National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

LATVIA

Version of 3 December 2014

Latvian Centre for Human Rights

Summary

[1]. The legal basis for conducting investigatory operations measures is prescribed by the Constitution of the Republic of Latvia (*Satversme*), Criminal Procedure Law (*Kriminālprocesa likums*), Investigatory Operations Law (*Operatīvās darbības likums*), other laws and international acts binding upon Latvia, which regulate the tasks, rights and obligations of state authorities responsible for the protection of national security, defence, economic sovereignty and public order. There is no special legislation governing non-suspicion based large scale operations by intelligence authorities in Latvia and there has been no indication that this is being conducted. There is no definition of mass scale surveillance anywhere in the legislation.

[2]. In accordance with the above legislation national intelligence agencies which have the right to conduct investigatory operations measures are, among others, the Constitutional Protection Bureau (*Satversmes aizsardzības birojs*), Security Police (*Drošības policija*) and Military Intelligence and Security Service (*Militārās izlūkošanas un drošības dienests*). The investigatory operations measures shall be performed in accordance with the general and special method. Investigatory operations measures in the course of which there is significant infringement of the constitutional rights of persons shall be conducted in accordance with special method.[1] In accordance with the Investigatory Operations Law a total of 13 different state bodies have the right to perform investigatory operations. In addition to the three intelligence agencies, these also include the Office for the Prevention of Combating Corruption, the State Police, Customs Police of the State Revenue Service, etc. [2] The main goals of surveillance are (1) the protecting of persons against criminal threats, (2) preventing, deterring and detecting of criminal offences, and the determining of persons committing criminal offences and the sources of evidence, (3) searching for certain persons, (4) obtaining, accumulating, analysing and utilising, in accordance with procedures prescribed by law, of political, social, military, economic, scientific and technical, criminal, and other information related to the criminal sphere and its infrastructure, and threats against State security, defence and economic sovereignty, (5) the protecting of official secrets and other interests important to the State.

[3]. In accordance with Article 7 of the Investigatory Operations Law, operative control of correspondence, acquisition of information via technical means, tapping of non-public conversations (over the telephone, electronic, or other means of communication) and investigatory entry may only be undertaken with the approval of the Chairman of the Supreme Court or his/her designated Supreme Court judge. Permission for these activities may be issued for a period of up to three months and may in the event of justified necessity be prolonged, but only as long as the relevant proceedings concerning the person are active. In exceptional cases, when there is a need to act without delay to prevent a threat to vital public interests, such as an act of terrorism or subversive activity, a murder or other serious crime, or if there is actual threat to the life, health, or property of a person, the above activities can be initiated without the judge's approval. The prosecutor must be notified within 24 hours and the judge's approval received within 72 hours. If the officers fail to do so, tapping must be terminated.[3] However, for one of the technical means (video control of

1 Latvia, Investigatory Operations Law (Operatīvās darbības likums), 16.12.1993, Section 7, available in Latvian at http://likumi.lv/doc.php?id=57573, published in "Latvian Herald", 131, 30.12.1993., "Ziņotājs", 1, 13.01.1994, at https://www.vestnesis.lv/?menu=doc&id=57573

2 Latvia, Investigatory Operations Law (Operatīvās darbības likums), 16.12.1993, Chapter 4, available in Latvian at http://likumi.lv/doc.php?id=57573, published in "Latvian Herald", 131, 30.12.1993., "Ziņotājs", 1, 13.01.1994, at https://www.vestnesis.lv/?menu=doc&id=57573

3 Latvia, Investigatory Operations Law (Operatīvās darbības likums), 16.12.1993, Section 17, available in Latvian at http://likumi.lv/doc.php?id=57573, published in "Latvian Herald", 131, 30.12.1993., "Ziņotājs", 1, 13.01.1994, at https://www.vestnesis.lv/?menu=doc&id=57573

non-public environment) a permission must be issued by the prosecutor, as a simple notification to him will not sufficient.

[4]. In line with the (now invalidated) Data Retention Directive 2006/24/EC Electronic Communications Law requires the providers of electronic communications to retain "storable data" for a period of 18 months. These data include data about callers and their telephone numbers, recipients and their telephone numbers, and mobile phone identifiers and location data.[4] According to the law, providers of electronic communications shall provide these data to the pre-trial investigatory institutions, to the subjects carrying out investigative activities, to state security institutions, prosecutor's office, and court, if these institutions request it.[5]

[5]. The data are requested by intelligence/security agencies and other bodies specified by law by sending a request to the provider of electronic communications by indicating the legal basis (in order to protect national and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings and also in order to ensure the protection of the rights and legal interests of the individual infringed online in the civil cases), scope, type of retained data to be provided/accessed and the time for the providing of a response. Electronic communications providers are required to annually submit information to the Data State Inspectorate *(Datu valsts inspekcija*) on institutions that have requested the data.[6] The Data State Inspectorate compiles the information within the period of two months and forwards it to the European Commission[7].

