I, who shall keep it in a safe place.

At the same time [the head of service] may apply for lifting of the seizure to, as appropriate, the chairman of the indictment division or the chairman of the inquiry committee which shall rule. [The head of service] and the chairman of the Standing Committee I shall be heard.

The application for lifting of the seizure shall have a suspensive effect.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 40

§ 1. In the context of house searches and seizures carried out in places other than those referred to in Article 38, if classified information or items originating from the intelligence and security services are discovered, [the head of service] shall immediately be notified by the investigating magistrate or the authorised officer of the criminal police.

§ 2. If [the head of service] is of the opinion that the seizure of classified information or items would constitute a threat to the execution of the assignments referred to in Articles 7 [...] and 11, §§ 1 and 2, or would risk exposing a natural person to danger, the case shall be handled as in Articles 38 and 39.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 41

When the seizure of classified information or items is conducted in accordance with Article 51 of the Act of 18 July 1991 governing review of the police and intelligence services, and [the head of service] is of the opinion that the seizure would constitute a threat to the execution of the assignments referred to in Articles 7 [...] and 11, §§ 1 and 2, the case shall be referred to the chairman of the Standing Committee I who shall rule.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

[…][1,2,3]

[1]Replaced under Article 3 of the Act of 3 April 2003 (BOJ 12 May 2003), [2] amended under Article 34 of the Act of 5 May 2014 (BOJ 8 July 2014) and [3]repealed under Article 70 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 43

[Without prejudice to Article 458 of the Penal Code and Articles 48 and 51 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment, the following penalties shall apply:

1. imprisonment for between eight days and six months with a fine of between one hundred euro and five hundred euro for the agent or the person referred to in Article 36 who reveals secrets in breach of this Article;

2. imprisonment for between six months and three years with a fine of between five hundred euro and thirty thousand euro or just one of the two penalties for the agent or the person referred to in Article 36 who reveals the identity of a person who has requested anonymity;

3. imprisonment for between six months and three years with a fine of between five hundred euro and thirty thousand euro or just one of the two penalties for anyone who, with malicious intent, via any means of expression, reveals the identity of agents of the intelligence and security services whose assignments, for safety reasons, require observance of the greatest discretion;

Replaced under Article 16 of the Act of 4 February 2010 (BOJ 10 March 2010).

[CHAPTER IV/1
CONTROL OF THE SPECIFIC AND EXCEPTIONAL METHODS FOR THE COLLECTION OF INTELLIGENCE BY THE INTELLIGENCE AND SECURITY SERVICES]

Heading introduced under Article 17 of the Act of 4 February 2010 (BOJ 10 March 2010)

[Article 43/1

§ *1.* An administrative commission shall be established which is charged with the control of the specific and exceptional methods for the collection of intelligence by the intelligence and security services referred to in Article 18/2.

The [Chamber of Representatives][2] shall annually determine, on a motion of the Commission, its budget, which is included in the budget of the appropriations, so that the Commission may have the human and material resources required to operate properly.

The Commission shall operate completely independently in carrying out its supervisory duties. It shall also be responsible for drawing up its own rules of procedure.

The Commission shall comprise three effective members. A substitute shall be appointed for each of the effective members.

The King shall appoint the effective members of the Commission and their substitutes on a motion of the Minister of Justice and the Minister of Defence in a decree deliberated in the Council of Ministers.

The effective members and their substitutes shall have the capacity of magistrate. One of the effective members shall hold the capacity of a member of the Public Prosecutor's Office and both others shall hold the capacity of judge, of whom one shall hold that of examining magistrate. The substitute members shall have the same capacity as the effective member that they replace.

[The Commission shall decide by a majority of the three effective members present or their substitutes or, if one of the effective members and his substitute are unable to attend, by the unanimous decision of the two effective members present or their substitutes.][3]

The Commission shall be chaired by the magistrate holding the capacity of examining magistrate.

Apart from the chairman, who must have adequate knowledge of French and Dutch, the two remaining effective members shall each be on a different language register.

§ *2*. At the moment of their appointment the effective and substitute members of the Commission shall meet the following conditions:

1. have attained the age of 40 years;

2. have at least five years' relevant experience in one of the areas referred to in Article 18/9, § 1;

3. hold top-secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances, certificates and advice.

