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

CYPRUS

Version of 1st October 2014

First Elements Euroconsultants and
Cyprus Institute of Church and State Relations
Michalis Kontos

Summary

1.The summary shall provide information on the following three issues:

Description of the surveillance legal framework in your country, including different laws governing surveillance by State actors and on-going legislative reforms. The summary should include the following aspects:

a. types of security services and bodies involved,
b. the extent of their powers in case of surveillance of individuals and also vis-a-vis private sector (right to acccess to data held by telecom or internet providers, right to refuse access),
c. control/oversight mechanisms,
d. geographical scope of surveillance
e. conditions under which intelligence services can conduct surveillance and for which purpose(s) (such as national security, investigation or prevention of crimes, etc.)
f. different stages of surveillance procedure (collection, analysis, storing, destruction).

2.Regarding the Republic of Cyprus the only public body that falls into the scope of this report is the Central Intelligence Service (CIS). The CIS deals with the collection, evaluation and utilization of intelligence that relates to the security of the State. Concerning matters of State security it is directly accountable to the President of the Republic, who appoints its Director. Administratively, CIS police members are subject to the Chief of the Police.[1] The CIS was established in 1970 by virtue of a Decision issued by the Council of Ministers.[2] There is no law regulating its functioning,[3] therefore there is no law regulating surveillance practices potentially undertaken by the CIS. Consequently, the extent of its powers, the geographical scope and the stages of surveillance procedure, or the conditions and the purposes of surveillance are not clearly defined. In order to contribute to the remedy of this shortcoming, the government formulated a bill, "Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών (ΚΥΠ) Νόμος του 2014" [Cyprus Intelligence Services (CIS) Law of 2014], which was submitted to the House of Representatives, on the 23rd of September 2014, for scrutiny and approval. Acting as usual, the House of Representatives referred this bill for scrutiny to the Parliamentary Committee on Institutions, Merit and the Commissioner for Administration (Ombudsman), which is currently working on it. Due to the so far vagueness regarding the activities of CIS, there are occasional references in media reports about alleged irregular surveillance activities undertaken by the CIS.[4] In relation to this matter, the Parliamentary Committee on Institutions, Merit and the Commissioner for Administration (Ombudsman) discussed an issue titled "The institutional role of the Central Intelligence Service, potential

[1] Data derive from the following sources: 1) Police Website, http://www.police.gov.cy/police/police.nsf/All/D39403D1ACD587B4C22578A900271B4E?OpenDocument. Accessed 25 July 2014. 2) Letter sent by Mrs Anna Aristotelous (Office of the Minister of Justice and Public Order), 4 August 2014.

[2] Decision of the Council of Ministers No 9955 [Απόφαση Υπουργικού Συμβουλίου Υπ' Αριθμόν 9955], 4 September 1970.

[3] Data derive from the following sources: 1) Letter sent by Mr. Constantinos Georgiades, Officer at the Office of the Commissioner for Personal Data Protection, 1 July 2014. 2) Letter sent by Mrs Anna Aristotelous (Office of the Minister of Justice and Public Order), 4 August 2014.

[4] See for example Chaili, D. (2010), 'The secret weapon for undermining and opponent', [Το μυστικό όπλο της υπόσκαψης του αντιπάλου] *Simerini*, 5 October 2010. Theocharides, P. (2014), 'They wiretap our mobile phones: A state-of-the-art system for mobile phone surveillance in Cyprus', [Υποκλέπτουν δεδομένα από τα κινητά μας τηλέφωνα: Εξελιγμένο σύστημα παρακολούθησης κινητών στην Κύπρο] *Phileleftheros*, 27 June 2014.

surveillance of citizens and subsequent responsibilities" (*Ο Θεσμικός ρόλος της Κεντρικής Υπηρεσίας Πληροφοριών, οι ενδεχόμενες παρακολουθήσεις πολιτών και οι προκύπτουσες ευθύνες*), on 17 September 2013. This session was attended by the Minister of Justice and Public Order, the Chief of the Police, the Director of the Central Intelligence Service and representatives from the Office of the Commissioner for Personal Data Protection. Due to the fact that the session was not open to the public, all the related details are considered as secret and they cannot be disclosed to persons other than the Members of the Parliament.[5]