[6]. According to Article 29 of the Personal Data Protection Law[8], the supervision of protection of personal data is carried out and the complaints regarding the protection of personal data are reviewed by the Data State Inspectorate (DSI) except cases when personal data has been recognized as an object of an official secret. DSI fulfils the functions specified in legislative acts, takes decisions and issues administrative acts in accordance with the law. DSI has the right to require that data be blocked, that is incorrect or unlawfully obtained data be erased or destroyed, or to order a permanent or temporary prohibition of data processing; to bring an action in court for violations of this Law; to impose administrative penalties according to the procedures specified by law regarding violations of personal data processing. DSI is entitled to perform inspections in order to determine the conformity of personal data processing to the requirements of legislative acts in cases where the system administrator has been prohibited by law to provide information to a data subject and a relevant submission has been received from the data subject.

4 Latvia, Electronic Communications Law (Elektronisko sakaru likums), 28.04.2004, Section 19 Part 1 11), available in Latvian at http://likumi.lv/doc.php?id=96611, published in "Latvijas Vēstnesis", 183 (3131), 17.11.2004., "Ziņotājs", 23, 09.12.2004, available in https://www.vestnesis.lv/?menu=doc&id=96611

5 Latvia, Electronic Communications Law (Elektronisko sakaru likums), 28.04.2004, Section 71.[1] part 1, available in Latvian at http://likumi.lv/doc.php?id=96611, published in "Latvijas Vēstnesis", 183 (3131), 17.11.2004., "Ziņotājs", 23, 09.12.2004, available in https://www.vestnesis.lv/?menu=doc&id=96611

6 Latvia, Cabinet of Ministers Regulations Nr 820 of 4 December 2007 „On Procedure How Pre-trial Institutions, Subjects of Investigatory Operations, State Security Institutions, Prosecutor's Office and Court Request and Electronic Communications Providers transfers Storable Data as Well as Procedure How Statistics is Compiled about Requests for Storable Data and their Issuance" (Ministru kabineta 2007.gada 4.decembra noteikumu Nr.820 "Kārtība, kādā pirmstiesas izmeklēšanas iestādes, operatīvās darbības subjekti, valsts drošības iestādes, prokuratūra un tiesa pieprasa un elektronisko sakaru komersants nodod saglabājamos datus, kā arī kārtība, kādā apkopo statistisko informāciju par saglabājamo datu pieprasījumiem un to izsniegšanu"), 04.12.2007, Section 6 & 12, available in Latvian at http://likumi.lv/doc.php?id=167539, published in "Latvijas Vēstnesis", 197 (3773), 07.12.2007, available at https://www.vestnesis.lv/?menu=doc&id=167539

7 Ibid., Section 13.

8 Latvia, Physical Person Data Protection Law (Fizisko personu datu aizsardzības likums), 23.03.2000, Section 29, http://likumi.lv/doc.php?id=4042, published in Latvijas Vēstnesis 06.04.2000., Nr.123/124 (2034/2035) at https://www.vestnesis.lv/?menu=doc&id=4042

[7]. If the personal data has been classified as an official secret object and either of national intelligence services (for example The Constitution Protection Bureau, the Military Intelligence and Security Service, and the Security Police) or the official of the national intelligence service, which work is related to the processing and using of official secrets in direct way, might have committed a violation in scope of personal data protection or processing, then according to Article 6 of the law On State Security Institutions and to Article 5 of the Investigatory Operations Law a person is entitled either to submit a complaint (about activities of the intelligence service or the official of the national intelligence service) to the prosecutor who, after completing an examination, provides an opinion with respect to the conformity of activities with the law, or to bring an action to a court.

[8]. According to law[9] all the information, including information about personal data, which is obtained during investigatory operations, is classified as a restricted access information or as an official secret. The list of information and other objects recognised as objects of official secrecy, and the scope and content thereof prescribe Cabinet Regulations No 887 "The List of Official Secret Objects", adopted 26 October 2004. According to these Regulations for example such kind of information has been prescribed as an official secret: the information about staff and personnel working in national security authorities, the National Armed Forces and the institutions of the system of the Ministry of the Interior; the identity of those officials conducting the investigatory detective work by getting involved in criminal circles; information regarding the identity of covert assistants located in foreign states or in Latvia.

[9]. In accordance with Article 25 of the law On State Security Institutions and Article 34 of the Investigatory Operations Law, the National Security Committee (*Nacionālās drošības komisija*) of the *Saeima* exercises parliamentary control over national security institutions. It hears reports and overviews by the heads of national security agencies (about the work of national security agencies) and by the heads of the investigatory operations institutions, considers results from the supervision of the activities of these agencies, reviews working documents and information of these agencies, except documents on sources of confidential information. The Cabinet of Ministers controls activities of state security institutions within the scope of its competence and receives annual reports on the results of investigatory operations and statistical data. Some sections of the annual reports are public and some are confidential and in separate cases if there is essential information on threats to national security or public order – an interim report ,[10] which is not public.

