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

CROATIA

Version of 14 October 2014

Croatian Law Centre
Tin Gazivoda

Summary

[1]. There are four laws directly governing various forms of surveillance conducted by security intelligence agencies, prosecutors and police officers. These are, in alphabetic order: Act on the Security Intelligence System of the Republic of Croatia,[1] Criminal Procedure Act[2], Electronic Communications Act[3], and Police Affairs and Powers Act[4] . The 2006 Act on the Security Intelligence System of the Republic of Croatia[5] defines surveillance that can be carried out by the civilian agency (*Sigurnosno obavještajna agencija* – from here on SOA) and the military agency (*Vojna sigurnosno obavještajna agencija* – from here on VSOA). Articles 33 to 38 of this Act specify a list of measures of secret collection of data.[6] For the following, more intrusive measures a judicial warrant is needed: secret surveillance of communication content, secret surveillance of mail and other postage, secret surveillance and technical recording of interior objects, closed environments and objects as well as the secret purchase of documents and objects. However, the following measures can be taken if approved by one of the agencies' directors: secret surveillance of telecommunication services, activities and traffic; secret monitoring and recording of persons in "open places and public spaces"; secret surveillance of data about telecommunication traffic, the users location, and all "international communication links".[7] The same act also sets the basis for the establishment of the Operative Technical Centre for Telecommunication Oversight

---

[1] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html. All hyperlinks were accessed on 30 September 2014.

[2] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

[3] Croatia, Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (2008), Official Gazette (*Narodne novine*) Nos. 73/08 , 90/11, 133/12, 80/13 and 71/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2824.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_80_1676.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_06_71_1336.html.

[4] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, Art. 80. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

[5] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[6] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, Art. 33-38. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[7] Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, Art.33. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

(*Operativno-tehnički centar za nadzor telekomunikacija* - from here on OTC)[8], while limiting the powers of the Council for Civic Oversight of the Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*) in the sense that the Council is no longer given the power to oversee the application of secret measures at the OTC and that employees of SOA and VSOA can no longer file a complaint with the Council. During the period 2003 – 2006, the Council had the possibility of unannounced on-site oversight of the agencies, and detected several cases of irregularities that lead to court proceedings. During these on-site visits the Council directly monitored the application of secret surveillance of telecommunications (i.e. who was being wire-tapped at the moment). The Act on the Security Intelligence System of the Republic of Croatia[9] states that the Council has the power to oversee 'the application of measures of secret collection of data that limit constitutionally guaranteed rights and fundamental freedoms' (Article 110) but the OTC is not explicitly mentioned. In practice, the introduction of this provision meant that the Council lost the power to directly monitor who was being wire-tapped.

[2]. In the meantime the OTC developed its capacities and became the key point of collection of personal data on the basis of requests from SOA and VSOA, prosecutors and police officers. The Electronic Communication Act specified the obligation of telecommunication firms and internet providers to hold personal data of their users for up to one year.[10] These entities are required to maintain their capacity for storage and to provide this data immediately upon receiving a request from the authorised bodies (SOA and VSOA), prosecutors and police officers).[11] While the storage of content data is strictly prohibited by this act,[12] there is a capacity to gather metadata. Consequently, there is a threat that under certain

---

[8] Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, Art. 18-22. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[9] Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, Art.33. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[10] Croatia, Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (2008), Official Gazette (*Narodne novine*) Nos. 73/08 , 90/11, 133/12, 80/13 and 71/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2824.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_80_1676.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_06_71_1336.html.

[11] Croatia, Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (2008), Official Gazette (*Narodne novine*) Nos. 73/08 , 90/11, 133/12, 80/13 and 71/14, Art. 108. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2824.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_80_1676.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_06_71_1336.html.

[12] Croatia, Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (2008), Official Gazette (*Narodne novine*) Nos. 73/08, 90/11, 133/12, 80/13 and 71/14, Art. 110, para 3. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2824.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_80_1676.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_06_71_1336.html.

conditions the technical capacities of the OTC could be misused.[13] Furthermore, the Police Affairs and Powers Act allows authorised police officers access to telecommunication data[14], while defining four monitoring activities as covert police activities.[15] In terms of the Criminal Procedure Act's Article 186, under the heading 'Collection, Usage and Storage of Personal Data for Purposes of Criminal Procedure', states that the police, prosecutors and courts collect, store and analyse personal data of citizens that are pertinent to the criminal proceedings.[16] This act defines sanctions for the OTC, telecommunication firms and internet providers who do not assist the police, while defining that special investigative measures can be taken for a period of six months and only exceptionally extended for another six months.[17]

[3]. The security intelligence agencies in Croatia carry out surveillance of various forms in order to prevent actions against the Constitutional order and activities that present a security threat to state bodies, citizens and national interests. In recent years most of the actives carried out by authorised bodies that limit citizen rights have been related to surveillance of telecommunication data, and most of these are carried out on the basis of request from authorised police officers (not SOA and VSOA).[18] [19] [20] For this reason there has been a push for additional oversight of the agencies and the police. While NGO's and experts were proposing to strengthen the powers of the existing parliament-based Council for Civic Oversight of the

---

[13] There is a danger of both local and international misuse. Gallagher, Ryan (2014), 'How Secret Partners Expand NSA's Surveillance Dragnet', 18 June 2014, available at: https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/. In the table of Approved SIGINT Partners Croatia is listed as under the category 'third parties'.

[14] Article 68 now specifies that authorised police officers can request from the providers of communication services information about 'the location of the communication devices, location in which all persons involved in the communication are located and the identity markers of the device. Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

[15] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, Art. 80. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

[16] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

[17] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 335. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

[18] The Chair of the Parliamentary Committee for Internal Affairs and National Security Miroslav Tuđman stated that there are currently 40,000 telephone numbers being controlled through the OTC, out of which 85 to 90% are carried out on the basis of requests from the police. Toma, I. (2014), 'Tuđman: Policija bez kontrole prati na desetke tisuća brojeva', 10 July 2014, available at: www.vecernji.hr/hrvatska/tudman-policija-bez-kontrole-prati-na-desetke-tisuca-brojeva-949767.

[19] Interview with Đuro Lubura, Permanent Court Expert for telecommunications and the methodology of surveillance, July 28, 2014.

