Ad hoc information request: National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

BELGIUM

Version of 1 October 2014

Milieu.ltd

Summary

1. Description of the legal framework

In Belgium the intelligence and surveillance activities are regulated at the Federal level.

As regards the legal framework, **s**urveillance activities are mainly governed by the law of 30 November 1998 on intelligence and security services and by the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data. The Act of 4 February 2010 on data collection methods by the intelligence and security services[1] (introducing amendments to the aforementioned law of 30th November 1998) came into force on 1 September 2010, providing more far reaching powers for intelligence and security services, including the possiblity to tap phones, to enter homes of people suspected of being involved in terrorist activities without their consent.

The law of 18 July 1991 governing the review of the police and intelligence services and of the coordination unit for threat assessment[2] subjects the intelligence services to a review by the Standing Committee I[3].

The Electronic Communications Act 2005[4] sets out principles relating to confidentiality of communications, processing data and protection of private life of users. The law mandates that telecommunications network operators and service providers store traffic and identification data of their end users for various law enforcement purposes for 12 months, including allowing intelligence services to access and gather that type of data in order to carry out their mission.

a. types of security services and bodies involved (and b. extent of their powers)

The Belgian intelligence and security community consists of the following **services and bodies**:

Bodies mainly undertaking surveillance:

- Intelligence and security services: there are two intelligence and security services in Belgium:
  - The **State Security** (Veiligheid van de Staat/Sûreté de l'Etat) is the civil intelligence service. The service is primarily under the authority of the Ministry of Justice and sometimes falls under the authority of the Minister

[1] Belgium, Act of 4 February 2010 on data collection methods by the intelligence and security services (Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité/ Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, published on 10-03-2010, no. 2010009144**,** http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2010020426&table_name=wet.

[2] Belgium, law of 18 July 1991 governing the review of the police and intelligence services and of the coordination unit for threat assessment (Loi du 18 Juillet 1991 organique du controle des services de police et de renseignements et de l'organe de coordination pour l'analyse de la menace/ Wet Van 18 Juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coordinatieorgaan voor de dreigingsanalyse), 1 April 2011, http://www.comitep.be/fr/Wet-Loi.pdf.

[3] See European Parliament study, 'Parliamentary and Specialised Oversight of Security and Intelligrance Agencies in the EU', p. 191, http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf .

[4] Belgium, law of 13 June 2005 (Loi du 13 Juin 2005 relative aux communications electroniques/Wet betreffende de elektronische communicatie) published on 20-06-2005, no. 2005011238, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2005061332.

of the Interior. The main mission of the service is to collect and analyse information that reveals a threat to Belgium and to inform the government. It is also responsible for protecting foreign VIPs, and vetting procedures with regard to classification and security clearances. It can also provide assistance and technical support in judicial investigations[5].

- The **General Intelligence and Security Service of the armed forces** (Algemene Dienst Inlichting en veiligheid/Service Général du Renseignement et de la Sécurité - GISS) is the military intelligence service and is under the authority of the Minister of Defence. It is part of the armed forces. Its main role is collecting and analysing intelligence relating to any activity that threatens or could threaten the national territory, military defence plans, the armed forces or Belgian nationals abroad. The service also ensures the military security of the personnel of the Defence. It is also mandated with neutralising cyber-attacks on Defence networks and identifying perpetrators. Similarly to the State Security this service carries out vetting procedures for individuals who have access to secret information in their work. It can also lend assistance and technical support to the judicial authorities.[6]

- The **Coordination Unit for Threat Assessment (CUTA)** has been operational since 1 December 2006 and is under the joint authority of the Ministers of the Interior and Justice. It draws up specific or strategic evaluations of terrorist and extremist threats in and to Belgium, relying on intelligence obtained by different services (including the State Security; the GISS; the Department of Customs and Excise of the Federal Public Service of Finance; the Department of Federal Immigration of the Federal Public Service of the Interior; the Federal Public service of mobility and transport; the Federal Public Service of Foreign Affairs, Foreign Trade and Development Co-operation). The threat assessments are made for the political, administrative and judicial authorities[7].

c. control/oversight mechanisms,

Two entities are in charge of reviewing special intelligence gathering methods: the administrative Commission and the Standing Committee I. This is regulated by the Law of 18 July 1991 and the Law of 30 November 1998 mentioned above.