3. Regarding surveillance undertaken by police in the context of criminal investigation, it is regulated by the Law that Provides for the Protection of Private Communications.[6] According to article 6(1) the initiation of a surveillance process (or the extension of an ongoing one) can be legally possible only after a judicial warrant which can be obtained by the Attorney General, after a request made by the Chief of the Police or the Director of the Customs and Excise Department. The Attorney General shall consent to this action only if he is persuaded that such a surveillance process can provide or has provided testimony for the commitment of a crime. Article 8 provides for several prerequisities that must be fulfilled and included in the Attorney General's application, upon which the request for the judicial warrant shall be justufied. Furthermore, according to article 9(1), the Attorney General can order for the initiation of a telecommunications surveillance through the Cyprus Telecommunications Authority in case he will be able to proceed to the application for a judicial warrant within 24 hours.

4. The body which is responsible for overseeing the CIS's functioning as regards data protection is the Office of the Commissioner for Personal Data Protection. The scope of the Processing of Personal Data (Protection of Individuals) Law,[7] as amended, applies to the processing of personal data carried out by intelligence services for purposes of national security.[8] Therefore, the CIS is oblidged to act in harmony with the provisions of this law. Regarding electronic communications and protection of the communications' privacy, the Office of the Commissioner for Electronic Communications and Post Regulation is responsible for overseeing the security level of the public networks. This obligation derives from the provisions of the Regulation of Electronic Communications and Post Services Law.[9] This applies to the security services which commit surveillance to the degree that they may use public networks to collect intellingence, in infringement of the related laws.

5. Safeguards put in place by the legal framework (described under 1 above) to ensure respect for privacy and data protection during surveillance measures (judicial warrant, right to be informed, right to rectification/deletion/blockage, right to challenge the surveillance, etc.)

6. Since there is no law regulating the CIS's functioning, the safeguards provided by the legal framework were not designed especially for that purpose, but they generally apply to cases of violation of personal data and privacy of communications. According to the Law that Provides for the Protection of Private Communications, article 3(1), surveillance or wiretapping of private communication, or disclosure of private communication content, or usage of such content suggest a crime that could lead to imprisonment penalty up to three

[5] Data derive from a letter sent by Mrs Vasiliki Anastasiadou, Director General of the House of Representatives, 18 July 2014.
[6] Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.
[7] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*).
[8] Letter sent by Mr. Constantinos Georgiades, Officer at the Office of the Commissioner for Personal Data Protection, 1 July 2014.
[9] Cyprus, Regulation of Electronic Communications and Post Services of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [Ν. 112(I)/2004]*), 30 April 2004.

years.[10] Derogations are feasible after the issue of a judicial warrant under the process described above. However, accoring to article 6(2), no application for a judicial warrant can be submitted by the Attorney General, neither a judicial authorisation for a surveillance process can be issued, unless in cases of surveillance of private communications that are being conducted by persons under imprisonment or detention or that are being conducted through illicit means.

7. According to the Processing of Personal Data (Protection of Individuals) Law, article 11(1), in case of personal data processing, the individual who is subject to the collection of his/her personal data must be informed of the identity of the collector, the purpose of the processing, the recipients of the data and the existance of a right to access and correct the data, during the collection stage. Derogations are feasible in case the personal data collection is related to purposes of defence, national needs or needs related to the national security of the Republic. In that case, the collector's obligation to inform the subject may be cancelled after a decision of the Commissioner for Personal Data Protection.[11] An individual who is subject to personal data collection can resort to the Commissioner for Personal Data Protection, who has the power to impose administrative sanctions in case of infrigement of the Processing of Personal Data (Protection of Individuals) (see "Remedies") Law. According to the same law, article 23(1), the Commissioner for Personal Data Protection may conduct inspections to records kept for national security reasons, including the CIS's. The only restrictions set out in the Law, as regards the Commissioner's competences, impose that the Commissioner himself is present at inspections of the CIS and, that the Commissioner cannot have access to data revealing the identity of CIS's collaborators.[12] Insofar, the Commissioner's Office had no reasons to believe that the CIS processes personal data outside its mandate, in infringement of the data protection Law.[13]