[10]. The Prosecutor General and public prosecutors specifically authorised by him or her carry out supervision over the processes of investigatory operations, intelligence and counterintelligence of State security institutions and the official secret protection system. In performing supervision they have the right to examine documents, materials and information at any stage of investigatory operations as is available to the investigatory operations institutions. Covert information and its sources may be revealed only to the Prosecutor General, but to the prosecutors specially authorised by the Prosecutor General – only with the approval of the head of the investigatory operation institution.

9 Latvia, Investigatory Operations Law (Operatīvās darbības likums), 16.12.1993, Article 24, part one, available in Latvian at http://likumi.lv/doc.php?id=57573, published in "Latvian Herald", 131, 30.12.1993., "Ziņotājs", 1, 13.01.1994, at https://www.vestnesis.lv/?menu=doc&id=57573

10 Latvia, Cabinet of Ministers Instruction Nr of 22 June 2007 „On the Procedure How the Cabinet of Ministers controles the fulfillment of tasks by institutions of investigatory operations (Ministru kabineta 2007.gada 12.jūnija instrukcija Nr.10 "Kārtība, kādā Ministru kabinets kontrolē operatīvās darbības subjektu uzdevumu izpildi"), 12.06.2007, available at http://likumi.lv/doc.php?id=158968, published in "Latvijas Vēstnesis", 97 (3673), 19.06.2007 at https://www.vestnesis.lv/?menu=doc&id=158968

[11]. The right to inviolability of one's private and family life, home and correspondence is protected by the Constitution,[11] and international human rights instruments binding upon Latvia. The right to one's private life is protected by Criminal Law which foresees criminal liability for unlawful activities with personal data, liability of officials for exceeding official authority or using official position in bad faith abuse of authority by officials.[12] In scope of the protection of private life, the Criminal Law foresees criminal liability for unlawful activities such as the entry in the property and secrets of a person, such as its correspondence and data.

[12]. However, the right may be subject to certain restrictions only for legitimate purposes the objectives of which are the protection of the life and health, rights and freedoms, honour, dignity and property of persons and the safeguarding of the Constitution, the political system, national independence and territorial integrity, the capabilities of the State regarding defence, the economy, science and technology, and State official secrets, against external and internal threats.

[13]. In accordance with Article 13 of the Physical Person Data Protection Law, a system administrator is obliged to disclose personal data in cases provided for by law to officials of state and local government institutions.

[14]. Any person if their personal data are inaccurate, outdated, false, have been obtained unlawfully or are not necessary for the purpose of personal data processing have the right to demand that they are updated, rectified or erased in a timely manner.[13] A data subject has the right to obtain all information that has been collected concerning himself or herself in any system for personal data processing, unless the disclosure of such information is prohibited by law in the field of national security, defence, public order, and criminal law.[14]

[15]. According to Section 24 of the Investigatory Operations Law information obtained in the course of investigatory operations measures shall be classified as restricted access information or a state secret object.

[16]. If information or measures undertaken during investigatory operations are classified as a state secret, the person has no right to get acquainted or verify the information. However, if the person under observation believes that his or her lawful interests and freedoms have been violated, the person has the right to either submit a complaint to the prosecutor, who after a review issues a compliance statement, or submit a claim in court. [15]

[17]. A person may request the issuance of restricted access information if he/she has substantiated his/her request and indicated the purpose for the use of such information. [16] If

---

11 Latvia, Republic of Latvia Constitution (Latvijas Republikas Satversme), Section 96 Everyone has the right to inviolability of his or her private life, home and correspondence.

12 Latvia, Criminal Law (Krimināllikums), 17.06.1998, Section 145, 317, 318, available in Latvian at http://likumi.lv/doc.php?id=88966, published in „Latvijas Vēstnesis" 08.07.1998., Nr.199/200 (1260/1261, at https://www.vestnesis.lv/?menu=doc&id=88966

13 Latvia, Physical Person Data Protection Law (Fizisko personu datu aizsardzības likums), 23.03.2000, Section 10 para 1 4), http://likumi.lv/doc.php?id=4042, published in Latvijas Vēstnesis 06.04.2000., Nr.123/124 (2034/2035) at https://www.vestnesis.lv/?menu=doc&id=4042

14 Ibid, Section 15.

15 Latvia, Investigatory Operations Law (Operatīvās darbības likums), 16.12.1993, Article 5, available in Latvian at http://likumi.lv/doc.php?id=57573, published in "Latvian Herald", 131, 30.12.1993., "Ziņotājs", 1, 13.01.1994, at https://www.vestnesis.lv/?menu=doc&id=57573; Latvia, Law On State Security Institutions (Valsts drošības iestāžu likums), 19.05.1994, Article 6, available in Latvian at http://likumi.lv/doc.php?id=57256, published in "Latvian Herald", 59 (190), 19.05.1994.