- **Standing Intelligence Agencies Review Committee (Standing Committee I)** is a permanent and independent parliamentary review body set up by the Act of 18 July 1991**.** It is responsible for reviewing the activities of the State Security, the General Intelligence and Security Service of the Armed Forces. The review usually relates to the legitimacy (review of observance of the applicable laws and regulations), effectiveness (supervision of the efficiency of the intelligence services), and coordination (the

[5] Belgium, Law on Intelligence and Security, Articles 7 and 20 (Wet houdende regeling van de inlichtingen- en veiligheidsdienst, B.S., 18 December 1998, Artikelens 7 en 20 ; Loi organique des services de renseignement et de sécurité,., Articles 7 et 20) 18 December 1998, no. 1998007272, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032.

[6] Belgium, more information on the GISS website: www.mil.be/is.

7 Belgium, as set out in the Threat Assessment Act of 10 July 2006 (Loi du 10 Juillet 2006 relative à l'analyse de la menace ; 10 Juli 2006 Wet Betrefende de Analyse Van de Dreiging), M.B. 20 July 2006 http://www.comiteri.be/images/pdf/wetgeving/wet%20van%2010%20juli%202006.pdf?phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb/.

mutual harmonization of the work of the services concerned). The Committee also reviews the Coordination Unit for Threat Assessment with regard to their obligation to pass on information on terrorism and extremism. The Committee oversees the policies of the intelligence and security services; completed and ongoing operations; administration and management; budgets and expenditure of the agencies. It also investigates complaints from the public and advises on draft legislation or statutory amendments. More specifically, the oversight body has the following powers:

- It performs its reviewing role through investigations that it starts on its own initiative, on the request of the Chamber of Representatives or the competent minister or authority, or on the request of a citizen or a civil servant who lodges a complaint or files a denunciation.
- It is also responsible for a posteriori controlling of the specific and exceptional intelligence data collection methods used by the intelligence and security services. Here the Committee acts as a judicial body.
- Provides written advice to the judicial authorities on the legality of the way in which information added to criminal proceedings was collected by the intelligence and security services.
- On request the Committee can advise on a Bill, draft Royal Decree, Circular Letters or any other document expressing the political orientations of the competent ministers regarding the functioning of the intelligence services or the Coordination Unit for Threat Assessment.
- Responsible for controlling interceptions of communications from abroad, which the military intelligence service can, for military purposes, intercept, tap and record.
- It can request to carry out an investigation in the framework of a parliamentary enquiry. Ensures the chairmanship and the registry of the Appeal body for security clearances, certificates, and advice.
- Judicial role: when instructed by the judicial authorities, its investigations service investigates the members of the reviewed services who are suspected of having committed a felony or misdemeanor.

- The **Administrative Commission** responsible for monitoring specific and exceptional intelligence data collection methods used by the intelligence and security services is the entity responsible for reviewing special intelligence gathering methods. It is made up of three acting members and three substitute members. One of the members has the capacity of State prosecutor, and the two others have the capacity of judge.
- **Standing Police Services Review Committee** –This Committee was created in 1991 as an oversight committee on the police. It has a monitoring role on the functioning of the police, including by channeling complaints from citizens[8].
- **Ministerial Committee for Intelligence and Security** (Ministerieel Comité voor inlichtingen en veiligheid/Comité ministériel du renseignement et de la sécurité) – This Committee is the political body determining the general intelligence policy of the government. It takes political and legislative initiatives with regard to intelligence and security, and instructs both intelligence services. The Committee is currently made up of the Prime Minister, the Minister of Foreign Affairs, the Minister of Justice, the Deputy Prime Minister and Minister of Economy, the Minister of Defence, the Minister

[8] Belgium, http://www.comitep.be/fr/index.asp.

of the Interior.[9] **Board of Intelligence and Security** (College voor inlichtingen en veiligheid/Collège du renseignement et de la sécurité) – This body executes the decisions made by the Ministerial Committee for Intelligence and Security.[10]

d. geographical scope of surveillance

The **geographical scope** of the State security department is limited to the Belgian national territory. The mandate of the Military security service is also to protect the operations of the Belgian Armed Forces and Belgian citizens abroad. This does not suggest extra-territorial power to Belgium to conduct surveillance in other EU MS however.

e. conditions under which intelligence services can conduct surveillance and for which purpose(s) (such as national security, investigation or prevention of crimes, etc.)

As mentioned above the national intelligence services can collect information that can be a threat or potential threat to Belgium and additionally for the GISS, military defence plans, the armed forces or Belgian nationals abroad. Specific threats to national security defined in law are any activity, individual or collective, carried out in Belgium or abroad, which can be linked to espionage, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations, and attempts to influence decision-making through misleading and illegal means. This includes disseminating propaganda as well as financial, technical and logistical support (Article 8, Law on intelligence and security 1998)[11].

To this end, intelligence and security services may resort to the following data collection methods (as set out in the law of 30th November 1998 on intelligence and security services):
Ordinary methods includes the use of open source; the use of informants (human sources; and observation of public places and private places accessible to the public without the use of technical means.