8. Regarding electronic communications, according to the Regulation of Electronic Communications and Post Services Law,[14] article 99(2), outside the communicating users, no one is permitted to listen, wiretap, save, intervene and/or proceed to any other form of surveillance committed through the communications network and the electronic services available to the public. The only case an intervention to the telecommunications can be legally possible is when provided by the law and with a judicial warrant, according to the process described above. Generally, article 19(1) provides that regarding the execution of the powers legally granted to the Commissioner for Electronic Communications and Post Regulation, the Commissioner is free to act impartially and indepedently. However, when it comes to defence and national security issues, he is subject to the Council of Ministers. A related decree issued by the Commissioner for Electronic Communications and Post Regulation on 28 December 2007 provides that some telecommunication data can be saved for billing purposes, only for a period of six months.[15] Furthermore, the providers of public

[10] Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.
[11] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*).
[12] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*). Letter sent by Mr. Constantinos Georgiades, Officer at the Office of the Commissioner for Personal Data Protection, 1 July 2014.
[13] Letter sent by Mr. Constantinos Georgiades, Officer at the Office of the Commissioner for Personal Data Protection, 1 July 2014.
[14] Cyprus, Regulation of Electronic Communications and Post Services Law of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]*), 30 April 2004.
[15] Cyprus, Commissioner for Electronic Communications and Post Regilation (*Επίτροπος Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων*) (2007), 'Περί Φύλαξης και Επεξεργασίας των Δεδομένων Κίνησης Διάταγμα', 28 December 2007.

networks or publicly available electronic communication services are obliged to notify the Commissioner's office on every breach of security or loss of their networks' integrity which would affect their networks or services' functioning. With a decree issued on 25 October 2013 the Commissioner for Electronic Communications and Post Regulation defines the notification process the providers of public networks or publicly available electronic communications services are obliged to implement when they notice a breach of security.[16] The measure is jointly conducted with the Office of the Commissioner for Personal Data Protection. In the same context, according to the Regulation of Electronic Communications and Post Services Law, article 98(A), a provider who notices a breach of security which affects an individual is obliged to report to the affected individual, at least as regards the nature of the breach and the contact points that could provide further information.[17]

9. Judicial or non-judicial remedies available to an individual subject to surveillance at different stages of surveillance procedures.

10. Since there is no law regulating the CIS's functioning and/or surveillance process, the remedies available to an individual subject to surveillance were not designed especially for that purpose, but they generally apply to cases of violation of personal data and privacy of communications. According to the Processing of Personal Data (Protection of Individuals) Law, article 12(1), every individual has the right to know whether he/she is being or has been subject to personal data processing. Therefore, the individual responsible for the processing is obliged to correspond to any request for related information made by the individual subject to the processing and, if requested, to provide copies of the data processed, if this does not entail disproportionate effort to be accomplished. If the individual responsible for the processing does not reply within four weeks after the request, article 12(3) provides that the individual subject to personal data processing has the right to resort to the Commissioner for Personal Data Protection, who can proceed to inspection.[18] According to article 12(4) derogations are feasible in case the personal data processing is related to purposes of national needs or needs related to the national security of the Republic. In that case, the collector's obligation to inform the subject may be cancelled after a decision of the Commissioner for Personal Data Protection.The Commissioner has the power to impose a fine up to 5000 Euro to anybody who does not comply or obstructs an inspection or the examination of a complaint. In case a related inspection reveals infringement of the Processing of Personal Data (Protection of Individuals) Law or any other regulation related to the protection of an individual who has been subject to personal data processing, article 25(1) provides that the Commissioner may impose administrative sanctions including warnings, fines up to 30,000 Euro, temporary revocation of a license, permanent revocation of a license, or destruction of a filing system and/or the cessation of processing and the destruction of the relevant data.[19] Moreover, according to article 16(1), anybody has the right to resort to the judicial system and apply for the cancellation of an act or decision made by any legal or natural person entailing personal data processing that relates to the evaluation of his/her personality, financial reliability or attitude in general. The individual responsible for the processing is obliged to compensate an individual who has been subject to personal