[20] Interview with Gordan Bosanac, Centre for Peace Studies (human rights NGO that has been systematically monitoring security developments during the last decade), July 21, 2014.

Security Intelligence Agencies,[21] the government opted for the establishment of yet another oversight body. On July 15, 2014 changes and amendments to the Police Affairs and Powers Act were passed by the Parliament, and the amendments entered into force on 5 August 2014. Among other provisions, the Act stipulates the establishment of the Council for Civic Oversight of the Application of Specific Police Powers (*Vijeće* za *građanski nadzor nad primjenom pojedinih policijskih ovlasti*).[22] However, the new Council has not been granted the power to conduct on-site oversight of the OTC. Despite changes of governments, one point of continuity has been the resistance towards providing any outside oversight body with the powers to effectively oversee the functioning of the OTC. When the Council for Civic Oversight of the Security Intelligence Agencies sought an official interpretation from the Parliamentary Committee for Internal Affairs and National Security in 2007, it received a reply from the then Director of SOA Tomislav Karamarko (now the president of the Croatian Democratic Union (*Hrvatska demokratska zajednica (HDZ)*) party) stating that this was a technical error which should be corrected. After seeing that there was no change in practice, the Council repeated the question. On March 2, 2010 the Chair of the Parliamentary Committee for Internal Affairs and National Security Ranko Ostojić (now the Minister of the Interior and a high ranking officer in the Social democratic Party of Croatia (*Socijaldemokratska partija Hrvatske (SDP)*) stated that they forwarded a request to the relevant parliamentary body for an authentic interpretation of the law with regards to this issue.[23] Following the change in government in 2011 and public discussion, the new SDP-lead ruling coalition opted for proposing a new council to be established (the Council for Civic Oversight of the Application of Specific Police Powers). However, again neither council has direct access to the OTC.

[4]. The laws mentioned above specify certain safeguards to ensure respect for privacy and data protection during the surveillance process. One of these safeguards is that there has to be a judicial warrant for those surveillance activities that would traditionally be considered as more intrusive on a persons' rights. However, there is no statistical data available on the number of these requests and the number of requests approved. Most experts, as well as members of oversight bodies, believe that the approval rate is exceedingly high.[24] In addition to the safeguards stipulated by the laws mentioned above, the Personal Data Protection Act sets another set of safeguards. Formally, the Croatian Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka*) has the powers to oversee the work of all public bodies (including the security intelligence agencies, prosecutors and the police) and ensure that citizens have the right to be informed that their data is being analysed, as well as the right to rectification, blockage and deletion.[25] Up to now the Agency's work

---

[21] Cvrtila, V. (2013) „Intelligence Governance in Croatia" in Strengthening Intelligence Governance in the Western Balkans, DCAF, available at: www.dcaf.ch/content/download/104961/1617969/version/2/file/croatia_eng1.pdf.
[22] Croatia, Act on Amendments to the Police Affairs and Powers Act (*Zakon o izmjenama i dopunama Zakona o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) No. 92/14, Articles 102.a, 102.b and 102.c. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.
[23] Statement for the Press issued by Ranko Ostojić, Chair of the Parliamentary Committee for Internal Affairs and National Security Available at: www.tportal.hr/vijesti/hrvatska/57792/Ostojic-Netocne-su-tvrdnje-Sarnavke-i-Gazivode.html.
[24] Interview with Đuro Lubura (an expert) in preparation of this report, 28 July 2014 and author's personal insight.
[25] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text), Art. 32-34. Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at:

has received limited attention, and there are doubts as to its effectiveness in relation to surveillance cases. In over a decade of work, the Agency has not gotten into a single public confrontation with SOA, VSOA or any other segment of the security intelligence system.[26] In Croatia, individuals can turn to different oversight bodies and the courts. Gradually there has been a proliferation of oversight bodies with limited powers and capacities, while court cases usually have to be taken up by the individuals as private cases with a perspective of extensive duration.

/www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

[26] While the Agency has been active in other aspects of personal data protection out of thirteen official opinions that can be found on the Agency web site not a single opinion is related to possible human rights abuse by or in relation to the security-intelligence system. Information from the Agency's web site at: www.azop.hr. On July 8, 2014 the Agency replied in writing to information request sent in preparation of this report, addressing several issues analyzed within the framework of this research. The Agency lists all relevant articles of the Personal Data Protection Act and states that there are five employees working on oversight. However, no examples or other data that would suggest substantial activity in this field are mentioned. Source: Croatia, Croatian Data Protection Agency (*Agencija za zaštitu osobnih podataka*) (2014). Written response to request for information in preparation of this report, 8 July 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)?
Act on the Security-Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*)[27] – Act of the parliament (passed June 30,	Categories of individuals are not specified. All individuals are liable to surveillance of information about their calls, their location and international communication.	Article 23 of the Act specifies that the activities of SOA aim to prevent acts carried out through: terrorism and other forms of organised violence, counter-intelligence carried out by	Surveillance is to be carried out in order to detect and prevent actions against the Constitutional order and actions which present a security threat to state bodies, citizens and national interests	For surveillance of the content of communication; postage and packages; technical recordings of non-public places and secret purchases of documents and objects there must be a prior judicial warrant (ex post exceptionally, 24 hours). For other	Those types of surveillance carried out with judicial warrant of a Supreme Court judge must be clearly defined (article 36) and can be prolonged with consent of three judges. Data that is not relevant for the defined purpose must be destroyed	Those types of surveillance carried out with judicial warrants can last for up to four months and can be prolonged only with consent of three Supreme Court judges and additional procedures (article 37).Other surveillance must	Among those types of surveillance which can be authorised by the Director of SOA or VSOA (without warrant) listed in article 33, section 3d we find 'secret surveillance of international telecommunicati

[27] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

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)?
2006)		foreign intelligence agencies, organizations and individuals forms of extremism, security threats to state dignitaries and protected objects, organized crime and economic crime, unlawful access to classified information and communication systems of state bodies; disclosure of classified data by the heads and staff of state bodies, scientific institutions and legal entities with		information (call numbers, duration, location) no juridical warrant.	within 30 days. Other data must be stored by telecommunication firms for one year.	be approved by the Director of SOA or VSOA and with reporting (art. 38)	on'. The other side of the communication could be anywhere.