Specific methods include observation using technical means, in public places and private places accessible to the public or observation, with or without the use of technical means, of private places which are not accessible to the public; inspection, using technical means, of public places, private places accessible to the public and closed objects located in these places; consulting data identifying the sender or addressee of a letter or the owner of a PO box; measures used to identify the subscriber or habitual user of an electronic communication service or the means of electronic communication used; and measures used to find call information for electronic communication methods and localisation of the origin or destination of electronic communications.

[9] Belgium, see Belgian Standing Intelligence Agencies Review Committee website: http://www.comiteri.be/index.php?option=com_content&task=view&id=53&Itemid=53&phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb%3F%3DEN&lang=EN.
[10] Belgium, see Belgian Standing Intelligence Agencies Review Committee website: http://www.comiteri.be/index.php?option=com_content&task=view&id=53&Itemid=53&phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb%3F%3DEN&lang=EN.
[11] Belgium, Law on Intelligence and Security (Wet houdende regeling van de inlichtingen- en veiligheidsdienst, B.S., 18 december 1998, Loi organique des services de renseignement et de sécurité, M.B. 18 December 1998, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032.

Exceptional methods include observation, with or without the use of technical means, among others in private places which are not accessible to the public, or in premises used for professional purposes or as a residence for a lawyer, doctor or journalist; inspection, with or without the use of technical means, among others of private places which are not accessible to the public or premises used for professional purposes or as a residence for a lawyer, doctor or journalist and of closed objects found in these places; setting up or appealing to a legal entity to support operational activities and appealing to officers of the service, under a false identity or in a false capacity; opening and reading letters, either sent via a postal service or not; collecting data on bank accounts and bank transactions; intrusion into a computer system, with or without the use of technical means, false signals, false codes or false capacities; tapping, listening to and recording communication.

For exceptional methods, the Administrative Commission also carries out an a priori review: it must provide assent prior to the use of such a method. Only for the cases where there is a judicial investigation in the same time than an intelligence investigation, the Commission decides, with the Federal court or competent magistrate, whether the service of information and security may continue its investigations.

f. different stages of surveillance procedure (collection, analysis, storing, destruction)

As regards storing and destruction, the Administrative Commission can visit the place where the intelligence is stored, it can seize and hold the intelligence under its surveillance and hear the involved members of the intelligence and security services.[12]

2. Safeguards foreseen by the legal framework

The Standing Intelligence Agencies Review Committee can act: 'ex officio', through a parliamentary or ministerial action or decision. It has its own investigations office acting through complaints (including from individuals), a public prosecutor or a decision by an investigating judge (procedure described above in the section on oversight bodies).

Specific safeguards:

The Law of 8th December 1992 on privacy and data protection sets out safeguards on right to information (Article 9); challenging the processing of data (Article 10). However these do not apply to the processing of personal data by the State Security, the General Intelligence and Security Service of the Armed Forces (Article 3 § 4)

Addressing the Commission for the Protection of Privacy: The law nonetheless sets out in Article 13 that **a**nyone proving his identity has the right to address the Commission for the Protection of Privacy free of charge,

Administrative Commission: reviewing specific and exceptional data collection methods used by the intelligence services.

3. Judicial or non-judicial remedies

[12] Article 18/3§2 and 18/10§6 Belgium, Law on Intelligence and Security (Wet houdende regeling van de inlichtingen- en veiligheidsdienst, B.S., 18 december 1998, Loi organique des services de renseignement et de sécurité, M.B. 18 December 1998, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032.

Any citizen who considers that his/her individual rights have not been respected by the State Security, the General Intelligence and Security Service, the Coordination Unit for Threat Assessment or by a supporting service acting in this capacity, may lodge a complaint. The law also enables citizens to inform the Standing Committee I of their complaints or denunciations in the event of any dysfunction noted within the services mentioned above.[13]

Complaint with the **Standing Intelligence Agencies Review Committee:** the Committee can examine, upon complaint by a citizen with a legitimate interest, the legality and effectiveness of activities and decisions of the intelligence services, and of the specific and exceptional methods used for collecting data. Anybody who is or has been directly affected by the action of an intelligence service, the Coordination Unit for Threat Assessment or a support service can lodge a complaint or file a denunciation to the Standing Committee I or its Investigations Service.
Moreover, any civil servant or any person who holds a public office and any member of the armed forces who is directly affected by the directives, decisions or rules of application thereof, as well as by procedures or actions, can lodge a complaint or file a denunciation without having his/her supervisor or hierarchical superiors' permission. Verbal complaints can be lodged in the offices of the Standing Committee I and written complaints can be lodged by e-mail, fax or letter. The Committee also acts as a judicial body. If the Standing Committee I notes that the decisions regarding special methods are illegal, it orders the cessation of the method concerned and prohibits the use of the data collected using this method and orders their destruction.

