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

BULGARIA

16 October 2014

Bulgarian Helsinki Committee
Nikolay Saykov

Summary

1. The main laws that concern special intelligence means (SIMs) are the Special Intelligence Means Act (SIM Act) (*Закон за специалните разузнавателни средства*, (1997) [1] , the Electronic Communications Act (*Закон за електронните съобщения*, (2007)[2])[3], and the Criminal Procedure Code (CPC). Under the present legal framework there are a number of security services that can request and use special intelligence means (SIMs): the State Agency Technical Operations (SATO), the National Intelligence Service, the intelligence services of the Ministry of Defence, specialized department "Technical Operations" to the SATO, and the State Agency National Security (SANS) (*Държавна Агенция "Национална сигурност*"[4]). The Ministry of Interior ensures the safety of Bulgarian citizens and their property and acts as a crime prevention and crime solving institution.[5] SANS investigates serious and organized crimes, as well as acts that could seriously affect the state and could have implications for its natonal security. SANS also acts as a counter intelligence service as well as anti and counter – terror service. The agency investigates high profile corruption allegations[6]. The authorities that can request use of SIMs are mentioned in Art. 13 of the SIM Act General Directorate "Criminal Police", General Directorate "Guard Police", General Directorate "Boarder Police", District Directorates to the Ministry of Interior, Directorates to the SANS, the National Intelligence Service, the "Military information" and "Military Police" services, the district prosecutors and supervising prosecutors in the pre-trial proceedings. The requests must be addressed to the specific (district) court. SANS has its own Specialised Directorate of Technical Operations that has the ability and authority to use SIMs. After the legislative reform in 2013, an independent agency of SIMs – SATO, was created, to be the state authority responsible for application of SIMs, Art.20, para.1 of the SIM Act. It has a broader function as it handles requests from all competent authorities while its counterpart in SANS handles SIM use only on behalf of the agency.

   (The term "special intelligence means" does not have the same content as the term "traffic data". According to the §71 of the Additional provisions of the ECA, 'traffic data" are data processed for the purpose of transmitting a communication over an electronic communication network, which is different from the operation of SIMs. In relation with art.2 and art. 3 of the SIM Act, SIMs are used to prevent and detect serious intentional crimes under Part I, Part II, Section I,II,IV,V,VIII and IX, Part V, Section I-VII, part VI, Section II-IV, part VIII, Part IXa, part XI, Section I-IV, as well as for the crimes in relation with art. 167, para. 3 and 4, art. 169d, art. 219, para 4, art.220, para. 2, art.253, art. 308, para. 2,3 and 5, art.321, art. 321a, art. 356k and art. 393 from the special part of penal Code.)

2. The main control mechanism is judicial control under articles15 and 34a of the SIM Act, which is exercised prior to the use of SIMs. There are two other significant oversight bodies: the National Bureau for Control over Special Intelligence Means (*Национално бюро за контрол на специалните разузнавателни средства*)[7] and the Parliamentary Committee for Control of the Security Services,

---

[1] Bulgaria, Special Surveillance Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[2] Bulgaria, Electronic Communications Act (Закон за електронните съобщения) (22.05.2007), available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2135553187.

[3] Bulgaria, State Agency "National Security" Act, Art. 21 states that SANS can use SIMs in relevance with the SIM Act. There are no further elaborations, which means, that the only relevant laws are the SIM Act and the Electronic Communication Act.

[4] Bulgaria, State Agency "National Security" (*Държавна агенция „национална сигурност*"), http://www.dans.bg/.

[5] Bulgaria, Ministry of Interior Act (Закон за Министерство на вътрешните работи) (27.06.2014), Art. 6, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2136243824.

[6] [6] Bulgaria, State agency "National security" Act (*Закон за държавна агенция „Национална сигурност"*) (20.12.2007), Art. 4, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2136243824.

[7] Bulgaria, Special Surveillance Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34b, Art. 34f, Art. 34g, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

Use and Employment of Special Intelligence Means and Access to Data under the Electronic Communications Act (*Комисия за контрол над службите за сигурност, използването и прилагането на специалните разузнавателни средства и достъпа до данните по закона за електронните съобщения*[8]). The National Bureau issues legally binding recommendations to the relevant security services regarding the application, collection, storage and destruction procedures for SIMs; upon request has access to all relevant documentation about application, collection, storage and destruction of SIMs.[9] The National Bureau also creates the forms with which all data registries regarding SIMs within the relevant services should abide.