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)?
		public authority. Article 24 states that VSOA collects, analyses, processes and evaluates data about the intensions, capabilities and plans of individuals, groups and organizations in the country who aim to undermine the defence capacity of the State, undertaking activities to detect, monitor and counteract such activities.					
Electronic	Categories of	Not listed in this	Criminal	There has to be	Telecommunication	The time limit is	Data about

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)?
Communication Act (*Zakon o elektroničkim komunikacijama*) [28] – Act of the parliament (passed June 19, 2008)	individuals not specified	law.	proceedings and protection of national security	approval from the Director of SOA or VSOA. The types of data are specified: data about the communication source, location, time and duration, type of communication and type of equipment (article 110)	firms and others providing publicly available e-services must maintain the functioning of the surveillance capacity at their own expense and they must immediately identify user upon request.(article 108)	again listed as one year although technical aspects of storage are specified (article 109). It is prohibited to store data about content of communication (article 110)	international communication is collected in line with the defined limitations.
Police Affairs and Powers Act (*Zakon o policijskim*	No categories specified. This applies to individuals	Preventing and revealing criminal acts, preventing	Criminal proceedings and conduct of police affairs	No judicial warrant is needed because measures exclude content. Approval	The above mentioned acts specify that telecommunication	The act states that approval for these measures can only be given	Data about international communication is collected in line

[28] Croatia, The Electronic Communications Act (*Zakon o elektroničkim komunikacijama*) (2008), Official Gazette (*Narodne novine*) Nos. 73/08 , 90/11, 133/12, 80/13 and 71/14, Art. 108. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_133_2824.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_06_80_1676.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_06_71_1336.html.

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)?
poslovima i ovlastima)[29] – Act of parliament (passed on June 30, 2009, amended on July 15, 2014)	defined as criminal suspects by different police units	danger and violence, searching for persons and objects (article 68, section 1)		is given by Chief of Crime Police Unit, Chief of the Unit for Combatting Corruption and Organized Crime (PNUSKOK) and the Chief of the Police Division. (art. 68, section 3)	data must be stored for one year. This act allows police units access to this data.	in cases where there is no other way to achieve the police objective at hand.	with the defined limitations
Criminal Procedure Act (*Zakon o kaznenom postupku*)[30] – Act of the parliament	No categories specified. This applies to individuals defined as criminal suspects by different police	Preventing criminal acts	Criminal proceedings	Order of authorised bodies – the police, state attorney. Special measures have to be authorised by the investigative judge. Sanctions are	The operative-technical centre for the supervision of telecommunications (OTC) in coordination with providers of telecommunication	When the conditions for the special measures cease to exist, the judge must put a stop to the measures. The principles of	Data about international communication is collected in line with the defined limitations.

[29] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

[30] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

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)?
(last major changes passed October 11, 2011)	units, the state attorney's office or a court			defined for the OTC and telecommunication firms whereas the special measures can last for six months at most, exceptionally another six months.	services must provide all technical support to the police. Data must be destroyed in accordance with rules (article 335).	proportionality of the measures conducted ought to be applied.	

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)**
Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*).[31] Act on the Security-Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom*	Articles 32, 34 and others define the right of citizens to be informed about whether their data is being analysed, for what purpose and on what basis. The right to rectification is defined as is the right to be protected from unauthorised access and usage, the blockage of the use of data (specified in relation to the prohibition of the transfer of personal data from Croatia), the right to deletion of personal data collected without a legal basis or without a connection to the purpose	By law the rules on privacy and data protection apply to all persons in the Republic of Croatia regardless of their citizenship, residence, race, ethnicity, gender, religious or any other belonging. However, article 33, point 3. d) of the Act on the Security Intelligence System of the Republic of Croatia defines 'secret surveillance of international telecommunication links' as one of the secret measures that can be applied (without a judicial warrant).[32] What is not clear is what	Relevant provisions of the Personal Data Protection Act are applied only on the territory of the Republic of Croatia, while they can be applied elsewhere in line with the relevant provisions of international law. The Agency recognizes that EU Directive 95/46/EC sets the relevant standards for the protection of personal data for EU member states.

[31] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

[32] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

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)
sustavu Republike Hrvatske) – Act of the parliament (passed 30 June 2006)	of collection. . Article 39 of the Act defines that SOA and VSOA hold collections and registers of personal data as well as other data and documents from their field of work and that employees who are aware of these data must keep them secret. Article 40, section 1 sets out a procedure in which SOA and VSOA are requited to respond within 15 days to any citizen requesting to know whether secret measures have been carried out against him/her, whether there is any personal data held by SOA and VSOA and to, upon request, present for viewing this data to the person in question. Article 40, section 2 states that the documents viewed by citizens cannot contain any data about employees of SOA or VSOA nor can they contain any data about sources. Article 40, section 3 states that SOA and VSOA are not	sort of data is treated under this category of secret measures and whether the CPDPA or another body is effectively overseeing the usage of this data. In general the oversight activities of the CPDPA are conducted by five staff members Not specified in the Act	Not specified in the Act.

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)
	required to follow these procedures in case that the information 'could jeopardise the fulfilment of the agencies objectives, harm the security of another person or bring about harmful consequences for the national security or national interests of the Republic of Croatia. When the reasons for denying access no longer hold article 40, section 4 defines that SOA and VSOA must follow the procedures set out in point 1 immediately in relation to the first two exemptions and after ten years in case of harmful consequences on national security or national interests. Article 41 states the procedures for the destruction of data that are not related to the purpose of surveillance and data that have been collected in an unlawful manner.		