16Latvia, Freedom of Information Law (Informācijas atklātības likums), 29.10.1998, Section 11 Part 4, in Latvian at http://likumi.lv/doc.php?id=50601, published in Latvijas Vēstnesis > 06.11.1998., Nr.334/335 (1395/1396) at https://www.vestnesis.lv/?menu=doc&id=50601

the institution refuses to provide the information the refusal can be appealed in court according to the procedure specified by the Administrative Procedure Law. [17]

[18]. Discussions have been under way for several years to significantly amend the Investigative Operations Law or draft a completely new law as certain provisions are outdated and do not meet human rights standards. On 24 April 2014 amendments to the law were approved at the Meeting of State Secretaries (the first of three stages of legislative approval by the government) [18]. The amendments foresee a new Section 23.[1] which provides for a more detailed procedure for the receipt of the approval by judge and prosecutor for the conducting of investigatory operations measures. They also foresee a new Article 24.[1] which provides that upon completing investigatory operations measures (e.g. wiretapping, video surveillance) the institution carrying out investigatory operational measure shall inform the person who was subject to special investigatory techniques, time when it was carried out in respect of that person. The amendments list conditions when provision of such information is to be restricted. They also specify reporting and review procedures concerning the investigatory operations measures approved by the prosecutor and judge as well as detail the control of activities of officials of investigatory operations institutions upon receipt of individual complaint. After the approval by the government, the amendments will further require the parliamentary approval in three readings.

17 Ibid, Section 15.

18 Latvia, Draft Law “Amendments to the Investigatory Operations Law”’ (Likumprojekts "Grozījumi Operatīvās darbības likumā") 24,04,2014, available in Latvian at http://tap.mk.gov.lv/doc/2014_05/IEMLik_07042014_GrozODL.758.doc

Annex 1 – Legal Framework relating to mass surveillance

There is no non-suspicion based and indiscriminate surveillance of the entire population of large population groups. There are neither legislative provisions, nor any evidence of that being carried out.

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)?**
Investigatory Operations Law (*Operatīvās darbības likums*)	Persons of whom there are reasonable grounds to believe that they are in preparation of a criminal offence or have been committed, or a threat to interests of importance to the State. The law does not	- the protecting of official secrets and other interests important to the State; - obtaining, accumulating, analysing and utilising, in accordance with procedures prescribed by law, of political, social,	Protection of the life and health, rights and freedoms, honour, dignity and property of persons and the safeguarding of the Constitution, the political system, national independence and territorial integrity, the capabilities of the	For conducting investigatory operations measures requiring special method (operative control of correspondence, acquisition of information via technical means, tapping of non-public conversations (over the telephone, electronic, or other means of	Investigatory operations institutions are entitled to collect, systematise, analyse, store and record official legal and secret information with respect to persons, facts, events and things (in the form of passive records) that are necessary and are significant for the	up to three months and may, in the event of justified necessity be prolonged, but only as long as the relevant proceedings concerning the person are active.	The law does not envisage it.

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)?
	provide for non-suspicion based large scale surveillance	military, economic, scientific and technical, criminal, and other information related to the criminal sphere and its infrastructure, and threats against State security, defence and economic sovereignty the protecting of persons against criminal threats.	State regarding defence, the economy, science and technology, and State official secrets, against external and internal threats.	communication) approval of the Chief Justice of the Supreme Court or a Justice of the Supreme Court specially authorised by him or her. The law does not provide for non-suspicion mass surveillance.	performing of their tasks with respect to investigatory operations and criminal procedure. The inclusion of persons in investigatory records (active form of records) is permitted only if investigatory process is being conducted with respect to them. If information on the basis of which a person is included in an investigatory record is not confirmed, such person shall be removed from the record.		
Law on Electronic Communications	A person who		Information can	There is no need	There are no such	Electronic	

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)?
(*Elektronisko sakaru likums*)	has entered into a contract with an electronic communications service provider regarding the receipt of specific electronic communications services.	If there are reasonable doubts that person is acting against national security or is involved in criminal offences.	be carried out in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings; in order to ensure the protection of the rights and legal interests of the individual infringed in the electronic environment in the civil cases.	for previous approval or a warrant.	steps.	Communications Law requires the providers of electronic communications to retain "storable data" for a period of 18 months.	The law does not envisage it.