4. during the five years prior to their appointment, not have been a member of the Standing Police Monitoring Committee or the Standing Intelligence Agencies Review Committee, nor been a member of a police force or an intelligence and security service.

These magistrates shall be appointed for a term of five years. Their term of office may be renewed twice.

[Apart from the deputy chairman, who must have adequate knowledge of Dutch and French, the substitute members][3] must belong to the same language register as the effective members they replace.

§ *3*. If one of the members of the Commission is unable to attend or is absent for more than three months, or if his position falls vacant, he shall be permanently replaced by his substitute.

If a member of the Commission ceases to exercise his duties, no longer holds the security clearance referred to in § 2, first paragraph, 3., or is appointed to another position, as a consequence of which he loses the capacity referred to in § 1, his term of office shall be completed by his substitute.

If the position of a substitute falls vacant or if a substitute completes the period in office of an effective member of the Commission under the application of the second paragraph, the King shall, on a motion of the Minister of Justice and the Minister of Defence, make a new appointment in a decree deliberated in the Council of Ministers.

In the event of serious shortcomings, the King may, on a motion of the Minister of Justice and the Minister of Defence, in a decree deliberated in the Council of Ministers, remove an effective member or a substitute from office.

§ *4*. The effective members shall fulfil their duties with the Commission on a full-time basis. During their term of office, effective members and their substitutes shall operate completely independently from their service of origin or from their hierarchical superior.

Following the appointment of an effective member, the jurisdictional body to which that magistrate belongs may proceed with his replacement by means of a supernumerary appointment with respect to the establishment plan of that jurisdictional body.

Effective members shall receive the salary set for federal magistrates, in accordance with Article 355*bis* of the Judicial Code.

If a substitute is called upon to replace an effective member for at least one month, for each full month he shall receive, in addition to his salary, the difference between his salary and the salary of an effective member, as specified in the third paragraph.

If a substitute is called on to replace an effective member, he shall receive an allowance for each day on which he replaces that effective member. The amount of this allowance shall be

1/20 of the difference between his own monthly salary and the monthly salary which he would receive if he was serving as an effective member.

§ 5. The Commission shall be supported by a secretariat consisting of staff members seconded from the intelligence and security services in accordance with further rules to be determined by the King. The King shall also determine the status of these members, without prejudice to their original administrative status and salary grade.][1]

[1]Introduced under Article 17 of the Act of 4 February 2010 (BOJ 10 March 2010), [2]replaced under Article 16 of the Act of 6 January 2014 (BOJ 31 January 2014) and [3]replaced under Article 71 of the Act of 30 March 2017 (BOJ 28 April 2017).

[CHAPTER IV/2
A POSTERIORI CONTROL OF THE SPECIFIC AND EXCEPTIONAL METHODS FOR THE COLLECTION OF INTELLIGENCE BY THE INTELLIGENCE AND SECURITY SERVICES

Article 43/2

Without prejudice to the competences defined in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment and [in Article 44/4] of the Act of 30 November 1998 on the intelligence and security services, the Standing Committee I is also called on to conduct a posteriori control of the specific and exceptional intelligence collection methods used by the intelligence and security services as referred to in Article 18/2.

The Standing Committee I shall rule on the legitimacy of decisions made regarding these methods, as well as on compliance with the principles of proportionality and subsidiarity, set out in Articles 18/3, § 1, first paragraph, and 18/9, §§ 2 and 3.

Replaced under Article 72 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 43/3

[…][2]

The competent authority shall immediately notify the Standing Committee I of all [decisions, authorisations, opinions, consents and confirmations][2] concerning specific and exceptional intelligence collection methods, in accordance with the further rules to be determined by the King.

[1]Replaced under Article 15 of the Act of 29 May 2016 (BOJ 18 July 2016) and [2]repealed and replaced under Article 73 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 43/4

The Standing Committee I shall operate:

- either on its own initiative;

- or at the request of the Privacy Commission, in accordance with further rules to be defined by the King, in a decree deliberated in the Council of Ministers, following the opinions of that Commission and of the Standing Committee I;

- or as the result of a complaint, which must be submitted in writing on pain of invalidity, stating the grievance, from anyone who can show a personal and legitimate interest, unless the complaint is clearly unfounded;

- on any occasions where the Commission has suspended use of a specific or exceptional method on the grounds of illegitimacy or forbidden the use of intelligence on the grounds of the unlawfulness of a specific or exceptional method;

- whenever the competent Minister has taken a decision on the basis of Article 18/10, § 3.