T**he administrative Commission responsible for monitoring specific and exceptional intelligence collection methods used by the intelligence and security services:** In the context of specific and exceptional intelligence data collection methods used by the intelligence and security services, the administrative Commission reviews the legality of the measures, including ensuring that the principles of subsidiarity and proportionality have been respected. In some cases, the methods can only be used after the administrative Commission has given its assent to the head of the intelligence service's decision to use a specific or exceptional method. If the strict rules have not been followed, the administrative Commission may order a provisional ban on the use of the data collected via the method as well as the suspension of this method.

- Other remedies:

Complaint with the **Commission for the Protection of Privacy**: If a citizen has been unable to apply the Open Government Act[14] to consult the information that an intelligence service (or the Coordination Unit for Threat Assessment) has collected on him/her, he/she can turn to the Commission for the Protection of Privacy. However, the citizen is not allowed to consult such information. The Commission can make recommendations. Moreover, it can decide to rectify or remove data, or have data introduced that differ from those processed; it may also prohibit the disclosure of data. Further, after the Commission's verifications, the service concerned shall inform the Commission of the effect that has been given to the recommendations

[13] Belgium, see Belgian Standing Intelligence Agencies Review Committee website: http://www.comiteri.be/index.php?option=com_content&view=article&id=4&Itemid=8&lang=EN.
[14] Belgium, Open Government Act (Loi n° 94-1724 du 11 avril 1994 relative à la publicité de l'administration/ Wet betreffende de openbaarheid van bestuur), 13 June 1994, no. 1994000357 ,http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1994041151&table_name=wet.

(Articles 43 and 44 of the RD of 13/02/2001). In addition, the Commission has the power to bring infringements of the laws to the attention of the judicial authorities.

Complaint with the **Federal Ombudsman**: This body supervises any 'federal administrative service' and thus also the services that the Committee reviews. The federal ombudsman can start an investigation after a complaint from a citizen or on the request of the Chamber of Representatives. Unlike the Standing Committee I, it does not have a right of initiative.

Complaint with the **general judiciary** (ordinary courts): If a basic right is violated or if a person has suffered damage due to unlawful or careless acts of government, the person concerned can go through the ordinary courts in order to stop an ongoing illegality and to award compensation.

Complaint with the **Council of State**: the Council of State can annul decisions by administrative authorities, if a person claims that a decision was made on the basis of an advice by the intelligence services about his situation which contained incorrect elements. In addition, the Council of State can quash the refusal of an intelligence service to allow a person to consult administrative documents that relate to him (on the basis of the Law of 11 April 1994 on the Open Government).

Annex 1 – Legal Framework relating to surveillance

A- Details on legal basis providing for surveillance

Name and type of the surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of surveillance as provided for by the law	Is the law allowing for surveillance in another country (EU MS or third countries)?
Law 30th November 1998 on intelligence and security services/Wet houdende regeling van de inlichting- en veiligheidsdienst/ Loi organique des services de renseignement et de sécurité (Ref. B.S./M.B., 18 december 1998/18 décembre 1998, www.ejustice.just.fgov.be	Events Groups Individuals including in specified professions: special rules for lawyers, doctors and journalists (i.e. the law provides in Art 2 §2 the prohibition for intelligence and security services to obtain, analyse or use data protected by professional	Espionage Terrorism Extremism Proliferation Harmful Sectarian organisation Criminal Organisation - Attempts to influence decision-making through misleading and illegal means	Protection of the internal State security and the durability of democratic and constitutional order, the external Security and the international relations and the scientific oreconomic potential. Protection of the national territory, , the military planning, the troops and the Belgian citizens	Ordinary intelligence methods: none Specific intelligence methods: the head of the Intelligence and Security Services takes the decision on the implementation of such a method. He or she may only execute the decision after receiving a notification from the Commission. The State Security	Subsidiarity and proportionality is necessary (ordinary, specific and exceptional) Storing and destruction of data are subject to a timing relevant to the goal and in accordance to the advice of the commission for the protection of privacy.	Specific intelligence methods: monthly reporting to the Administrative Commission Exceptional intelligence methods: two months (can be repeated) and limited towards: espionage, terrorism, proliferation, harmful sectarian organisations and criminal	No.

	secrecy of lawyers, doctors or the confidentiality of sources of journalists (exceptions to this is where there is evidence that a lawyer, doctor or journalist was personally involved in the development of the potential threat).		abroad .	service is primarily under the authority of the Ministry of Justice. With regard to matters concerning State Security, the Ministry of Interior does not intervene within the framework of the implementation of specific and exceptional methods. The General Intelligence and Security Service of the armed forces is under the authority of the Minister of Defence. Exceptional intelligence methods: formal assent from the Administrative Commission. In the event of failure of the Commission, the Ministry of Interior may intervene.		organisations.	