B- Details on the law providing privacy and data protection safeguards against mass 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)**
Latvijas Republikas Satversme (*The Constitution of the Republic of Latvia*)	Everyone has the right to inviolability of his or her private life, home and correspondence.	The Constituton of the Republic of Latvia is binding on any person.	The Constituton of the Republic of Latvia is binding on any person.
Personal Data Protection Law (*Fizisko personu datu aizsardzības likums*). The purpose of this law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of	The rights of data subject to protection of his or her personal data are defined in Personal Data Protection Law (article 15.-20.). A data subject has the right to obtain all information that has been collected concerning himself or herself in any personal data processing system. A data subject has the right to obtain information concerning those natural or legal persons who within a prescribed time period have received information from a	Any data subject whose data are processed by a data controller established in Latvia.	The law applies to the processing of all types of personal data if: 1) the system administrator is registered in the Republic of Latvia; 2) data processing is performed outside the borders of the Republic of Latvia in territories, which belong to the Republic of Latvia in accordance with international agreements; and 3) in the territory of the Republic of

private life, with respect to the processing of data regarding natural persons.	data controller concerning this data subject. In the information to be provided to the data subject, it is prohibited to include State institutions, which administer criminal procedures, investigatory operations authorities or other institutions concerning which the disclosure of such information is prohibited by law. A data subject has not the right to receive the information, if it is prohibited to disclose such information in accordance with the law in the field of national security, State protection, public security, criminal law, as well as with a view to ensure the State financial interests in the tax affairs or supervision of participants of the financial market and macroeconomic analysis. A data subject has the right to request that his or her personal data be supplemented or corrected, as well as that their processing be discontinued or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected. If the data subject is able to substantiate that the personal data		Latvia is located equipment, which is utilised for the processing of personal data.

	are incomplete, outdated, false, unlawfully processed or no longer necessary for the purposes for which they were collected, the data controller has an obligation to rectify this inaccuracy or violation without delay and notify third persons who have previously received the processed data of such. If a data controller fails to comply with the obligations laid down in Personal Data Protection Law, a data subject has the right to appeal to the Data State Inspectorate the refusal of a data controller to provide the information referred in this Law or perform the activities referred in this Law, appending the documents attesting that the data controller refuses to comply with or fails to comply with the obligations laid down in the Law. In case of unlegal processing of a natural person's data the administrative liability might arise according to Latvian Administrative Violations Code. In some cases might arise also criminal liability, for example - arbitrary accessing automated data processing systems.		
The Investigatory	If investigatory operations	The law is binding to every person	The law is binding to the whole

Operations Law (*Operatīvās darbības likums*)	measures significantly infringe the constitutional rights of persons, investigatory operations shall be conducted in accordance with the special method, which means that a body performing investigatory operations shall get the approval of the Chairman of the Supreme Court or his/her designated Supreme Court judge. Special method includes operative control of correspondence, acquisition of information via technical means, tapping of non-public conversations (over the telephone, electronic, or other means of communication), video control of non-public environment and entry in object using special measures.	who is in the territory of Republic of Latvia (citizens of LR, non-citizens, stateless persons, foreigners).	territory of Republic of Latvia.

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
The *Saeima*/ Saeima	A parliament of Republic of Latvia.	Law On State Security Institutions, Investigatory Operations Law.	Parliamentary control	100 deputies	Carries out parliamentary control over activities of State security institutions.
National Security Committee	After the *Saeima* convenes, it forms this committee, which have one representative from each parliamentary group.	Law On State Security Institutions, Investigatory Operations Law.	Parliamentary oversight	Each political party elected to the *Saeima* is represented in the committee by one member. Currently the Committee consists of five members.	Carries out parliamentary control over activities of State security institutions; Hears the reports and overviews by the heads of national security agencies (about the work of national security agencies) and by the heads of the investigatory operations institutions, considers results from the supervision of the activities of these agencies, reviews working documents and information of these agencies, except documents on sources of confidential information.

Cabinet of Ministers	The highest executive body of Republic of Latvia.	Law On State Security Institutions, Investigatory Operations Law, Cabinet instruction No.10 "Order in which the Cabinet of Ministers controls the implementation of tasks of bodies performing investigatory operations", adopted 12 June 2007.	Control activities of state security institutions within the scope of its competence.	The Cabinet of Ministers consists of 13 ministers and prime minister. Number of staff: N/A.	Controls the implementation of tasks of bodies performing investigatory operations; organises the protection of official secrets in case if the personal data have been declared to be official secret objects; might request an emergency report about threats to national security and public order.
Prosecutor General and prosecutors specially authorised by the Prosecutor General	Prosecutor's Office	The Law On State Security Institutions, Investigatory Operations Law.	Supervision	N/A	Supervision over the processes of investigatory operations, intelligence and counterintelligence of State security institutions and the official secret protection system. When carrying out supervision, the Prosecutor General and public prosecutors specifically authorised by him or her are entitled to get