[16] Cyprus, Commissioner for Electronic Communications and Post Regulation (*Επίτροπος Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων*) (2013), 'Περί κοινοποίησης των παραβιάσεων ασφαλείας ή απώλειας ακεραιότητας δικτύων ή και υπηρεσιών, Διάταγμα του 2013', 25 October 2013.
[17] Cyprus, Regulation of Electronic Communications and Post Services Law of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [Ν. 112(Ι)/2004]*), 30 April 2004.
[18] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[Ι]/2001*).
[19] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[Ι]/2001*).

data processing in breach of the Processing of Personal Data (Protection of Individuals) Law, unless if he/she can prove that he/she is not responsible for the harm.[20]

11. Regarding electronic communications, according to the Regulation of Electronic Communications and Post Services Law the remedy process involves three levels: The submission of a complaint to the Commissioner for Electronic Communications and Post Regulation regarding a possible infringement of the Law by a service provider, the administrative examination of a complaint and the imposition of administrative sanctions to the providers, and finally the penal cases which are being transferred to the courts.[21] When it comes to infringement of personal data the Regulation of Electronic Communications and Post Services Law, article 107, provides that the Commissioner for Personal Data Protection may be in charge of any such cases or complaints.[22] No derogations to the application of these remedies are explicitly referred in the law, outside the derogations related to the powers of the Commissioner for Personal Data Protection described above, when it comes to the process described by article 107. Generally, article 19(1) provides that regarding the execution of the powers legally granted to the Commissioner for Electronic Communications and Post Regulation, the Commissioner is free to act impartially and indepedently. However, when it comes to defence and national security issues, he is subject to the Council of Ministers.

[20] Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*).
[21] Interview with Mr. Antonis Antoniades and Ms. Vassiliki Mylona, officers at the Office of the Commissioner for Electronic Services and Post Regulation, 17 July 2014.
[22] Cyprus, Regulation of Electronic Communications and Post Services Law of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]*), 30 April 2004.

Version of 1 October 2014

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	**A definition of the categories of individuals liable to be subjected to such surveillance**	**Nature of circumstances which may give rise to surveillance**	**List purposes for which surveillance can be carried out**	**Previous approval / need for a warrant**	**List key steps to be followed in the course of surveillance**	**Time limits, geographical scope and other limits of mass surveillance as provided for by the law**	**Is the law allowing for mass surveillance in another country (EU MS or third countries)?**
Full name in English and national languages indicating its type – Act of the parliament, Government order, etc.			*National security, economic well-being, etc.…*	*Indicate whether any prior/ex post judicial warrant or a similar permission is needed to undertake surveillance and whether such approval/warrant needs to be regularly reviewed*	*See for example the principles developed by the European Court of Human Rights in the case of Weber and Saravia v. Germany*, (dec.) n°54934/00, 29 June 2006, para. 95 *Steps could include collecting data, analysing data, storing data, destroying data, etc.*	*Clearly state if there are any existing limitations in terms of nationality, national borders, time limits, the amount of data flow caught etc.*	*Please, provide details*