Annex 2 – Oversight bodies and mechanisms[33]

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Committee for Internal Affairs and National Security of the Croatian Parliament (*Odbor za unutarnju politiku i nacionalnu sigurnost Hrvatskog Sabora*)	parliamentary	Act on the security-intelligence system of the Republic of Croatia – articles 104 and 105 define scope of powers.[34]	The Committee has authority for direct on-site oversight of the SOA and VSOA but it is not clear whether this applies to OTC (different interpretations of article 104, sections 4 and 5).[35] In practice, on-site visits take place only	Thirteen members of the Committee are MP's with an interest in national security matters, selected according to the general rules for selection of members of parliamentary committees. The Act on the security-intelligence system specifies that the Chair of the Committee has to be from the opposition, whereas the	Issues non-binding decisions, conclusions and recommendations. Generally reporting to the parliament and the public. Article 104 section 2 sets that Committee can demand: reports from SOA and VSOA about the activities and measures it is undertaking; reports from the President of the

[33] According to the current Act on the Ombudsman, "the Ombudsman is a commissioner of the Croatian Parliament for the promotion and protection of human rights and freedoms laid down in the Constitution, laws and international legal acts on human rights and freedoms accepted by the Republic of Croatia." (Article.2, line1). The Ombudsman „shall promote and protect human rights and freedoms and the rule of law by examining the complaints of the existence of unlawful practices and irregularities with respect to the work of government bodies, bodies of local and regional self- government units, legal persons vested with public authority and legal and natural persons in accordance with special laws". (Article 4). Thus, the Ombudsman has the legal authorities to consider claims of human rights violations committed by police and security services. However, no staff member of the Ombudsman's Office is tasked specifically to deal with violations in this context. Additionally, there is no publicly available information that would indicate that human rights violations of interest to this study have been considered by the Ombudsman. Croatia, Ombudsman's Act (*Zakon o pučkom pravobranitelju*) (2012), Official Gazette (*Narodne novine*) No. 76/12. Available in English at: www.ombudsman.hr/index.php/en/documents-3/legislation/finish/16-legislation/41-the-people-s-ombudsman-act Last checked on 11 September 2014.

[34] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[35] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
			in relation to major cases that receive media attention. Otherwise, receives, reviews and discusses reports from agencies (annual reports as well as reports in relation to specific cases or themes), Article 105 section 1 gives the Committee power to conduct in person hearings of representatives of SOA or VSOA..	ruling coalition has a majority of members.[36] The Committee has its secretary and one to two additional staff are engaged to support its work.	Supreme Court about surveillance measures it has approved; reports from SOA and VSOA about ongoing surveillance and reports about whether SOA and VSOA are carrying out secret measures against a parliamentary representative or a member of his household. Article 104 section 3 states that the Committee can request that the Office of the Council for National Security carries out expert oversight of SOA and VSOA activities and provides it with all information. Organizes hearings for candidates for the positions of agency directors, analyses annual reports of the agencies, the Ombudsman, the Council for civic oversight of the

[36] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					security-intelligence agencies, etc.
The Office of the Council for National Security - OCNS(*Ured Vijeća za nacionalnu sigurnost* - UVNS)	government-expert	Act on the security-intelligence system of the Republic of Croatia – articles 106 to 109 define scope of powers[37]	Expert oversight of the legality, proportionality and effectiveness of the work of the agencies. Oversees whether the agencies are accomplishing their objectives, oversees spending as well as special measures that limit human rights (article 107).[38] On-site oversight in agencies and OTC.	The Head of UVNS is selected by and reports to the Prime Minister and to the President of the Republic. UVNS is a professional body (the National Security Authority of Croatia). It has a special Department for Analytics and Oversight, with several full time professionals engaged in oversight. Specifically, when it comes to regulation of OCNS's structure and staff, tasks of organisational units, approximate staff needed for each group of activities , and some other issues relevant	When this is necessary for UVNS oversight purposes identity of sources must be revealed. Article 109 states that in cases when UVNS confirms violations of the Constitution or detects unlawful activities , it must undertake measures to immediately rectify these irregularities and UVNS must report to the President of the Republic, President of the Parliament and Prime Minister about the measures it has undertaken.

[37] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[38] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
				for the Office's activities are regulated by the Regulation on Internal Organisation of the OCNS (Uredba o unutarnjem ustrojstvu UVNS-a), enacted by the Government with the prior approval of the President of the Republic of Croatia. The Head of OCNS, with the approval of the Council of National Security, issues the Ordinance on the Internal Structure (Pravilnik o unutarnjem redu), wherein the number of employees of organisational units is regulated, among other issues. Both regulations are classified, and the information on the Office's staff is consequently not publicly available. [39]	

[39] Croatia, Office of the Council for National Security (2014) Written response to request for information in preparation of this report, 10 September 2014.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Council for Civic Oversight of Security and Intelligence Agencies (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*)	Parliamentary-civic	Act[40] on the security-intelligence system of the Republic of Croatia – articles 110-114	Currently only regular ex-post oversight of agencies (not OTC) focused on legality of work and applications of special measures of information gathering. In its first mandate (2003-2006), the Council had possibility of unannounced on site oversight.	The Council is composed of seven citizens chosen on the basis of a public call for four year mandates but with certain expertise and with full security clearances. The President of the Council and six other members are chosen by the parliamentary Committee for Internal Affairs and National Security. There is one staff member of the Parliament assigned for the administrative support of the Council.	The Council analyses reports and documents of the agencies and conducts interviews with the SOA and VSOA directors and staff. It acts on the basis of requests sent by citizens and other legal entities about potential irregularities and human rights violations. If these are established the Council reports to the President of the Republic, President of Parliament, PM and State Attorney (article 113) The State Attorney is generally obliged to act upon any information received about possible illegal activities. In terms of the President, PM and President of Parliament this is an issue of political responsibility.

[40] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Council for Civic Oversight of the Application of Specific Police Powers (*Vijeće za građanski nadzor nad primjenom pojedinih policijskih ovlasti*)	Parliamentary-civic	Police Affairs and Powers Act – based on changes and amendment just passed by the Parliament on July 15 (articles 102.a, 102.b, 102.c, 102.d, 102.e)[41]	Regular ex-post oversight of documentation related to police initiated application of measures to detect location of communication devices, location of contacted persons and device identity (article 68) by comparing data from the OTC with police data.	The Council is composed of five members and five deputies. These must be citizens who are not party members, meet additional criteria and who are selected by the Parliament on the basis of a public call (article 102.c). They must obtain basic security clearances. All Council members will serve as volunteers while the chief of police will appoint one police officer to provide expert assistance to Council members.	The Council acts on the basis of its program, requests by citizens and other entities who suspect illegal application of specific police powers. It compares data of OTC and police by analysing documents and conducting interviews with police officers. Reports findings to President of the Parliament, two parliamentary committees, Minister of Interior and Chief of police (article 102.a section.5)
Commission for work in relation to complaints raised against the Ministry of Interior	civic-internal	Act on the Police (article 6) – March 11, 2011	Ex-post work in relation to all types of alleged police abuse, which included allegations of police conducting unlawful surveillance of	Article 6 defines that the Commission is composed of three members: a police employee of the Ministry of Interior as well as two representatives of the public who are chosen by the parliamentary Committee for human rights and the	The Councils methods of work and powers are defined in an internal acts passed by the Minister of Interior. Practical experience has shown that this Commission has limited independence and an extremely big