The Standing Committee I shall rule within one month following the day on which the case was referred to it in accordance with the first paragraph.

A decision by the Standing Committee I not to act on a complaint shall be justified and the complainant shall be notified.

Unless the Standing Committee I rules otherwise, its control shall not have a suspensive effect.

Article 43/5

§ *1.* The control of the exceptional intelligence collection methods is conducted inter alia on the basis of the documents provided by the Commission in accordance with Article 18/10, § 7, and of the special register referred to in Article 18/17, § 6, which is kept continuously available to the Standing Committee I, and on the basis of any other relevant document provided by the Commission or which the Standing Committee I requests submission to.

The control of the specific intelligence collection methods is conducted [...][3] on the basis [...][3] of any [...][3] relevant document provided by the Commission or which the Standing Committee I requests submission to.

The Standing Committee I shall have access to the complete dossier compiled by the intelligence and security service involved, as well as to that of the Commission, and may require the intelligence and security service involved and the Commission to provide any additional information which it deems useful for the review to which it is authorised. The intelligence and security service involved and the Commission are required to act on this request immediately.

§ *2.* The Standing Committee I may entrust investigation assignments to the Investigation Service of the Standing Committee I. In this context this service may employ all the powers granted to it under the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

§ *3.* The complainant and his lawyer may consult the dossier at the registry of the Standing Committee I, for a period of five working days, on the days and times notified by the Committee. This dossier shall contain all information and intelligence relevant to this case, except for those which would breach the protection of sources, the protection of the privacy of third parties, the classification rules set out in the Act of 11 December 1998 on classification and security clearances, certificates and advice, or which would prevent the execution of the assignments of the intelligence and security services referred to in Articles 7 [...][2] and 11.

The intelligence and security service involved shall be given the opportunity to voice its opinion in advance on the information included in the dossier provided for consultation.

[Except if this could harm the assignments of the intelligence and security service involved,] [3]the dossier that is accessible to the complainant and his lawyer must at least include the following:

1. the legal basis justifying use of the specific or exceptional intelligence collection method;
2. the nature of the threat and its degree of gravity which justified use of the specific or exceptional intelligence collection method;

3. the type of personal data collected in the course of the use of the specific or exceptional method to the extent that this personal data only relates to the complainant.

§ *4.* The Standing Committee I can hear the members of the Commission, as well as the head of service of the service involved and the members of the intelligence and security services who used the specific or exceptional intelligence collection methods. They shall be heard in the absence of the complainant or his lawyer.

The members of [the intelligence and security services][3] are required to disclose the secrets that they know to the Standing Committee I. If this secret information is related to an ongoing criminal investigation or judicial inquiry, the Standing Committee I shall first consult the competent magistrate.

If the member of the intelligence and security service considers it necessary not to reveal a secret which he holds because its disclosure would prejudice the protection of sources, the protection of the privacy of third parties or the execution of the assignments of the intelligence and security services as referred to in Articles 7 […][2] and 11, the matter shall be submitted to the chairman of the Standing Committee I who shall rule after hearing the head of service.

The complainant and his lawyer may be heard by the Standing Committee I at their request.

[1]Replaced under Article 16 of the Act of 29 May 2016 (BOJ 18 July 2016), [2]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [3]repealed and replaced under Article 74 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 43/6

§ *1.* When the Standing Committee I finds that decisions concerning specific or exceptional intelligence collection methods were illegitimate, it shall order the use of the method to cease if it is still in progress or if it was suspended by the Commission, and shall order that the intelligence acquired by this method cannot be used and is to be destroyed, in accordance with further rules to be determined by the King on the basis of opinions from the Privacy Commission and the Standing Committee I.

The reasoned decision shall be sent immediately to the head of service, to the Minister involved, to the Commission and, where relevant, to the Privacy Commission.