3. The parlamentary committee exercises overall control over the security services in the country; its main functions include inquiries, analysis, issuing recommendations to the National Assembly on related bill propositions; issuing reports to the National Assembly regarding the funtioning and status of the security services. The functions of the Commission are described in Art. 34h of the SIM Act and Art. 16 of the Rules of Procedure of the National Assembly and the Internal rules for the Commission's work.

4. Essentially any person, under Art. 12, para.1, p.1,2 and 3 of the SIM Act, who is within the Bulgarian borders or within the Bulgarian jurisdiction – when the prerequisites of the Art.3, para.1 of the SIM Act exist, can be subject to SIM and traffic data retention.

5. The security services have a legal ability to use SIMs and collect traffic data. This is allowed for the prevention or investigation of serious deliberate offences regarding art.3, para.1 of the SIM Act, national security purposes (the concept for "national security" is defined in art.4, para.1 of the Act. Art. 12 of the SIM Act lists the persons who SIMs may be used for.

6. In Bulgaria, there are several stages for the use of SIMs: collecting data, storing data, analysing the data, preparing material evidence from the data, destroying all data that is not used as material evidence. These stages are executed by the services that utilize SIMs: SATO (State Agency "Technical operations" – *Държавна агенция „Технически операции")* and SDTO (Specialised Directorate "Technical Operations" – *Специализирана дирекция „Технически операции*") with SANS as well as the National Intelligence Service and the intelligence services of the Ministry of Defence.

7. Article 15 of the Special Intelligence Means Act defines the judicial control over the use of SIMs. Every request for that use has to be approved by the chairperson of the corresponding (district) court. Furthermore, a new provision – Art. 15, para. 2 - allows the judge to demand any information about an individual request in order to exercise their individual judgment efficiently when approving or denying the request for use of SIMs. The law requires all approvals and dismisses to be accompanied by argumentation.

8. The same provision requires that all requests be sent to the corresponding regional court. This is to stop the occasional practice of sending requests to regional courts known to be more likely to issue a warrant for use of SIMs, as per the old version of the SIM Act any judge from any regional court could have issued a warrant.[10]

---

[8] Bulgaria, Special Surveillance Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34h, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[9] The National bureau has access only to the documentation regarding the destruction of SIM primary data carriers but not to the carrier themselves; Art. 34f, the SIM Act.

[10] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 15, para 1, available in Bulgarian at: www.mvr.bg/NR/rdonlyres/44C8FE13-0311-4918-8CAD-1C692B23A5C5/0/ZSRS.pdf.

9. The SIM Act also establishes the National Bureau for Control over Special Intelligence Means (National Bureau).[11] It has wide-ranging authority over the requests, collection, storage, analysis and destruction of special intelligence means. The members of the National Bureau are elected by the National Assembly.

10. The National Bureau has the authority to request full access to any and all information and documentation regarding the requested special intelligence means.[12] The law, however, fails to give its members access to the primary physical carriers of the acquired information in order to oversee their destruction. These actions are placed in the competence of a committee, whose members are selected by state institutions which apply special intelligence means – the Special Agency of Technical Operations and the Specialised Directorate of Technical Operations within the State Agency of National Security.[13]

11. The law has provisions granting people subjected to improper use of SIMs information about this fact from the National Bureau, *ex officio*, according art. 34g, para.1 of the SIM Act.[14] It should be noted that there is no specific provision that allows for persons to check whether this obligation is being adhered to. The only possible way might be a request for information under the Access to Public Information Act. The exceptions are formulated in art. 34g of the Act.[15] The exceptions include cases that the National Bureau might consider endanger the purposes of criminal investigation, national security reasons, possibility to uncover the technical means and operational patterns that are used. Furthermore, the current provisions give the possibility to learn about the infraction only to people subjected to improper use of special intelligence means. People under lawful but unnecessary surveillance (for example, persons who were suspected of having committed a crime and thus a judge had approved a request for use of SIMs but no charge against has been filed in the end; via special intelligence means have absolutely no legal ways to become aware of the fact. The investigative authorities use SIMs in accordance with art. 14, para.1, p.7 of the SIM Act (art. 172, para.2, p.6 of the CPC). The existing redress mechanisms apply only to cases of improper surveillance when the use of SIMs temporarily limits the privacy, the housing and the confidentiality of the correspondence and other communication – art. 1, para 2 of the SIM Act.