[41] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
			citizens	rights of national minorities on the basis of nominations from non-governmental organizations and individuals.	workload, both of which limit its effectiveness.
The Croatian Personal Data Protection Agency (CPDPA)	parliamentary based autonomous body	Article 27 and 32 of the Personal Data Protection Act[42]	The CPDPA carries out ex-post oversight on basis of request of citizens, other entities and official duty, including oversight of intelligence agencies (articles 32 and 33).	These oversight activities are carried out by the Department for Oversight and the Central Register of the CPDPA and its five full time employees (four with B.A: degrees and one with a M.A. degree)	Article 32 of the Personal Data Protection Act specified that the CPDPA has the power to access personal data in all personal data collections as well as all related documents, including electronic collections of data. If data are classified the Director, Deputy Director and other authorised staff of the CPDPA have the power to access all data. Article 34 of this Act states that in the case of a breach the CPDPA can: order that the irregularities are corrected; temporarily forbid the

[42] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text), Art. 32-34. Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					collection, processing and usage of the personal data in question; order the deletion of all personal data collected without a legal basis; forbid the transfer of data outside of Croatia and forbid those institutions found in violation of the rules from carrying out similar tasks.
Supreme Court	Judicial	Act on the Security-Intelligence System of the	Analysis of SOA and VSOA proposals for the more intrusive	Supreme court judges	Authorised Supreme Court judges can decide on the validity of the requests for the application of intrusive surveillance measures by SOA and VSOA. Article 36, section 3 specifies that the authorised judge must inform UVNS if he/she rejects the proposal from

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
		Republic of Croatia.[43]	surveillance measures specified in article 33.	authorised by the President of the Supreme Court for this purpose.	SOA or VSOA, specifying the reasons for the decision. Article 36, section 4 specifies what the information that the agencies proposal has to contain. Article 37 defines that these surveillance measures can be extended for four months only in exceptional cases. The proposal must contain the expert opinion of UVNS and the decision has to be reached by three authorised judges of the Supreme Court.

[43] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

Annex 3 – Remedies[44]

[Act on the Security Intelligence System of the Republic of Croatia][45]				
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**
	No, unless there is a request by the subject who suspects to be subject to surveillance..	Upon receiving a request the security intelligence agencies are required to respond in writing within 15 days, clearly stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council for Civic Oversight of the Security Intelligence Agencies) as well as the Ombudsman of the Republic of Croatia. The Act does not regulate, and thus does not specify legal remedies available to individuals whose rights have been violated by institutions within the security intelligence system. Court protection is available on the basis of general regulation in the field of administrative[46], civil[47], and	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)

[44] In case of different remedial procedures please replicate the table for each legal regime.
[45] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.
[46] Croatia, Act on Administrative Disputes (*Zakon o upravnim sporovima*) (2010), Official Gazette (*Narodne novine*) Nos.20/10 and 143/12, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2010_02_20_483.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3036.html.

			criminal law[48] Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	
Collection*	No	Upon receiving a request the security intelligence agencies are required to respond in writing within 15 days, clearly stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council for Civic Oversight of the Security Intelligence Agencies) as well as the Ombudsman of the Republic of Croatia. The person can also lodge a complaint with the courts in line with relevant laws. Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)
Analysis*	No	Upon receiving a request the security intelligence agencies are required to	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)

[47] Croatia, Civil Procedure Act (*Zakon o parničnom postupku*) Official Gazette, Gazette (*Narodne novine*) Nos.148/11 (consolidated text) and 25/13, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_12_148_2993.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2013_02_25_405.html.

[48] Croatia, Criminal Code (*Kazneni zakon*) (2011), Official Gazette (*Narodne novine*), No. 125/11, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_11_125_2498.html.

* 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

		respond in writing within 15 days, clearly stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	for Civic Oversight of the Security Intelligence Agencies as well as the Ombudsman of the Republic of Croatia. The person can also lodge a complaint with the courts in line with relevant laws. Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	
Storing*	No	Upon receiving a request the security intelligence agencies are required to respond in writing within 15 days, clearly stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council for Civic Oversight of the Security Intelligence Agencies) as well as the Ombudsman of the Republic of Croatia. The person can also lodge a complaint with the courts in line with relevant laws. Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)
Destruction*	No	Upon receiving a request the security intelligence agencies are required to respond in writing within 15 days, clearly	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council for Civic Oversight of the Security Intelligence Agencies) as well as	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)

		stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	the Ombudsman of the Republic of Croatia. The person can also lodge a complaint with the courts in line with relevant laws. Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	
After the whole surveillance process has ended	No	Upon receiving a request the security intelligence agencies are required to respond in writing within 15 days, clearly stating whether they have been undertaking any measures against this person and giving them access to the data unless conditions states in article 40 apply	A person can turn to the listed oversight bodies: the parliamentary Committee for internal affairs and national security and the Council for Civic Oversight of the Security Intelligence Agencies) as well as the Ombudsman of the Republic of Croatia. The person can also lodge a complaint with the courts in line with relevant laws. Article 41 specified the procedure for the deletion of the data collected by the services in an unlawful manner or that are not pertinent for the purpose of collection.	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.)

[Criminal Procedure Act][49]				
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**
	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been collected, analysed and stored. This information can be given one year after the investigation order was made.	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.).
Collection*	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of data, etc.).

[49] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

* 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

		collected, analysed and stored. This information can be given one year after the investigation order was made.		
Analysis*	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been collected, analysed and stored. This information can be given after one year from the moment the investigation order was filed.	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
Storing*	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been collected, analysed and stored. This information can be given after one year from the moment the	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).

		investigation order was filed.		
Destruction *	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been collected, analysed and stored. This information can be given after one year from the moment the investigation order was filed.	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
After the whole surveillance process has ended	No	No, the right to access is not specified. Article 188 defines the right to be informed upon request whether someone's personal data have been collected, analysed and stored. This information can be given after one year from the moment the investigation order was filed.	An individual can file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).