				Interference with a police or judicial investigation needs to be reported to the Administrative Commission taking the final decision how to act in the future In accordance with the Law of 8th December of 1992 on privacy and data protection/Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/ Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. (Ref. B.S./M.B. 18 maart 1993/18 mars 1993)			

B- Details on the law providing privacy and data protection safeguards against surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Law 8th December 1992 on privacy and data protection/Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Ref. B.S./M.B. 18 maart 1993/18 mars, www.ejustice.just.fgov.be	The Law 8th December 1992 on privacy and data protection sets out safeguards on the right to information (Article 9); challenging the processing of data (Article 10). However these do not apply to the processing of personal data by the State Security Service, the General Intelligence and Security Service of the Armed Forces (Article 3 § 4) *Addressing the Commission for the Protection of Privacy:* Anyone proving his identity has the right to address the Commission for the Protection of Privacy free of charge, in order to exercise the rights referred to in articles 10 and 12 (right to	Only protection in relation to the processing of data for all citizens.	Applicable to Belgium (legal and natural persons) and Belgian citizens abroad. The law on the protection of privacy with respect to personal data treatment of 8 December 1992 is applicable in Belgium and abroad when the cumulative conditions formulated in Article 3(a) of the DPL are fullfilled.

	information; challenging data; respectively). By decree after deliberation in the Council of Ministers, having received the opinion of the Commission for the Protection of Privacy, the King shall establish the manner in which these rights are to be exercised. The Commission for the Protection of Privacy shall only inform the data subject of the fact that the necessary verifications have been carried out. If the data subject's request, however, relates to the processing of personal data by the police services with a view to an identity check, then the King shall establish the information the Commission may disclose to the data subject by decree after deliberation in the Council of Ministers, having received the opinion of the Commission for the Protection of Privacy. (Article 13) *Requirements for collecting data* Article 4: Personal data must be: 1° processed fairly and lawfully; 2 ° collected for specified, explicit		

	and legitimate purposes. 3 ° It must be adequate, relevant and not excessive in relation to the purposes for which it is collected or processed; 4 ° accurate and kept up-to-date; 5 ° kept in a form that allows identification of data subject for no longer than necessary with a view to the purposes for which the data is collected or further processed.		
Law of 30th November 1998 on intelligence and security services; Loi organique des services de renseignement et de sécurité ; Wet houdende regeling van de inlichtingen- en veiligheidsdienst 1/02/1999, 1998007272http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032	Prohibits the use of information and security services of using analysing or obtaining data protected by profession confidentiality (doctors; lawyers; journalists). (Article 2 paragraph 2). The information collected must have a link with the final data collection objective (Art. 13); Information and security services must take care that their investigation does not negatevely affect a judicial procedure (Article 13/2). If this might be the case the information and security services must inform the Administrative Commission, who decides in consultation with the federal court if the investigation may continue. The Commission then informs the	Protection in relation to the processing of data for all citizens.	Applicable to Belgium and Belgian citizens abroad.

	Standing Committee I of its decision. (Article 13/2); The intelligence and security services may request the judiciary, civil servants and public officials to inform their department of information for them to carry out their investigation. However, if these judicial authorities, officials and public employees, including police, believe that the information requested from them is likely to affect a judicial investigation or the collection of information covered by the law of 11 January 1993 on the prevention of the use of the financial system for the purpose of money laundering and financing of terrorism, or is likely to harm the physical integrity of a person, they may refuse to disclose within five working days of the request, stating their reasons in writing (Article 14).		
Electronic Communications Act of 13 June 2005 Belgium, (Loi du 13 Juin 2005 relative aux communications electroniques/Wet betreffende de elektronische	Title IV, Chapter III (Protection of final users): Sub-section I. - Information for final users (sets out requirements for the type of information to be provided to users).	Protection in relation to the processing of data for all citizens	Applicable to Belgium and Belgian citizens abroad.

communicatie) published on 20-06-2005, no. 2005011238, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2005061332.	Sub-section 5. - Measures for disabled final users (includingequal access to services equivalent to those available to all users). Section 2. – Confidentiality of communications, data protection and right to privacy (requirement that operators delete or anonymise data as soon as they are no longer necessary for the communication). If it does not do so, the operator must inform, prior to using the data, the user of the type of data being used, the precise objective of the processing of data, and the duration. Operators must provide a free and easy way for subscribers to withdraw their consent to the processing of data.		