12. Persons under surveillance are not notified of the fact at any time and there is no legal way to challenge the request for use of SIM's. After the application of SIMs, citizens against whom this method have been used, must be notified unless it can endanger the investigation or endanger someone's life, health or significant property interests.

13. As for the Electronic Communications Act, the law allows investigative authorities to access traffic data. The law states that the approval of a judge is a necessary prerequisite for access to traffic data[16] according to art. 250c of the SIM Act and under the CPC's rules. The provision of Art. 250c, para. 4 refers to the procedure provided for in the Criminal Procedure Code, namely that "for the purpose of

---

[11] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 24b, available in Bulgarian at: www.mvr.bg/NR/rdonlyres/44C8FE13-0311-4918-8CAD-1C692B23A5C5/0/ZSRS.pdf.

[12] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34e, para. 4, available in Bulgarian at: www.mvr.bg/NR/rdonlyres/44C8FE13-0311-4918-8CAD-1C692B23A5C5/0/ZSRS.pdf.

[13] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 31, para. 3, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[14] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34g, para. 3, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[15] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34g, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[16] Bulgaria, Electronic Communications Act (*Закон за електронните съобщения*) (22.05.2007), Art. 250c, available in Bulgarian at: http://www.lex.bg/bg/laws/ldoc/2135553187.

criminal proceedings, the data in Art.250a, para.1 shall be provided to the Court and the pre-trial authorities under the conditions and rules of the Criminal Procedure Code." The general rule of Art 250c provides full judicial control over the requests under Art. 250a, para.1. Moreover, Art.250a, para.6 of the ECA contains an explicit reference to the Law on Protection of Personal Data in relation to the procedure for collecting and storage the data, which is an additional guarantee for individuals.

14. Currently there are limited remedies for an individual subject to surveillance. There is the judicial option of a lawsuit under Art. 2, para. 1, point 7 of the State and Municipal Liability Act[17] for a compensation for being subjected to illegal surveillance. A person can learn that he had been subjected to illegal use of SIMs through the National Bureau for Control over Special Intelligence Means who *ex-officio* notifies anyone subjected to improper surveillance. There are however, exceptions even to that rule. The National Bureau does not inform persons, subjected to surveillance when that can endanger the national security of the state; when that can impede an ongoing investigation; when that can reveal the technical means themselves, as well as the operational methods for collecting data; when that can potentially endanger the life of an undercover operative[18], according to art. 34g, para.2 of the SIM Act. Furthermore, there is no legal way for a person to find out if he had been under unnecessary surveillance. The information acquired through the use of SIM is considered confidential, so there is no access through Access to Public Information Act.[19]

15. It should be explained the role of the Personal Data Protection Act[20] in the case of mass survellance and its application in regard to law enforcement and intelligence agencies. First of all, law enforcement and intelligence services do fall under the authority of the PDPA. However, Art. 1, para. 5 provides exceptions for the applicability of the PDPA in regard to security services. These include instances when the national security, crime prevention, criminal procedeengs, etc. are concerned and when another law regulates these instances[21]. Also the application of the PDPA in cases with use of special intelligence means is in essence non-existing. Art. 34, para. 1 of PDPA[22] allows administrators to deny requests for information *about per*sonal data when this is prohibited by law. The disclosure of information related to use of SIMs is prohibitted under Art. 34, PDPA. Furthermore, the same article elaborates further and speciffically states that classified information and information regarding the national security is protected and cannot be disclosed. The same applies for ongoing investigations or even court trials. Furthermore, from the caselaw of the Personal Data Protection Commission[23] is evident that the commission does not take on cases which are related to state-authorized surveillance even when the latter is conducted on behalf of the Ministry of the interior. No complaints regarding the use of SIMs by SANO have been brought before the Commission to this day. Thus, the PDPA cannot provide a person with information whether he/she had been under improper surveillance. As for the unlawful surveillance, the National bureau has the obligation to inform the person under unlawful surveillance for the fact as per the text of Art. 34g. There are exeptions to that rule as well as explained in the report[24], related to national security.