If the Standing Committee I considers that a specific or exceptional intelligence collection method has been used in compliance with the provisions of this Act, while the Commission had forbidden the use of the intelligence collected with this method, and had suspended the use of this method, the Standing Committee I shall lift this prohibition and suspension by means of a reasoned decision and shall immediately inform the head of service, the competent Minister and the Commission.

§ *2.* In the event of a complaint the complainant shall be informed of the decision under the following conditions: any information which could have an adverse impact on the protection of the inviolability of the national territory, the military defence plans, the execution of the assignments of the Armed forces, the safety of Belgian nationals abroad, the internal security of the State, including aspects relating to nuclear energy, the maintenance of democratic and constitutional order, the external security of the State and international relations, the operations of the decision-making bodies of the State, the protection of sources or the protection of the privacy of third parties, shall, with reference to this legal provision, be omitted from the transcript of the decision revealed to the complainant.

The same procedure shall be followed if the decision includes information which could compromise [the secrecy of the criminal investigation or judicial inquiry], if information relates to an ongoing criminal investigation or judicial inquiry.

Replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017).

Article 43/7

§ *1.* Where the Standing Committee I operates in the context of this chapter, the functions of the registry shall be performed by the registrar of the Standing Committee I or by a level 1 staff member appointed by him.

§ *2.* The members of the Standing Committee I, the registrars, the members of the Investigation Service, and the administrative staff are required to maintain secrecy concerning the facts, actions or information that come to their attention as a result of their cooperation in the application of this Act. They may however use the information and intelligence that they acquire in this context for the execution of their assignment, as set out in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment for between eight days and one year, and a fine of between one hundred euro and four thousand euro, or only one of these penalties, if they divulge these secrets in circumstances other than those stipulated in this Act.

Article 43/8

No appeal is possible against the decisions of the Standing Committee I.]

Introduced under Article 18 of the Act of 4 February 2010 (BOJ 10 March 2010).

[CHAPTER V
SPECIAL PROVISIONS CONCERNING THE EXECUTION OF THE ASSIGNMENTS OF THE GENERAL INTELLIGENCE AND SECURITY SERVICE]

Heading replaced under Article 75 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 44

The General Intelligence and Security Service may trace, intercept, listen to, take note of and record any form of communication originating or received abroad, in accordance with the further rules as laid down in Articles 44/3 and 44/4, for the purpose of the assignments referred to in Article 11, § 1, 1. to 3. and 5.][1, 2 and 3]

[1]See § 5 of Article 259*bis* of the Penal Code, [2]repealed under Article 35 of the Act of 5 May 2014 (BOJ 8 July 2014) and [3]restored under Article 76 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 44/1.

The General Intelligence and Security Service may proceed to penetrate a computer system that is located abroad, disable its security features, operate technical procedures on it in order to decipher, decode, save and manipulate the data stored, processed or forwarded by the computer system, as well as disrupt and neutralise the computer system, according to the

further rules laid down in Articles 44/3 and 44/4, for the purpose of the assignments referred to in Articles 11, § 1, 1. to 3. and 5.]

Introduced under Article 77 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 44/2.

The General Intelligence and Security Service may use devices abroad to record fixed or moving images, in accordance with the further rules as laid down in Articles 44/3 and 44/4, for the purpose of the assignments referred to in Article 11, § 1, 1. to 3. and 5.]

Introduced under Article 78 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 44/3

The review by the Standing Intelligence Agencies Review Committee with regard to the interception of communications [originating or received abroad, the penetration of a computer system that is located abroad, and the recording of fixed or moving images abroad][2,5] by the [General Intelligence and Security Service][4] shall be conducted as follows:

1. The review prior [to the interceptions, penetrations or recordings of fixed or moving images][5] shall be performed on the basis of [annually drafted lists][5].

To this end, at the beginning of December each year, the [General Intelligence and Security Service][4] shall submit [lists][5] of the organisations or institutions that will be subject to interceptions of their communications[, penetration of their computer systems or recordings of fixed or moving images][5] during the coming year for authorisation by the Minister of Defence. [These lists justify why each organisation or institution will be subject to an interception, penetration or recording of fixed or moving images related to the assignments referred to in Article 11, § 1, 1. to 3. and 5., and state][5] the anticipated duration. The Minister of Defence shall take a decision within ten working days and notify the General Intelligence and Security Service of this. This service shall pass on [the annual lists][5], with the authorisation of the Minister of Defence, to the Standing Intelligence Agencies Review Committee.