[Police Affairs and Powers Act][50]				
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**
	No	No, the right to access is not specified. Article 102.a. foresees the possibility of a person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	When the Council for Civic Oversight of the Application of Special Police Powers is established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
Collection*	No	No, the right to access is not specified. Article 102.a. foresees the possibility of a person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	When the Council for Civic Oversight of the Application of Special Police Powers is established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
Analysis*	No	No, the right to access is not specified. Article 102.a.	When the Council for Civic Oversight of the Application of	Violation of constitutionally guaranteed rights (to privacy,

[50] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

* 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

		foresees the possibility of a person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	Special Police Powers is established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	protection of date, etc.).
Storing*	No	No, the right to access is not specified. Article 102.a. foresees the possibility of a person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	When the Council for Civic Oversight of the Application of Special Police Powers is established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
Destruction *	No	No, the right to access is not specified. Article 102.a. foresees the possibility of a person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	When the Council for Civic Oversight of the Application of Special Police Powers is established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).
After the whole surveillance process has	No	No, the right to access is not specified. Article 102.a. foresees the possibility of a	When the Council for Civic Oversight of the Application of Special Police Powers is	Violation of constitutionally guaranteed rights (to privacy, protection of date, etc.).

ended		person being informed about the process on the basis of a request to the newly established Council and only after the criminal investigation has been completed.	established in the coming months an individual will be able to lodge a claim with this body. An individual can also file a complaint with the courts.	
[Personal Data Protection Act][51]				
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**
	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days.	Constitution of the Republic of Croatia[55] Personal Data Protection Act[56]

[51] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

[55] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.

[56] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

	data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of personal data recipients, and whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal	stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state (including monetary, budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in	Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act on the Security Intelligence System of the Republic of Croatia[52], Criminal Procedure Act[53], Police Affairs and Powers Act[54]) "Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request	

[52] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[53] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

[54] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall be provided to the data subject regardless of whether data is collected directly from the subject or from other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal	question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be used exclusively for statistical purposes.“	about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding	

	data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the		the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate an administrative procedure.	

	copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

Collection*	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days. Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act	Constitution of the Republic of Croatia[60] Personal Data Protection Act[61]

* 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

	personal data recipients, and whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall	(including monetary, budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be	on the Security Intelligence System of the Republic of Croatia[57], Criminal Procedure Act[58], Police Affairs and Powers Act[59]) "Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data	

[60] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.

[61] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.

[57] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

[58] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.

[59] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	be provided to the data subject regardless of whether data is collected directly from the subject or from other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or	used exclusively for statistical purposes.“	undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The	

	plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use,		CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate an administrative procedure.	

	5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

Analysis*	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of personal data recipients, and	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state (including monetary,	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days. Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act on the Security Intelligence System of the Republic of Croatia[62],	Constitution of the Republic of Croatia[65] Personal Data Protection Act[66]

[62] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

	whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall be provided to the data subject regardless of whether data is collected directly from the subject or from	budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be used exclusively for statistical purposes.“	Criminal Procedure Act[63], Police Affairs and Powers Act[64]) “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source,	

[65] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.
[66] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.
[63] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.
[64] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data		3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate	

	relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose		an administrative procedure.	

	and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

Storing*	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of personal data recipients, and	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state (including monetary,	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days. Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act on the Security Intelligence System of the Republic of Croatia[67],	Constitution of the Republic of Croatia[70] Personal Data Protection Act[71]

[67] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

	whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall be provided to the data subject regardless of whether data is collected directly from the subject or from	budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be used exclusively for statistical purposes.“	Criminal Procedure Act[68], Police Affairs and Powers Act[69]) “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source,	

[70] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.
[71] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.
[68] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.
[69] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data		3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate	

	relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose		an administrative procedure.	

	and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

Destruction *	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of personal data recipients, and	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state (including monetary,	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days. Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act on the Security Intelligence System of the Republic of Croatia[72],	Constitution of the Republic of Croatia[75] Personal Data Protection Act[76]

[72] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

	whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall be provided to the data subject regardless of whether data is collected directly from the subject or from	budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be used exclusively for statistical purposes.“	Criminal Procedure Act[73], Police Affairs and Powers Act[74]) “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source,	

[75] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.
[76] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.
[73] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.
[74] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data		3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate	

	relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose		an administrative procedure.	

	and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

After the whole surveillance process has ended	Article 23 of this Act specifies that rights and obligations stipulated in the Articles 9 and 19 of this Act (see quoted Articles below) can be restricted by special regulations. "Article 9 Prior to collecting any personal data, the personal data filing system controller or the processing official must inform the data subject whose personal data is being collected about the identity of the personal data filing system controller, the intended purpose of processing this data, about the reason for processing such data, about the right to information access and the right to data correction pertaining to him/her, about recipients or categories of personal data recipients, and	Article 19, line 3 of this Act defines that the subject or their authorised representative have the right to access the collected data within 30 days of the date of submission of request. However, the access to the data is limited as described in Article 23 of this Act: "Article 23 The obligations and rights stipulated by the provisions of Articles 9 and 19 of this Act may be restricted in the way and under conditions established by special acts if deemed necessary for the protection of state security, defence and public safety; for the prevention, investigation, detection or persecution of any criminal act or breaches of ethical codes for regulated professions; for the protection of important economic or financial interests of the state (including monetary,	Article 20 of this Act specifies that the concerned individual or their authorised representative can request that the person in charge of the personal data collection: amends, changes or deletes personal data if the data is incomplete, incorrect or old. The person in charge of the personal data collection must inform the concerned individual about activities that have been taken to rectify the concern within 30 days. Article 23 of the Act defines that the rights listed in Article 19 (see quoted Article 19 below) can be limited in cases related to national security, defence, public security, prevention of crime and criminal investigation, violations of ethical standards for certain professions, protection of important economic and financial interests of the state and in cases where human rights of others might be violated. Limitations are specified in special regulations mentioned above (Act on the Security Intelligence System of the Republic of Croatia[77],	Constitution of the Republic of Croatia[80] Personal Data Protection Act[81]