---

[17] Bulgaria, State and Municipality Liability Act (*Закон за отговорност на държавата и общините за вреди*), (1.01.1989), available in Bulgarian at: http://www.lex.bg/bg/laws/ldoc/2131785730.

[18] Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 34g, para.2, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[19] Bulgaria, Access to Public Information Act (*Закон за достъп до обществена информация*), (7.07.2000), available in Bulgarian at: http://www.lex.bg/bg/laws/ldoc/2134929408

[20] Bulgaria, Personal Data Protection Act (Закон за защита на личните данни) (01.01.2002), available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2135426048.

[21] Bulgaria, Personal Data Protection Act (Закон за защита на личните данни) (01.01.2002), Art. 1, para. 5, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2135426048.

[22] Bulgaria, Personal Data Protection Act (Закон за защита на личните данни) (01.01.2002), Art. 34, para. 1, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2135426048.

[23] The commission is established by Art. 6, Personal Data Protection Act (Закон за защита на личните данни) (01.01.2002), available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2135426048.

[24] See paragraph 14.

Bulgaria – Version of 16 October 2014

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass 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 mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Special Intelligence Means Act (SIM Act); (Закон за специалните разузнавателни средства)	All persons[25] who have committed, are commiting or are preparing to commit serious crimes; All persons who are influenced by the persons mentioned above; the former are unaware of the	Suspicion of conducting criminal activity; conducting criminal activity; threat to national security (although the exact concept is not specifically	National security; criminal investigation; prevention of crime	Prior warrant is required to start the application of SIMs. It is issued by the chairman of the particular regional court. The warrant can be issued post factum but only within 24 hours after the start of the application or the	1. Collecting data 2. Storing data 3. Analyzing data 4. Preparing material evidence from the data to be used during the court proceedings – this stage may not occur 5. Destroying all data that is not used as material evidence	SIMs are to be utilized only within the borders and jurisdiction of the Republic of Bulgaria; the time period is up to 2 months but can be extended to a total of 6 months;	No, it does not

[25] Bulgarian criminal law only applies to physical persons

	criminal nature of the activities; All persons and objects related to national security matters as well as	defined in the bulgarian law)[28]		application would be unlawful. The warrant is for a period of 2 months after which it can be			

[28] Bulgaria, State agency "National security" Act (*Закон за държавна агенция „Национална сигурност"*) (20.12.2007), Art. 4, available in Bulgarian at: http://www.dans.bg/images/stories/promzak/zdans-24072013.pdf. Art. 4 (last amended in June 2013) states that: "The State Agency "National Security" performs activities for protection of the national security from violations of the independence and sovereignty of the Republic of Bulgaria, the territorial integrity, the national interests, the estimated constitutional order and the fundamental rights and freedoms of the citizens related to:
1.intelligence in favour of foreign forces;
2.danger for the sovereignty and territorial integrity of the state and unity of the nation;
3. anti-constitutional activities ;
4. corruption activities of persons at high state, public and other positions in the public or the private sector;
5. application of force and use of mass dangerous means with political aim;
6. danger for economics and financial security of the state;
7. danger for ecological security of the state;
8. violation of the functioning of the national system for protection of classified information;
9. endangerment of the security of strategic objects and activities;
10. destructive influence over the communication and information systems;
11. international terrorism and extremism as well as their financing;
12. international trade with weapons and products and technologies with double use;
13. production, keeping and distribution of mass dangerous means and products or technologies with double use, drug substances and precursors when this implies danger for the normal functioning of the state bodies;
14. organized crime activities of local and transnational crime structures;
15. customs regime, monetary, tax or social security systems;
16. trafficking in human beings ;
17. cybercrimes or crimes perpetrated in or through computer webs or systems;
18. intellectual property;
19. fake or false money, pay instruments and official documents;
20. trafficking in cultural objects and gambling;
21. activities of groups or persons supporting foreign agencies, terroristic or extremist organizations;
22. migration process;
23. signing contracts that are not in favour of the state, money laundering and implementation of projects under EU funds through fraud.

	objects used to identify persons under the first paragraph, as per Art. 12, para. 3 and 4[26];, which is broadly defined and can include any number of people thus justifying mass surveillance; Persons who have requested themselves the use of SIM for their own protection[27];			extended for 4 more months.			