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Standing Intelligence Committee Agencies Review Committee/ Comité I/Comité R	A collegial body of three members chaired by a magistrate are nominated by the Federal Parliament (the president is not acting as a magistrate once nominated, and the two other members are counsellors that should not necessarily be magistrates).	Law of July 18th 1991 on Oversight/Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse/Loi organique du contrôle des services de police et de renseignement et de l'organe de coordination pour l'analyse de la menace (Ref. B.S.26 juli 1991/26 juillet 1991), www.ejustice.just.fgov.be	Ex officio' Through a parliamentary or ministerial decision Through complaints, public prosecutor's or investigating judge's decision On activities, functioning, policies and members of the intelligence and security Services and the Coordination Unit for Threat Assessment (l'Organe de Coordination pour l'Analyse de la Menace – OCAM) The oversight is a posteriori.	One president and two advisors appointed for six years (renewable); administrative staff (16 staff), one clerk; and an investigations Service (5 members). The members are nominated by the Federal Parliament for a period of six years (can be prolonged) and do have a law degree. The same is applicable to the head of the administrative staff. The head of the investigations	- Investigates either from its own initiative or at the request of the House of Representatives, the Senate, the competent minister or the competent authority. The Committee may also investigate a complaint or report of a citizen or official. - Responsible for verifications *a posteriori* of specific and exceptional methods of data collection by the intelligence and security services. The Committee acts here as a judicial body. - The Committee may also give written notice to the judicial authorities regarding the legitimacy of the way the data used in a criminal case were collected by the

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
				Service is a magistrate or a member of an intelligence or police service or a public servant nominated by the Standing Intelligence Committee Agencies Review Committee for a period of five years. The same is applicable to the head or *Clerk* of the administrative staff.	intelligence and security services. - Responding to requests for advice from the House of Representatives, the Senate or a competent Minister on any bill or royal decree, circular or any other document that expresses political statements of a competent minister concerning the functioning of the intelligence services or the Coordinating Body for Threat Analysis. - The military intelligence service may, for military purposes, intercept, listen to and record calls made abroad. The Standing Committee I is responsible for conducting the monitoring of these interceptions of communications.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					- Competent to preside and clerk the Appeal Body for clearances, certificates and security advice. - The Investigations Service of the Standing Committee I also has jurisdiction: it can be required by the judicial authorities to investigate the crimes of which are suspected members of the relevant services Annual reporting to the Federal Parliament ; These are activity reports – reporting on the way the Committee has analysed terrorist threats; the way police service and security services carried out their duties with regard to terrorist threats; updates such as effects of new laws; conclusions and recommendations. The latest report dates from 2013:

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2013.pdf. Six monthly reporting to the Federal Parliament on specific and exceptional intelligence data collection methods;
Administrative commission/Bestuurlijke commissie/Commission administrative	Article 43/1 of Law 30th November 1998 on intelligence and security services affirms that the Commission is independent and is competent to set its own internal rules. However, its members are appointed by the Federal government and the Belgian House of Representatives (part of the Belgian Federal Parliament) fixes the budget (upon suggestion of the Commission)	Law 30th November 1998 on intelligence and security services/Wet houdende regeling van de inlichtingen- en veiligheidsdienst/Loi organique des services de renseignement et de sécurité – Article 43/1 (Ref. B.S./M.B., 18 december 1998/18	Oversees the use of specific or exceptional data collection methods by the intelligence and security services.	Three members. All of them are magistrates. Administative secretariat.	The Administrative Commission controls the legality (including compliance with principles of proportionality and subsidiarity) of specific and exceptional intelligence methods of data collection by the intelligence and security services. In certain cases such methods may only be used once the Administrative Commission has given its assent to the decision of the head of the intelligence service to use them. If an intelligence and security service

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					conducts an investigation which can be prejudicial to a judicial investigation it must inform the Commission. The Commission decides, with the Federal court or competent magistrate, whether the intelligence and security service may continue its investigations. The Commission informs the Standing Intelligence Committee Agencies Review Committee of its decision. This decision is binding and the intelligence and security service must follow it (Article 13/2). In case of breach of rules, the Administrative Commission can issue a ban on using the data which has been collected using the questioned measure. The Commission can also order for the intelligence

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					and security services to stop using this measure. As regards storing and destruction, the Administrative Commission can visit the place where the intelligence data collected through a specific or exceptional method are stored, it can seize and hold these intelligence data under its surveillance and hear the involved members of the intelligence and security services. The Commission may notify on its own initiative its decision to the Standing Intelligence Committee Agencies Review Committee. (Article 18/2)