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)?
Cyprus, Law that Provides for the Protection of Private Communications *(Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996)*, 18 November 1996. Act of the parliament.	Article 6(2): Cases of surveillance of private communications that are being conducted by persons under imprisonment or detention or that are being conducted through illicit means.	Article 6(1): The initiation of a surveillance process (or the extension of an ongoing one) can be legally possible only after a judicial warrant which can be obtained by the Attorney General, after a request made by the Chief of the Police or the Director of the Customs and Excise Department. The Attorney General shall consent to this action only if he is persuaded that such a surveillance	Articles 8(1), 9(1): Crime prevention or investigation.	Articles 6, 7, 8: Ex post or prior judicial warrant is needed. Article 9(1): The Attorney General can order for the initiation of a telecommunications surveillance through the Cyprus Telecommunications Authority in case he will be able to proceed to the application for a judicial warrant within 24 hours. Article 8(2): The judicial warrant can provide for the specific time period	Article 13: The content of a private communication surveillance process undertaken according to the provisions of this law is stored in any suitable way (imprinted, taped, recorded on any kind of tape or printed matter or text or other suitable devise), whereas it is protected from any kind of vitiation or leak or modification or any other intervention. Right after the end of the judicial warrant's validity the surveillance content is delivered to the Attorney General	Article 8(2): The judicial warrant can provide for the specific time period of the surveillance authorization and whether surveillance is automatically terminated or not after the related communication has been recorded. Reviews are feasible if the reasons for issuing the warrant are still valid. Time extensions cannot exceed 30 days. Moreover, the judicial warrant can provide for	No

		process can provide or has provided testimony for the commitment of a crime.		of the surveillance authorization and wether surveillance is automatically terminated or not after the related communication has been recorded. Reviews are feasible if the reasons for issuing the warrant are still valid. Time extensions cannot exceed 30 days.	who provides for its safe storage. It is not destroyed unless if the Attorney General instructs accordingly and only in case it is deemed as not supportive or related to or necessary for the investigation of the crime.	the identity of the person subject to the surveillance, as well as the nature, the place (if known beforehand), and the kind of the surveillance. Article 17(1): In a reasonable time limit not exceeding 90 days after the issue of the judicial warrant, the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus). The report includes notification of the issue of the warrant, the date the warrant was issued and the	

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)?
						period of the authorized surveillance and information whether the surveillance took place or not.	
Cyprus, Regulation of Electronic Communications and Post Services Law of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [Ν. 112(Ι)/2004]*), 30 April 2004.	Not defined.	Not defined. Accroding to article 99(2) the only case an intervention to the telecommunications can be legally possible is when provided by the law and with a judicial warrant.	Not defined.	Accroding to article 99(2) the only case an intervention to the telecommunications can be legally possible is when provided by the law and with a judicial warrant. No further details included.	Not defined.	Not defined.	Not defined.

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)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*
Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*). Article 3(1): This law applies to cases of fully or partially automatic, as well as to non-automatic process of personal data processing, which is -or is about to be- included in a record.	The individual subject to personal data processing has the right to be informed of the identity of the collector, the purpose of the processing, the recipients of the data and the existance of a right to access and correct the data, during the collection stage. Moreover, it has the right to resort to the Commissioner for Personal Data Protection who can impose administrative sanctions, including warnings, fines,	Rules apply to both nationals/EU citizens and third country nationals. Article 3(3) provides that the law applies to any case of personal data processing that is being conducted by an individual who is settled in the Republic of Cyprus.	Rules apply inside the Republic of Cyprus or in any other place where the Cypriot law is implemented. Moreover, article 3(3) provides that the law applies to any case of personal data processing that is being conducted by an individual who is not settled in the Republic of Cyprus or any other member state of the Eropean Union and the European Economic Area, but for the purpose of personal data processing he/she uses means which are installed in the Republic of Cyprus, except if these means are used only in order to transfer the data through the Republic of Cyprus.