[26] Bulgaria. Special Surveillance Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 12, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

[27] Bulgaria. Special Surveillance Means Act (*Закон за специалните разузнавателни средства*) (21.10.1997), Art. 12, available in Bulgarian at: http://lex.bg/bg/laws/ldoc/2134163459.

Electronic Communications Act (Закон за електронните съобщения)	All persons who may be part of investigations for serious criminal offences or for missing persons;	Suspicion of conducting criminal activity; conducting criminal activity; threat to national security; search for missing persons;	criminal investigation; prevention of crime; national security	Prior warrant is required to receive traffic data. It is issued by the chairman of the particular district court. Under the instructions of the Attorney General, investigative services may not require prior judicial authorization for receiving traffic data from the providers under Art. 250c, pr. 4 (чл. 250в, ал 4), Electronic Communications Act, which allows access of traffic data to investigative authorities as this article specifically does not require prior judicial	1. Collecting data 2. Storing data 3. Analyzing data 4. Preparing material evidence from the data – this stage may not occur 5. Destroying all data that is not used as material evidence	The request for receiving traffic data concerns only traffic data within the borders and jurisdiction of the Republic of Bulgaria; it encompasses traffic data by providers operating in Bulgaria; the time period is specified in the request but cannot exceed 12 months (art. 250a, Electronic Communications Act)	No, it does not

				control over the requests for access; The possibility of obtaining traffic data without judicial authorization may be used by the pre-trial proceedings authorities, under the Criminal Procedure Code. In this case, article 250c of the ECA is applicable, not the instructions of the Prosecutor General.			

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

Please, bear in mind that the author considers that the PDPA is not applicable in cases, related to mass surveillance. For specific explanations, please see paragraph 15 of the Report form. The author has added the PDPA and its provisions to the tables below, but as can be seen – the PDPA has no relevance.

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)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*
The SIM Act, Art. 34g (чл. 34ж)	Right to be informed in case of an illegal surveillance. This is done *ex officio* by the National Bureau for Oversight over Special Intelligence Means	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the SIM Act to indicate otherwise
The SIM Act, Art. 15	Judicial control over the request for use of SIMs	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the SIM Act to indicate otherwise The application of special means of surveillance in another country, when the intention is to collect evidence for Bulgarian criminal proceedings, shall take place through an investigation

			order under the law of the Requested Party.
Electronic Communications Act, Art. 250c	Judicial control over the request for access to traffic data	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the Electronic Communications Act to indicate otherwise
Personal Data protection Act (PDPA), Art. 28, para. 1	Right to information whether a person's personal data is collected, the purposes for the collection and the persons who have access to the personal data	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the PDPA to indicate otherwise
Personal Data protection Act (PDPA), Art. 28a	Right to request from the personal data controller to delete, change or block personal data that are not processed in accordance with the PDPA	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the PDPA to indicate otherwise
Personal Data protection Act (PDPA), Art. 38	Right to lodge an application before the Personal Data Protection Commission for violations of the PDPA	Applies to all persons within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the PDPA to indicate otherwise
Personal Data protection Act (PDPA), Art. 39	Right to lodge a complaint before the specific administrative court or the Supreme administrative court for violations of the PDPA and request just satisfaction for damages	Applies to all person within the borders and jurisdiction of the Republic of Bulgaria	The protection applies only inside the country as Bulgarian law applies only within the borders and jurisdiction of the country and there is no provision in the PDPA to indicate otherwise

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*
Control of the Security Services, Use and Employment of Special Intelligence Means and Access to Data under the Electronic Communications	Parlamentary commission	Constitution[29]; Rules of organization and procedure of the National Assembly[30];	Ex post oversight over the security services that can utilize SIMs; oversight over related national security matters; this oversight is regular and ongoing;	13 Members of the National Assembly, elected by the National Assembly to participate in this Parlamentary commission; that is the number of members of the National Assembly listed as members of the Committee[31] during	The commission exercises overall control over the security services in the country; its main functions include inquaries, analysis, issuing recommendations to the National Assembly on related bill propositions; issuing regular reports to

[29] Bulgaria, Constitution of the Republic of Bulgaria, (*Конституция на Република България*), Art. 79, available in Bulgarian at: http://www.parliament.bg/bg/const.

[30] Bulgaria, Rules of organisation and procedure of the National Assembly, (*Правилник за организацията и дейността на Народното събрание*), Art. 15, available in Bulgarian at: http://www.parliament.bg/bg/rulesoftheorganisation.