Annex 3 – Remedies15

• **Organic Law of 30 November 1998 on the intelligence and security services** • **Law of 18 July 1991 on the monitoring of police and intelligence services and the coordination unit for threat assessment** • **Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data**				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
				Violation of data protection, private life, specific legislation, etc.
Collection*	No – however, upon request by a person with a legitimate interest, that person is informed in writing by the intelligence service that he/she has been the subject of a specific or	Law of 11 April 1994 on the Open Government (Article 4): Upon request, each person with a legitimate interest can have access to administrative documents from an administrative government body relating to him/her, receive information	(1) Complaint before the **Commission for the Protection of Privacy**: the Commission can examine complaints about the protection of privacy in relation to the processing of personal data. Processing of personal data includes collecting, storing, analysing and destructing. (Article 1 of the Law of 8 December 1992) [1]. The citizen can however not be granted access in this context to his personal data. The Commission's competences	Article 31 of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data

15 In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

	exceptional method for the collection of data, on the condition that more than 5 years have passed since the finalizing of the method and that, since then, no new data have been collected with respect to that person. (Article 2 of the Law of 30 November 1998 on the intelligence and security services). However, see judgment of the Constitutional Court of 22 September 2011: article 2(3) is considered in violation of the Consitution – the intelligence	about these documents and receive a copy. This applies to the data collected and stored by the intelligence services. (Source: http://www.comiteri.be/index.php?option=com_content&view=article&id=33&Itemid=67%3F%3DEN&lang=EN) There are exceptions : see article 6 of the Law of 11 April 1994	are limited: formulate recommendations and notifying the citizen that a verification has been carried out. The Commission cannot communicate anything about the content of the documents. (Source: http://www.comiteri.be/index.php?option=com_content&view=article&id=33&Itemid=67%3F%3DEN&lang=EN) (2) Complaint at the **Standing Intelligence Agencies Review Committee**: the Committee can examine, upon complaint by a citizen with a legitimate interest, the legality and effectiveness of activities and decisions of the intelligence services, and of the specific and exceptional methods used for collecting data. In this context, the Standing Committee can act as a parliamentary review body; as a judicial body; and as a prejudicial advisory body (in criminal matters). (Source: http://www.comiteri.be/index.php?option=com_content&view=article&id=4&Itemid=8&lang=EN)	Article 34 of the Law of 18 July 1991 on the monitoring of police and intelligence services and the coordination unit for threat assessment + Article 43/4 of the Law of 30 November 1998 on the intelligence and security services

	services must themselves take the initiative to inform persons that they have been the subject of a specific or exceptional method for data collection.			
Analysis*	See above	See above	See above	See above
Storing*	See above	See above	See above	See above
Destruction *	See above	See above	See above	See above
After the whole surveillance process has ended	No See above	See above	See above	See above

- **Right to private life, article 22 of the Constitution**

Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
				Violation of data protection, private life, specific legislation, etc.
General (all stages)			Complaint with the **Federal Ombudsman**, who supervises any	Law of 22 March 1995 on the federal ombudsman (amended

			federal administrative service, including the intelligence services. He can start an investigation. Complaint with the **general judiciary (ordinary courts)**, if person claims a basic right has been violated (to stop ongoing illegality and to claim compensation for damages). Complaint with the **Council of State**, which can annul decisions by administrative authorities, if person claims that a decision was made on the basis of an advice by the intelligence services about his situation which contained wrongful elements. In addition, the Council of State can quash the refusal of an intelligence service to allow a person to consult administrative documents that relate to him (on the basis of the Law of 11 April 1994 on the Open Government).	several times). With reference to any legal provision allegedly violated, including the right to private life (Article 22 of the Constitution) Judicial Code of 10 October 1967 (amended several times) With regard to any basic right allegedly violated, including the right to private life (Article 22 of the Constitution) Law of 12 January 1973 on the Council of State (amended several times) With regard to any legal provision allegedly violated.