					acquainted with the documents, materials and information at disposal of State security institutions. Identity of information sources shall be disclosed only in such cases when they are directly involved in committing of a criminal offence, moreover, only to the Prosecutor General, but to public prosecutors specifically authorised by him or her – only upon consent of the head of the State security institution; it is prohibited to disclose the identity of information sources under supervision procedures.
Administrative Court	An appeal body	The Law On State Security Institutions, Investigatory Operations Law, Administrative Procedure Law.	Control of State security institutions	There are 5 District Administrative Courts and 1 administrative Regional Court, and Supreme Court Senate in Administrative Matters	Revises a complaint of a person if a body performing investigatory operations has through its actions infringed the lawful rights and freedoms of the person, evaluates if their conduct is lawful and corresponds to law.

The Data State Inspectorate / Datu valsts inspekcija	The Data State Inspectorate is a direct administration authority under the supervision of the ministry of Justice.	Freedom of Information Law	The supervision of protection of personal data, except cases when personal data has been recognized as an official secret. DSI is also the national supervisory authority carrying out the national supervision of the Schengen information system and monitors the processing of personal data carried out in collaboration with the European Police Office, are complied with laws and regulations of personal data processing conditions.	a total number of staff - 19 employees; a total number of supporting staff – 11; a total number of managing staff – 8. A Director of the Data State Inspectorate accepts visitors once a month (on the second Wednesday of each month) according to the schedule established in advance.	The Data State Inspectorate: - examines the administrative violation matters in the case of the illegal operations with a natural person's data, in the case of failure to provide information specified by the law to a data subject, in the case of the processing of a natural person's data without registration specified by law, in the case of failure to provide the information provided for by the law or the provision of false information to the Data State Inspectorate, in the case of failure to accredit the persons specified by the law at the Data State Inspectorate, in the case of violation of the prohibition on sending commercial information as specified in the law;

					- draws up an administrative violation report; - imposes administrative penalties according to the procedures specified by law regarding violations of personal data processing; - reviews complaints regarding the protection of personal data; - takes decisions and issues administrative acts in accordance with the law.

Annex 3 – Remedies[19]

Investigatory Operations Law				
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.*
Collection*	No	No, because the information obtained in the course of investigatory operations measures is classified as restricted access information or an official secrets	If a person believes that a body performing investigatory operations has through its actions infringed the lawful rights and freedoms of the person, such person is entitled to submit a complaint to a prosecutor who, after conducting an examination,	Unlawful action from bodies performing investigatory operations.

[19] 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

		object.	shall provide an opinion with respect to the conformity to law of the actions of the officials of the body performing the investigatory operations, or the person may bring an action in court. If a person has suffered the harm (also moral injury), a person may initiate civil proceedings.	
Analysis*	No	No	See above	See above
Storing*	No	No	See above	See above
Destruction *	No	No	See above	See above
After the whole surveillance process has ended	No	No	See above	See above
Law On State Security Institutions				
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,*	*Violation of data protection, private life, specific legislation, etc.*

			executive, parliamentary) providing such remedies.	
Collection*	N/a	N/a	If a person believes that State security institutions through their actions have infringed on the lawful rights and freedoms of a person, such person is entitled to submit a complaint to the public prosecutor who, after completing an examination, shall provide an opinion with respect to the conformity of activities of the official of the State security institution with the law, or to bring an action to a court. If a person has suffered the harm (also moral injury), a person may initiate civil proceedings.	Unlawful action from State security institutions.
Analysis*	N/a	N/a	See above	See above
Storing*	N/a	N/a	See above	See above
Destruction*	N/a	N/a	See above	See above
After the whole surveillance process has ended	N/a	N/a	See above	See above

* 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

Law on Electronic Communications				
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.*
Collection*	Yes	No, because the law doesn't provide it.	.An Electronic communications merchant has a duty to ensure the protection of personal data. In case of violation of personal data the electronic communications merchant immediately informs Data State Inspectorate which initiates a review. A person regarding a breach of personal data protection is notified, if it is likely to cause consequences for the person or privacy thereof.	A breach of personal data protection.

* 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

Analysis*	No	No, because the law doesn't provide it.	See above	See above
Storing*	Yes	No, because the law doesn't provide it.	See above	See above
Destruction*	No	No, because the law doesn't provide it.	See above	See above
After the whole surveillance process has ended	No	No, because the law doesn't provide it.	See above	See above
Personal Data Protection Law				
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.*
Collection*	Yes, except: (1) the cases	A data subject has the right to obtain all information that has	A data subject has the right to appeal to the Data State Inspectorate the refusal of a system	The refusal of a system administrator to provide the information, supplement, rectify,