[31] Bulgaria, Control of the Security Services, Use and Employment of Special Intelligence Means and Access to Data under the Electronic Communications Act Committee, (Комисия за контрол над службите за сигурност, използването и прилагането на специалните разузнавателни средства и достъпа до данните по закона за електронните съобщения),available in Bulgarian at: http://www.parliament.bg/bg/parliamentarycommittees/members/2084

Act Committee (Комисия за контрол над службите за сигурност, използването и прилагането на специалните разузнавателни средства и достъпа до данните по закона за електронните съобщения)				the tenure of the 42nd National Assembly; number of staff members is still 5;	the National Assembly regarding the funtioning and status of the security services; overall, the power of the commission are not particularly well defined;, as its authority and powers are not well defined[32];
National Bureau for Control over Special Intelligence Means (Национално бюро за контрол на специалните разузнавателни средства)	Independent institution whose members are appointed by the National Assembly	Special Intelligence Means Act, Art. 34b (34б)	Both ex ante and ex post; the oversight is ongoing	5 permanent members, appointed by the National Assembly; 14 staff members[33]	The national bureau issues legally binding recommendations to the relevant security services regarding the application, collection, storage and destruction procedures for SIMs; on request has access to all relevant documentation about application, collection,

[32] Council of Europe, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Inf/DH%282013%297&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864.

[33] Bulgaria, Legal World (Правен свят (2014), "The chairman of the Burgas Regional court is an example for responsibility in granting permission for use of SSM" („Председателят на ОС-Бургас е еталон за отговорност при разрешаването на СРС"), 21.07.2014, available in Bulgarian at: http://www.legalworld.bg/37840.predsedateliat-na-os-burgas-e-etalon-za-otgovornost-pri-razreshavaneto-na-srs.html.

					storage and destruction of SIMs[34]; the National Bureau creates the forms to which all data registries regarding SIMs within the relevant services should abide;
All regional courts	Judicial institutions	Special Intelligence Means Act, Art. 15	Ex ante oversight; this oversight is regular and ongoing;	-	The chairpersons of the regional courts decide whether to approve a request for the use of SIMs or not;
All regional courts	Judicial institutions	Electronic Communications Act, art. 250c	Ex ante oversight; this oversight is regular and ongoing;	-	The chairpersons of the district courts decide whether to approve a request for access to traffic data
All administrative courts/ the Supreme administrative court	Judicial institutions	Personal Data Protection Act, Art. 39	Ex post oversight; this oversight is regular and ongoing		The courts rule whether there has been a violation of the PDPA and award just satisfaction when a complaint is lodged before them

[34] The National Bureau has access only to the documentation regarding the destruction of SSM primary data carriers but not to the carriers themselves; Art. 34f, The SSMA;

Personal Data Protection Commission	Special jurisdiction	Personal Data Protection Act, Art. 39	Ex post oversight; this oversight is regular and ongoing	5 members, appointed by the National Assembly	The commission rules whether there has been a violation of the PDPA when an application is lodged before it

Annex 3 – Remedies[35]

Special Intelligance Means Act				
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**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collecting data	No	No	-	-
Storing data	No	No	-	-
Analyzing data	No	No	-	-
Preparing material evidence from the data	Yes, but only if this stage occurs	Yes, as a part of the criminal charge against him	-none	-none
Destruction of data not used as a material evidence	No	No	-	-

[35] In case of different remedial procedures please replicate the table for each legal regime.

After the whole surveillance process has ended	Yes, but only if the surveilance has been illegal, as per Art. 34g, the SSM Act;	No, as there is no existing mechanism to allow persons to check whether he/she has been surveiled;	Lawsuit for compensation for the use of illegal surveilance under Art. 2, para.1, point 7 of the State and Municipal Liability Act; the complaint is filed before a civil court; the subject is notified *ex officio* by the National bureau	Illegal surveillance under Art. 2, para.1, point 7 of the State and Municipal Liability Act
Electronic Communications Act				
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**
Collecting data	No	No	-	-
Storing data	No	No	-	-
Analyzing data	No	No	-	-
Preparing material evidence from the data	Yes, but only if this stage occurs	Yes, as a part of the criminal charge against him	-	-
Destruction of data not used as a material evidence	No	No	-	-
After the whole surveillance process has ended	No	No	-	-
Personal Data Protection Act				

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
Collecting data	No	No	-	-
Storing data	No	No	-	-
Analyzing data	No	No	-	-
Preparing material evidence from the data	No	No	-	-
Destruction of data not used as a material evidence	No	No	-	-
After the whole surveillance process has ended	No	No	-	-

Annex 4 – Surveillance-related case law at national level

No important caselaw, regarding redress mechanisms for illegal use of SIMs has been identified in the data base of the Supreme Cassation Court or the Supreme Administrative Court. The steps taken include as thorough as possible search in the data base of the SCC. It appears that no lawsuit has been initiated of the Snowden revelations.