If the Minister of Defence does not reach a decision or if this has not been sent to the General Intelligence and Security Service before 1 January, this service may start the scheduled interceptions, [penetrations and recordings of fixed or moving images][5], without prejudice to any subsequent decision by the Minister of Defence.

If interceptions of communications[, penetrations in computer systems or recordings of fixed or moving images][5], not stated on the annual [lists][5], turn out to be essential and urgent for the execution of an assignment of the General Intelligence and Security Service, this service shall notify the Minister of Defence at the earliest possible opportunity and no later than the first working day following the start of the interception[, penetration or recording of fixed or moving images][5]. If the Minister does not agree, he may call a halt to this interception[, penetration or recording of fixed or moving images][5]. [The General Intelligence and Security Service shall notify the Standing Committee I of the Minister of Defence's decision as soon as possible][3,5].

2. The review during the interception[, intrusion or recording of fixed or moving images][5] is carried out [at any time][5] by means of visits to the installations where the [General Intelligence and Security Service][4] is performing these interceptions[, penetrations or recordings of fixed or moving images][5].

3. The review after the interceptions [, penetrations and recordings of fixed or moving images][5] is conducted on the basis of [monthly lists of countries or of organisations or institutions that have actually been the subject of interception, penetration or recording of images during the

previous month, that were brought to the attention of the Standing Committee I, and that justify the reasons why the interception, penetration or recording of images was carried out in the context of the assignments referred to in Article 11, § 1, 1. to 3. and 5., as well as on the basis of][5] the inspection of [logbooks that][5] the [General Intelligence and Security Service][4] continuously [keeps][5] at the place of the interception[, penetration or recording of fixed or moving images][5]. [These logbooks are][5] always accessible to the Standing Intelligence Agencies Review Committee.][1]

[1]Introduced under Article 4 of the Act of 3 April 2003 (BOJ 12 May 2003), [2]introduced under Article 19 of the Act of 4 February 2010 (BOJ 10 March 2010), [3]replaced under Article 36 of the Act of 5 May 2014 (BOJ 8 July 2014), [4]replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [5]renumbered, replaced and introduced under Article 79 of the Act of 30 March 2017 (BOJ of 28 April 2017).

[Article [44/4][4]

In relation to the interception of communications [originating or received abroad, penetration of a computer system that is located abroad and recording of fixed or moving images abroad][2,4] by the [General Intelligence and Security Service][3], the Standing Intelligence Agencies Review Committee, regardless of the other powers granted to this Committee on the basis of the Act of 18 July 1991, is entitled to halt interceptions[, penetrations or image recordings][4] that are in progress if it turns out that […][4] they […][4] do not observe the statutory provisions […][4] or the authorisation referred to [in Article 44/3][4], 1., paragraph 2. [It shall order that the data which has been illegitimately obtained may not be used and must be destroyed, in accordance with further rules that are to be determined by the King.][4] Notice of this detailed and reasoned decision must be given to the Head of the [General Intelligence and Security Service][3] and the Minister of Defence.] [1]

[1]Introduced under Article 5 of the Act of 3 April 2003 (BOJ 12 May 2003), [2]introduced under Article 20 of the Act of 4 February 2010 (BOJ 10 March 2010), [3]renumbered and replaced under Article 3 of the Act of 30 March 2017 (BOJ 28 April 2017) and [4]replaced and introduced under Article 80 of the Act of 30 March 2017 (BOJ 28 April 2017).

[Article 44/5.

If intervention is required on a communications network to enable the interception of communications originating or received abroad, as referred to in Article 44, the network operator or electronic communications service provider will receive a written request from the head of service and must cooperate as soon as possible.

Any person who refuses to cooperate in the requests as referred to in paragraph 1 shall be subject to a fine of between twenty-six euros and twenty thousand euros. The services rendered will be reimbursed on the basis of the actual costs, after supporting documents are submitted.

On a motion of the Minister of Defence and the Minister competent for electronic communications, the King shall decide the further rules for this cooperation.]

Introduced under Article 81 of the Act of 30 March 2017 (BOJ 28 April 2017).