* 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

	related to State institutions, which administer criminal procedeeings, investigatory operations authorities or other institutions concerning which the disclosure of such information is prohibited by law (2) if personal data have not been obtained from the data subject and if personal data have been processed for scientific, historical or statistical research, or the establishment	been collected concerning himself or herself in any system for personal data processing, unless the disclosure of such information is prohibited by law in the field of national security, defence and criminal law.	administrator. Decisions by the Data State Inspectorate may be appealed to a court. If a person has suffered the harm (also moral injury), a person may initiate civil proceedings.	suspend data processing or destroy data. Violation of data protection, private life, home and correspondence.

	of Latvian national archive holdings, (3) the informing of the data subject requires inordinate effort or is impossible (4) if the law (Investigatory Operations Law; Law On Official Secrets; Criminal Procedure Law; Latvian Administrative Violations Code etc.) provides for the processing of personal data without informing the data subject thereof.			
Analysis*	Yes, with	A data subject has the	See above	See above

	above mentioned exeptions	right to obtain information concerning those natural or legal persons who within a prescribed time period have received information from a system administrator concerning this data subject. In the information to be provided to the data subject, it is prohibited to include State institutions, which administer criminal procedures, investigatory operations authorities or other institutions concerning which the disclosure of such information is prohibited by law.		
Storing*	Yes, with above mentioned exeptions	See above	See above	See above
Destruction *	Yes, with above mentioned	See above	See above pluss a data subject has the right to request that his or her personal data be supplemented or	See above

	exeptions		rectified, as well as that their processing be suspended or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully obtained or are no longer necessary for the purposes for which they were collected	
After the whole surveillance process has ended	Yes, with above mentioned exeptions	See above	See above	See above

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.

There have been no law suits initiated and based on the Snowden revelation. However, there were the "Jaunalksne" Criminal case Nr.112812002606 where public officials were prosecuted because of taping telephone conversations of the journalist;

Case title	The claim of Ilze Jaunalksne against the Republic of Latvia (RL), represented by the Ministry of Finances of RL, the State Revenue Service of RL, Financial Department of SRS of RL, about invasion in private life and compensation of moral harm in amount of 300 000 LVL.
Decision date	18 february 2010
Reference details (type and title of court/body; in original language and English [official translation, if available])	Augstākās tiesas Senāta Civillietu departaments/ The Chamber of Civil Cases of the Supreme Court
Key facts of the case (max. 500 chars)	Starting from 7 September 2007, several newspapers and internet portals published excerpts from telephone conversations between a journalist Ilze Jaunalksne and several public officials. The telephone of the journalist was tapped by the public authorities responsible for fighting economic crimes on the basis of permission given by a judge of the Supreme Court. It turned out that there did not exist a valid reason under the law for tapping telephone conversations of the journalist.
Main reasoning/argumentation (max. 500 chars)	The court founded that the Ministry of Finances and the State Revenue Service acted unlawful and didn't comply the requirements of law thus allowing violation of private life. The State of Latvia tolerated that messages containing state secrets - recorded telephone conversations – were accessible in public space, and didn't guarantee the confidentiality of those conversations.

Key issues (concepts, interpretations) clarified by the case **(max. 500 chars)**	The telephone conversations between the applicant and other person and information, which was obtained listening to those conversations during investigatory operations, are an official secret. Illegal disclosure of this kind of information significantly violate applicant's right to respect for private life, home and correspondence.
Results (sanctions) and key consequences or implications of the case **(max. 500 chars)**	The Chamber of Civil Cases of the Supreme court partially satisfied the claim in the case of Ilze Jaunalksne against the Republic of Latvia about interference in private life and compensation of moral harm, recovered from the Republic of Latvia in person of the State Revenue Service 12 000 LVL (appr.17 000 EUR) and costs in amount of 306.40 LVL (appr.436 EUR). In the rest part claim of I. Jaunalksne was rejected.

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.

There are no academic institutions or non-governmental organisations working in this area in Latvia.

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**
Satversmes aizsardzības birojs/Constitutional Protection Bureau	state security service	Miera iela 85a, Riga, LV-1013, Latvia Phone : 67025404 Fax : 67025406 E-mail: info@sab.gov.lv	www.sab.gov.lv
Drošības policija/Security Police	state security service	Kr. Barona iela 99a, Riga, LV-1012, Latvia Phone: 67208991 (assistant to Chief of Security Service)	No website, general website of Ministry of Interior http://www.iem.gov.lv/lat/drosibas_policija/drosibas_policijas_darbiba/