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	
Decision date	
Reference details (type and title of court/body; in original language and English [official translation, if available])	
Key facts of the case (max. 500 chars)	
Main reasoning/argumentation (max. 500 chars)	

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	

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**
Control of the Security Services, Use and Employment of Special Intelligence Means and Access to Data under the Electronic Communications Act Committee (Комисия за контрол над службите за сигурност, използването и прилагането на специалните разузнавателни	Parliament	1169 Sofia, пл. "Княз Александър I" №1, зала 242 **Телефон:** (02) 939 32 01; 9810965; **Факс:** (02) 939 36 43	http://www.parliament.bg/bg/parliamentarycommittees/members/2084/info

средства и достъпа до данните по закона за електронните съобщения)			
National Bureau for Control over Special Surveillance Means (Национално бюро за контрол на специалните разузнавателни средства)	Independent state organization		
State Agency "National Security" (Държавна агенция „Национална сигурност")	Government organization (law enforcement and national security)	**State Agency for National Security**, 45 Cherni vrah Blvd., 1407 Sofia, Bulgaria	http://www.dans.bg/en
Ministry of the Interior (Министерство на вътрешните работи)	Government organization (law enforcement and national security)	Sofia 1000 29, Shesti Septemvri Str. +35929825000 - Central MoI	http://www.mvr.bg/en/default.htm
State agency "Technical operations" (Държавна агенция	Government organization (law enforcement and national security)		

"Технически операции)			
Ombudsperson of the Republic of Bulgaria (Омбудсман на Република България)[36]	Public authority	1202 Sofia, 22 "George Washigton" str.	www.ombudsman.bg
Eurorights Association (Асоциация за европейска интеграция и права на човека)	Private sector, Civil society organization;	4000, Plovdiv, 2, Han Kubrat, Str, fl.3tel/fax +359 32/62 32 64; +359 32/26 40 97e-mail: hurights@mail.bg	www.eurorights-bg.org
Bulgarian Helsinki Committee (Български Хелзинкски Комитет)	Private sector; Civil society organization;	**Central office** 7 Varbitsa Street 1504 Sofia BULGARIA**Tel.:**++359 2 943 4876, ++359 2 944 0670, +3592 943 4405**Fax:**++359 884 185 968**E-mail:** bhc@bghelsinki.org	http://www.bghelsinki.org/en/
Access to Information Programme (Програма достъп до информация)	Private sector; Civil society organization;	**bul. Vasil Levski 76 floor 3; apt. 3, Sofia 1142, Bulgaria**	http://www.aip-bg.org/en/

[36] The function of the Ombudsperson is extremely limited. The Ombudsperson acts as an intermediary between the applicant and the public authority. The Ombudsperson can signal public authorities for potential violations of people's rights and freedoms. The Ombudsperson can issue recommendations.

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources *(in accordance with FRA style guide)***:

1. Government/ministries/public authorities in charge of surveillance

Control of the security services, use and employment of special surveillance means and access to data under the electronic communications act committee, Bulgaria (2014), regular reports of the committee, available in bulgarian at: http://www.parliament.bg/bg/parliamentarycommittees/members/2084/reports

Tzvetelin Iovchev, Minister of Interior, Bulgaria (2014), "Tzvetelin Iovchev: For a long time i haven't allowed any SSMs" (Цветлин Йовчев: От много време не разписвам СРС-та), Труд, 30.05.2014, available in bulgarian at: http://www.trud.bg/Article.asp?ArticleId=4111775

Tzvetelin Iovchev, Minister of Interior, Bulgaria (2013), "Tzvetelin Iovchev reveals misuse of SSMs" (Цветлин Йовчев разкрива злоупотребите със СРС-та), iNews, 25.10.2013, available in bulgarian at: http://www.livenews.bg/cvetlin-jovchev-razkriva-zloupotrebite-sys-srs-ta-47558.html