[77] Croatia, The Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*) (2006), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2006_07_79_1912.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2006_09_105_2371.html.

	whether data provision is voluntary or mandatory, as well as about possible consequences of withholding data. In case of mandatory provision of personal data, the legal basis for personal data processing shall be indicated as well. Prior to providing personal data to other recipients, the personal data filing system controller shall inform the data subject about this. Information from paragraphs 1 and 2 of this Article shall be provided to the data subject regardless of whether data is collected directly from the subject or from	budgetary and taxation issues) and for the protection of data subjects or the rights and freedoms of others, within the scope necessary for the fulfilment of purposes for which the limitation in question has been determined. The obligations and rights stipulated by the provisions of Articles 19 and 20 of this Act may be restricted by special acts in case the personal data are processed exclusively for the purpose of scientific research or for the purpose of establishing statistics and stored for a longer period to be used exclusively for statistical purposes.“	Criminal Procedure Act[78], Police Affairs and Powers Act[79]) “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source,	

[80] Croatia, Constitution of the Republic of Croatia (*Ustav Republike Hrvatske*) (1990) Official Gazette (*Narodne novine*) No. 85/10 (consolidated text). Available at: www.sabor.hr/fgs.axd?id=16481.
[81] Croatia, Personal Data Protection Act (*Zakon o zaštiti osobnih podataka*) (2003), Official Gazette (*Narodne novine*) Nos. 103/03, 118/06, 41/08, 130/11, 106/12 (consolidated text). Consolidated text available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html. Unofficial English translation available at: /www.azop.hr/download.aspx?f=dokumenti/Razno/PersonalDataProtectionAct_revisedtext-unofficialtranslation_1.doc.
[78] Croatia, Criminal Procedure Act (*Zakon o kaznenom postupku*) (2008), Official Gazette (*Narodne novine*) Nos. 121/2011 (consolidated text), 143/2012, 56/2013, 145/2013. Art. 186. Available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2012_12_143_3031.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1142.html, http://narodne-novine.nn.hr/clanci/sluzbeni/2013_12_145_3090.html.
[79] Croatia, Police Affairs and Powers Act (*Zakon o policijskim poslovima i ovlastima*) (2009), Official Gazette (*Narodne novine*) Nos. 76/09 and 92/14, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2009_07_76_1835.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2014_07_92_1845.html.

	other sources. Exceptionally, information from paragraphs 1 and 2 of this Article does not have to be provided to the data subject if personal data is provided for usage or is collected from the existing personal data files in order to be processed for statistical purposes or for the purposes of historic or scientific research, or if the provision of such information would require an excessive effort, if such processing of personal data has been explicitly determined by law.“ “Article 19 The personal data filing system controller shall, at the latest within 30 days from receiving a request about it, provide the following to every data subject or his/her legal representative or plenipotentiary: 1. deliver a confirmation as to whether or not data		3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“ On the basis of the Act anyone can turn to the CPDPA if they believe their rights have been violated. The CPDPA replies by reaching an official decision. The concerned individual cannot raise a complaint against this decision but can initiate	

	relating to data subject are being processed, 2. communicate to data subject in an intelligible form of the data undergoing processing and of any available information as to their source, 3. allow access to the personal data filing system records and to the personal data in the personal data filing system relating to the data subject, and allow the copying of such files, 4. deliver excerpts, certificates or printouts of the personal data held in the personal data filing system relating to the data subject, which must contain an indication of the purpose and legal basis for their collecting, processing and use, 5. deliver a printed copy containing the information on who obtained access to the data, for what purpose		an administrative procedure.	

	and on what legal basis regarding the personal data of the data subject, 6. provide information about the logic involved in any automatic processing of data concerning him/her.“			

Annex 4 – Surveillance-related case law at national level

Please provide a maximum 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	Sandra Benčić against SOA[82]
Decision date	May 8, 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Constitutional Court of the Republic of Croatia Ustavni sud Republike Hrvatske Broj: U-III-164/2013
Key facts of the case (max. 500 chars)	Sandra Benčić claimed the security intelligence agency (SOA) conducted unlawful activities in the context of her security clearance. The security clearance was carried out on the basis of a request from the government Office for Associations when Ms. Benčić was nominated for membership in the Council for Civil Society Development in the fall of 2006. During the clearance, SOA requested telecommunication data pertaining to a phone number belonging to the boyfriend of Ms. Benčić. The clearance procedure was revealed when an agent openly called an NGO in which Ms. Benčić had been working.
Main reasoning/argumentation (max. 500 chars)	The case is a striking example of how infringements on human rights can take place in cases that have nothing to do with national security or criminal acts. Membership in the Council for Civil Society Development is a consultative part time engagement while the purpose of the Council is to discuss the frame for the further development of civil society. On the basis of an outdated government Decree one suspicious official had the authority to send the request while the agency formally had the grounds to conduct the security clearance. Without any

[82] Constitutional Court of the Republic of Croatia (*Vrhovni sud Republike Hrvatske*) (2014), Decision No. U-III-164/2013, available at: http://sljeme.usud.hr/usud/praksaw.nsf/94b579567876f9fcc1256965002d1bf4/c12570d30061ce54c1257cd2004a4efc/$FILE/U-III-164-2013.pdf.

	consideration the agency not only conducted the clearance but employed a surveillance measure.[83]
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case raised the issue of how, when and how security clearances should be carried out. This was specifically important at a time when the government was increasingly using security clearances as a means of obtaining information about people who were often in the most remote matter connected to some segment of government work. The case showed that the Council for Civic Oversight of the Security Intelligence Services had the powers to conduct effective oversight at the time. The case also showed how long it takes for someone to get legal satisfaction through the available remedies.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Soon after the clearance operation was revealed this case was all over the media and Deputy PM for social affairs (later PM) Jadranka Kosor had to respond. However, the revelation mounted pressure on the government to develop a new Security Clearances Act (which was passed a year after the incident).[84] The new act was based on the principle of proportionality, instituted three levels of security clearances and limited the number of bodies that can request clearances. In its judgement the Constitutional Court recognized that the conduct of SOA presented an unnecessary human rights infringement and that Ms. Benčić is entitled to compensation.