		Fakss: 67273373 E:mail: kanc@dp.gov.lv	
Militārās uzlūkošanas un drošības dienests/Military Intelligence and Security Service	state security service	Grostonas iela 2, Rīga, LV-1013, Latvia Telephone: +371 67177877 Fax: +371 67177878 E-mail: kanceleia@midd.gov.lv	http://www.midd.gov.lv/MIDD/Par_mums.aspx
Nacionālās drošības komisija/National Security Commission	parliament	Jēkaba iela 11, Rīga, LV-1811, Latvia Phone: 6708 7251 e–mail: drosibas.komisija@saeima.lv	Main webpage of parliament http://www.saeima.lv/lv/par-saeimu/saeimas-darbs/komisijas
Ģenerālprokuratūra/Office of the Prosecutor General	Prosecutor's office	Kalpaka bulvāris 6, Rīga, LV-1801, Latvia E-mail: Gen@lrp.gov.lv Phone: 67044400 Fax: 67044804	http://www.prokuratura.gov.lv/public/30225.html
Datu Valsts Inspekcija / The Data State Inspectorate	a state administration institution	Blaumana iela 11/13-15, Riga, LV-1011, Latvia Phone. : 67 22 31 31 Fax : 67 22 35 56 E-mail : info@dvi.gov.lv	http://www.dvi.gov.lv/en/
LR Advokātu kolēģija/ Latvian Council of Sworn Advocates	Bar	Brīvības boulevard 34, Riga, LV1050, Latvia Fax: +371 67358488 E:mail: adv-pad@latnet.lv	http://www.advokatura.lv

Defence Intelligence and Security Service	Public Authority	Email: kanceleja@midd.gov.lv	

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

   SAB (Satversmes aizsardzības birojs) (2013). Annual Report of the Activities of the Constitutional Protection Bureau (SAB 2013.gada darbības pārskats), 11 p., available in Latvian at http://www.sab.gov.lv/downloads/2013_parskats.pdf

   SAB (Satversmes aizsardzības birojs) (2012).). Annual Report of the Activities of the Constitutional Protection Bureau (SAB 2012.gada darbības pārskats), http://www.sab.gov.lv/index.php?lang=lv&page=3&sid=10&nid=303

   DP (Drošības policija) (2013). 2013 Annual Report of the Security Police, available in Latvian at http://www.iem.gov.lv/files/text/DPpaarskats.pdf

   DP (Drošības policija) (2012). 2012 Public Report of the Activities of the Security Police (Drošības policijas 2012.gada darbības publiskais pārskats). Available in Latvian at http://www.iem.gov.lv/files/text/DP_2012(2).pdf

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:

- Data State Inspectorate (Datu Valsts inspekcija) (2009). Recommendations of the Data State Inspectorate "Data Processing in the Realm of Video Surveillance" (*Datu valsts inspekcijas rekomendācija „Datu apstrāde videonovērošanas jomā"*), available in Latvian at http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_videonoverosana.pdf

- Data State Inspectorate (Datu Valsts inspekcija) (2010). Recommendations of the Data State Inspectorate "Personal Data Processing in Online Social Networks" (*Datu valsts inspekcijas rekomendācija "Personas datu apstrāde tiešsaistes sociālajos tīklos"*), available in Latvia at http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/rekomendacija_soc.pdf

- Data State Inspectorate (Datu Valsts inspekcija) (2013). Recommendations of the Data State Inspectorate "Security of Personal Data Processing" (Datu valsts inspekcijas rekomendācija „Personas datu apstrādes drošība"), available in Latvian at http://www.dvi.gov.lv/lv/wp-content/uploads/jaunumi/publikacijas/Rekomendacija_PDA_drosiba_27062013.pdf

2. Non-governmental organisations (NGOs)

   N/A There are no NGOs in Latvia focusing on surveillance issues. (data base of national news agency LETA, websites of NGOs)

3. Academic and research institutes, think tanks, investigative media report:

- Vaznis A. (2010). Satversme garantē. Bet kā ir praksē? [Constitution Guarantees. But How About Practise?] Referāts 2010.gada 19.marta konferencē "Cilvēktiesības kriminālprocesā" [Report in 19 March 2012 conference "Human Rights in Criminal Proceedings]. http://www.latvijasadvokats.lv/article/48/

- Vītoliņš V. (2012). Privātās dzīves aizsardzības robežas, uzsākot operatīvās darbības pasākumus. [Protection of Private Life in Starting Operational Investigatory Measures]"Jurista Vārds" [Supplement to the Official Gazette "Lawyer's Voice"] , Nr.49 (748),4 December 2012, available in Latvia at: https://defense.lv/wp-content/uploads/2013/01/jv_priv_operdarb.pdf

- Ziemele I. (2012). Likumos jālīdzsvaro sabiedrības intereses un privātās dzīves neaizskaramība. [Laws Should Balance Public Interest and Inviolability of Private Life], Latvijas Avīze, available in Latvian at http://www.la.lv/ziemele-likumos-jalidzsvaro-sabiedribas-intereses-un-privatas-dzives-neaizskaramiba/

- Privacy International (2011). Global Surveillance Monitor. Report on Latvia, available at https://www.privacyinternational.org/reports/latvia