Sotir Tzatzarov, Attorney General, Bulgaria, Georgieva, I. (2013), "Tzatzarov wants a joint SSM register" (Цацаров иска единен регистър на СРС-та), iNews, 14.05.2013, available in bulgarian at: http://inews.bg/%D0%A6%D0%B0%D1%86%D0%B0%D1%80%D0%BE%D0%B2-%D0%B8%D1%81%D0%BA%D0%B0-%D0%B5%D0%B4%D0%B8%D0%BD%D0%B5%D0%BD-%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%8A%D1%80-%D0%BD%D0%B0-%D0%A1%D0%A0%D0%A1-%D1%82%D0%B0_l.a_i.288059.html

Sotir Tzatzarov, Attorney General, Bulgaria (2013), "As a judge Tzatzarov was mislead by Roman Vasilev for use of SSMs" (Като съдия Цацаров бил подведен от Роман Василев за използване на СРС-та), 24 часа, 11.04.2013, available in bulgarian at: http://www.24chasa.bg/Article.asp?ArticleId=1912174

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

   Boyko Rashkov, Chairman of the National bureau, Bulgaria (21014), Bulgarian National Television (Българска Национална Телевизия), 02.01.2014, available in Bulgarian at: http://bnt.bg/part-of-show/kak-se-kontrolirat-srs

   Konstantin Penchev, Ombudsman of the Republic of Bulgaria, Bulgaria (2013) Legal World, (Civil oversight over the use of SSMs is necessary" (Трябва граждански контрол върху прилагането на СРС), Правен свят, 17.04.2013, available in Bulgarian at: http://www.legalworld.bg/30539.triabva-grajdanski-kontrol-vyrhu-prilaganeto-na-srs.html

   Supreme Court of Cassation, Bulgaria, Girginova, G. (2014), "Supreme Court of Secession: the implemented restrictions with the Electronic Communications Act on freedom of correspondence and the right of private life are unconditional, wide-ranging and permanent, therefore unconstitutional" (ВКС: Въведените със Закона за електронните съобщения ограничения на неприкосновеността на личния живот и свободата на кореспонденцията са безусловни, всеобхватни и постоянни, поради което са конституционно нетърпими), Съдебни репортажи, 08.07.2014, available at: http://judicialreports.bg/2014/07/%D0%B2%D0%BA%D1%81-%D0%B2%D1%8A%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%82%D0%B5-%D1%81%D1%8A%D1%81-%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B0-%D0%B7%D0%B0-%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD/

3. Non-governmental organisations (NGOs)

   Alexander Kashamov, **Access to information Programme,** Bulgaria (2013), "Where will lead us the debate about surveillance?" (Докъде ще ни доведе дебатът за подслушванията?), available in Bulgarian at: http://www.aip-bg.org/publications/newsletter+print.php?NewsletterID=103966&ArticleID=1000532927

   Mihail Ekimdziev, **Eurorights Association** , Bulgaria (2013), (Analysis of the correspondence between the right to private life under Art. 8 of the European Convention of Human Rights and the national legal framework for use of special means" (Анализа за съответствието между правото на личен живот по чл.8 от Конвенцията за защита правата на човека и основните свободи и националната правна уредба на използването на специални разузнавателни средства), 9.12.2013, available in Bulgarian at: http://eurorights-bg.org/?p=790

4. Academic and research institutes, think tanks, investigative media report.

Videv, D., Bulgaria (2013), "26% more requests for use of SSMs by the Ministry of Interior in 2011" (26 % повече са исканията на МВР за СРС-та през 2011 година), Bulgarian National Radio (BNR) (*Българско национално радио, БНР*), 12.10.2013, available in Bulgarian at: http://bnr.bg/archive/Horizont/Politics/Bulgaria/2012/10/Pages/1210SRS.aspx

Tsonev, D., Bulgaria (2013), "For another year there is an increase in the number of requests for SSMs by the Ministry of Interior" (МВР за поредна година бележи ръст в исканите СРС) *Правен свят*, 14.03.2013, available in Bulgarian at: www.legalworld.bg/30168.mvr-za-poredna-godina-beleji-ryst-v-iskanite-srs.html