[83] Obris.org (2014), 'Slučaj Benčić – poučak o tajnim službama i tzv. neovisnom nadzoru', 7 June 2014, available at: http://obris.org/hrvatska/slucaj-bencic-poucak-o-tajnim-sluzbama-i-tzv-neovisnom-nadzoru.

[84] Croatia, Security Clearances Act (*Zakon o sigurnosnim provjerama*) (2008), Official Gazette (Narodne novine) Nos. 85/08 and 86/12, available at: http://narodne-novine.nn.hr/clanci/sluzbeni/2008_07_85_2729.html and http://narodne-novine.nn.hr/clanci/sluzbeni/2012_07_86_1968.html.

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**
Security Intelligence Agency (*Sigurnosno obavještajna agencija* – SOA)	*Government*	*Savska cesta 39/I, Zagreb* *+ 385 1 377 2222* *informiranje@soa.hr*	*www.soa.hr*
Military Security Intelligence Agency (*Vojna sigurnosno obavještajna agencija* – VSOA)	*Government*	*Trg Petra Krešimira IV broj 1, Zagreb* *+ 385 1 456 7111* *infor@morh.hr*	*www.morh.hr*
**Office of the Council for National Security (*Ured Vijeća za nacionalnu*	*Government*	*Jurjevska 34, Zagreb* *+ 385 14681 222*	*www.uvns.hr*

***sigurnost* – UVNS)**			
Operational Technical Centre for Surveillance of Telecommunication (*Operativno-tehnički centar za nadzor telekomunikacija* – OTC)	*Government*	*not available publicly* *(SOA, Savska cesta 39/I for more information)*	*not available*
Committee for Internal Affairs and National Security (*Odbor za unutarnju politiku i nacionalnu sigurnost*)	*Parliament*	*Trg. sv. Marka 6, Zagreb* *+ 385 1 4569 459* *odbupns@sabor.hr*	*www.sabor.hr*
Committee for Human Rights and Rights of National Minorities (*Odbor za ljudska prava i prava nacionalnih manjina*)	*Parliament*	*Trg sv. Marka 6, Zagreb* *+ 385 1 4569 416* *odbor.prava@sabor.hr*	*www.sabor.hr*
Council for Civic Oversights of the Security Intelligence Agencies (*Vijeće za građanski nadzor sigurnosno obavještajnih agencija*)	*Parliamentary based – civic body*	*Trg sv. Marka 6, Zagreb* *+ 385 1 4569 222*	*www.sabor.hr*

Supreme Court of the Republic of Croatia (*Vrhovni sud Republike Hrvatske*)	*court*	*Trg N.Š. Zrinskog 3, Zagreb* *+ 385 1 4862 222* *vsrh@vsrh.hr*	*www.vsrh.hr*
Croatian Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka*)	*public authority*	*Martićeva 14, Zagreb* *+ 385 1 4609 000* *azop@azop.hr*	*www.azop.hr*
Centre for International and Security Studies (*Centar za međunarodne i sigurnosne studije*)	*academia*	*Faculty of Political Science, University of Zagreb* *Lepušićeva 6, Zagreb* *+ 385 1 4642 000*	*www.fpzg.hr*
Vern University (*Veleučilište Vern*)	*academia*	*prof. Vlatko Cvrtila, dean* *Trg bana Jelačića 3, Zagreb* *dekan@vern.hr*	*www.vern.hr*
Centre for Peace Studies (*Centar za mirovne studije*)	*civil society organisation*	*Selska 112a, Zagreb* *+ 385 1 482 0094* *cms@cms.hr*	*www.cms.hr*

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

   - Council of Europe, Parliamentary Assembly (PACE) (2014), Committee on Legal Affairs and Human Rights: "Massive Eavesdropping" and "Additional Protocol to the ECHR on Protection of whistle-blowers", Introductory memorandum, 23 January 2014, available at: www.assembly.coe.int/CommitteeDocs/2014/ejdoc022014.pdf.

   - European Data Protection Supervisor (2014), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU - US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", February 2014, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf.

   – State Attorney's Office of the Republic of Croatia (*Državno odvjetništvo Republike Hrvatske*) Annual Report for 2013 (*Izvješće o radu za 2013. godinu*)

   - Council for Civic Oversight of the Security Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*) (2014), Annual report of the Council for Civic Oversight of the Security Intelligence Services 2013 (*Godišnje izvješće Vijeća za građanski nadzor sigurnosno-obavještajnih agencija za 2013.)*

   - Toma, I. (2014), 'Tuđman: Policija bez kontrole prati na desetke tisuća brojeva', 10 July 2014, available at: www.vecernji.hr/hrvatska/tudman-policija-bez-kontrole-prati-na-desetke-tisuca-brojeva-949767. (Mr. Tuđman is the Chair of the parliamentary Committee for Internal Affairs and National Security).

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

- Council for Civic Oversight of the Security Intelligence Services (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*) (2014), Annual report of the Council for Civic Oversight of the Security Intelligence Services 2013 (*Godišnje izvješće Vijeća za građanski nadzor sigurnosno-obavještajnih agencija za 2013.)*

- Croatia, People's Ombudsman (*Pučki pravobranitelj*) (2014), Annual report of the People's Ombudsman for 2013 (*Izvješće Pučke pravobraniteljice za 2013.*), available at: www.ombudsman.hr/index.php/hr/izvjesca/izvjesce-pucke-pravobraniteljice/finish/20-2013/55-izvjesce-pucke-pravobraniteljice-za-2013-po-prvi-puta-objedinjeno-izvjesce-o-stanju-ljudskih-prava-u-hrvatskoj-i-radu-ureda. Summary in English available at: www.ombudsman.hr/index.php/en/documents-3/ombudsman-s-reports/finish/15-ombudsman-s-reports/76-summary-annual-report-for-2013.

- Croatian Personal Data Protection Agency (*Agencija za zaštitu osobnih podataka*) Annual report (*Godišnje izvješće o radu*)

3. Non-governmental organisations (NGOs)

- Centre for Peace Studies (*Centar za mirovne studije*), Reports and statements, available at: www.cms.hr.

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

- Gallagher, Ryan (2014) 'How Secret Partners Expand NSA's Surveillance Dragnet', 18 June 2014, available at: https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.

- Web portal Orbis.org, Articles, available at: www.orbis.org.