Annex 4 – Surveillance-related case law at national level

Please provide a maximun of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

Case title	Belgium Constitutional Court, case No. 145/2011, 22 September 2011 at paras 88 and 92
Decision date	September 2011
Reference details (type and title of court/body; in original language and English [official translation, if available])	Belgium Constitutional Court, case No. 145/2011, 22 September 2011
Key facts of the case (max. 500 chars)	The Act of 4 February 2010 on data collection methods by the intelligence and security services was passed and came into force on 1 September 2010. It inserted provisions in the 1998 Act providing new far reaching powers for the secret services (intelligence methods). These include the possibility to tap phones, to enter homes of people suspected of being involved in terrorist activities without their consent. The Flemish, francophone and germanic bar councils requested, jointly with the Ligue des Droits de l'Homme that the Act should be declared unconstitutional.
Main reasoning/argumentation (max. 500 chars)	Not having an active notification of the person subject to a secret intelligence method was deemed very serious as every possibility of effective supervision and legality control would be excluded. The reasoning used was the same as the reasoning of the ECtHR in the Klass case.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Belgian Constitutional Court declared the Act partly incompatible with the Consitution . Article 2 para. 3 of the 1998 Act as rewritten by the 2010 reform (providing that a person subject to a secret intelligence methods is only informed afterwards on request) was declared unconstitutional and contrary to the ECHR.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Belgian Constitutional Court ruled for a partial annulment of the reform Act of February 2010.

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
State security department/Veiligheid van de Staat/Sûreté de l'Etat	Public authority	Tel.: +32 2 205 62 11 Fax : +32 2 201 57 72 E-mail: info@vsse.be	http://justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/onafhankelijke_diensten_en_commissies/veiligheid_van_de_staat/
General Intelligence and Security service/Algemene Dienst Inlichting en Veiligheid/Service Général du Renseignement et de la Sécurité	Public authority	Tel:. +32 800 33348	http://www.mil.be/nl/
Standing Intelligence Committee Agencies Review Committee/Comité I/Comité R	Public authority	info@comiteri.be	www.comiteri.be
Administrative	Public authority	No specific contact details?	www.comiteri.be

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Commission/Bestuurlijke commissie/ Commission administrative	monitoring legality of measures in context of specific and exceptional methods for data collection by intelligence services	Enquiries via Standing Intelligence Agencies Review Committee: info@comiteri.be	
Commission for the protection of privacy/Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée	Public authority	commission@commissionprivacy.be	www.privacycommission.be
Belgian Intelligence Studies Centre	Academia	info@intelligencestudies.be	http://www.intelligencestudies.be/
Ministerial committee for intelligence and security/ Ministerieel Comité voor inlichtingen en veiligheid/Comité ministériel du	Public authority instructing both intelligence services (State security and Military security)	Enquiries via the office of Prime Minister: info@premier.fed.be	No website? [2]. Office of Prime Minister: http://www.premier.be/nl

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
renseignement et de la sécurité			
Board of intelligence and security/College voor inlichtingen en veiligheid/Collège du renseignement et de la sécurité	Public authority executing decisions of the Ministerial committee for intelligence and security	No specific contact details? Enquiries via the office of Prime Minister: info@premier.fed.be	No website? Office of Prime Minister: http://www.premier.be/nl
Parliament/ Parlement/Parlement	Parliament	info@dekamer.be	www.belgium.be
Government/ Regering/Gouvernement	Government	info@just.fgov.be	www.belgium.be
Ligue des Droits de l'Homme	NGO	Tel.: +32 2 209 62 80 Fax: +32 2 209 63 80 E-mail: ldh@liguedh.be	http://www.liguedh.be/

Annex 6 – Indicative bibliography

1. Government/ministries/public authorities in charge of surveillance
   Standing oversight committtee:
   - Van Laethem, W., Vanderborght, J., Inzicht in toezicht (2013), *Regards sur le controle*, Antwerpen, Intersentia, 2013.
   - Annual activity reports from 1994 till 2012 (the latest annual report is from 2012: http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag%202012_FR.pdf.). Vast Comité I (2006), *Codex Inlichtingen*, Brugge, die Keure.
2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance
   Commission for the protection of privacy:
   - Annual reports from 2012 and 2013
   - Infobrochure 'cybersurveillance'.
3. Non-governmental organisations (NGOs)
   None.
4. Academic and research institutes, think tanks, investigative media report.
   The Belgian Intelligence Studies Centre publications :
   - Cahiers Inlichtingenstudies/Cahiers d'études du renseignement, Antwerpen, Maklu, nr. 3, 2013.
   - Cahiers Inlichtingenstudies/Cahiers d'études du renseignement, Antwerpen, Maklu, nr. 2, 2012.
   - *Ethiek en inlichtingen – Ethique et renseignement*, Cahiers Inlichtingenstudies/Cahiers d'études du renseignement, Antwerpen, Maklu, nr. 1, 2012.
   - Cools, M., Dassens, K., Libert, R., Ponsaers, P., De Staatsveiligheid (2005), *Essays over 175 jaar Veiligheid van de Staat – La Sureté. Essais sur les 175 ans de la Surreté de l'Etat*, Brussels, Politeia.