Article 4(1): Personal data must be subject to lawful process and collected for pre-defined, certain and lawful purposes. Article 5(1): Personal data may be processed only with the consent of the individual who is subject to the processing.	license revocation , destruction of a filing system and/or the cessation of processing and the destruction of the relevant data.		
Cyprus, Regulation of Electronic Communications and Post Services of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]*), 30 April 2004. Article 99(2): Outside the communicating users, none is permitted to listen, wiretap, save, intervene and/or proceed to any other form of surveillance committed through the communications network and the electronic services available to the public. The only case an intervention to the telecommunications can be	According to article 98(3) The providers of public networks or publicly available electronic communication services are oblidged to notify the office of the Commissioner for Electronic Communications and Post Regulation on every breach of security or loss of their networks' integrity which would affect their networks' or services' functioning. According to article 98A(3) a provider who notices a security threat which affects a publicly	Rules apply to both nationals/EU citizens and third country nationals. Article 3(1) provides that the law suggests the framework for the regulation of netwowrks, electronic communiations services and post services which are being provided by individuals in the Republic of Cyprus.	Rules apply only inside the Republic of Cyprus. Article 3(1) provides that the law suggests the framework for the regulation of netwowrks, electronic communiations services and post services which are being provided by individuals in the Republic of Cyprus.

possible is when provided by the Law and with a judicial warrant.	available communications network is oblidged to notify the users. According to article 31(1) the Commissioner for Electronic Communications and Post Regulation, after the submission of a complaint regarding the activities of a communications service/network provider, has the right to proceed to administrative examination of the complaint and issue legally binding decisions.		
Cyprus, Law that Provides for the Protection of Private Communications *(Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996)*, 18 November 1996. Act of the parliament.	Article 3(1): Surveillance or wiretapping of private communication, or disclosure of private communication content, or usage of such content suggest a crime that could lead to imprisonment penalty up to three years.	The law applies to cases related to individuals living or residing in the Republic of Cyprus. No conditions related to the nationality of the implicated persons are included.	Only inside the Republic of Cyprus.

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	**Type of the body/mechanism**	**Legal basis**	**Type of oversight**	**Staff**	**Powers**
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoing/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*
Office of the Commissioner for Personal Data Protection (Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).	Government	Cyprus, Processing of Personal Data (Protection of Individuals) Law (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001*). Article 23(1): The Commissioner for Personal Data Protection may conduct inspections to records kept for national security reasons.	Ex post and during the surveillance. The Commissioner has the right to execute his oversight authority ex officio, or after a complaint made by an individual who has been subject to personal data processing.	According to the Processing of Personal Data (Protection of Individuals) Law, article 18, the Commissioner is appointed by the Council of Ministers after a suggestion made by the Minister of Interior and in consultation with the parliamentary Committee for Foreign and European Affairs. The Commissioner should be a person who fulfills (or has fulfilled in the past) the criteria for appointment as a judge of the Supreme	According to the Processing of Personal Data (Protection of Individuals) Law, article 23(1), the Commissioner's powers include issuing both legally binding and non-binding decissions and recommendations, as well as reporting obligation to the Council of Ministers, the Minister of Interior and the House of Representatives.

				Court, namely at least 12 years of practice as member of the Bar and/or the judiciary. In addition he/she should have professional excellence and high moral standing. Appart from the Commissioner, the Office of the Commissioner for Personal Data Protection is staffed by nine officers and five secretarial officers.[23]	
Office of the Commissioner for Electronic Communications and Post Regulation (Γραφείο Επιτρόπου Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων).	Government	Cyprus, Regulation of Electronic Communications and Post Services Law of 2004 (*Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]*), 30 April 2004. Article 99(2): Outside the communicating users, none is permitted to listen, wiretap, save, intervene and/or proceed	Ex post. The Commissioner's oversight authority is indirect and it relates to the monitoring of the public network providers, to the degree that they notify the Commissioner of potential security breaches or if a network user issues a complaint regarding the network's integrity.	According to the Regulation of Electronic Communications and Post Services, article 5(1), the Commissioner is appointed by the Council of Ministers in consultation with the parliamentary Committee for Foreign and European Affairs. The Commissioner should have professional excellence and high moral standing and he/she should have experience and proven capacity on all, some of, or one of the issues related to	According to the Regulation of Electronic Communications and Post Services Law, articles 20 and 98A, the Commissioner's powers include issuing legally binding decisions, consulting the Minister of Communications and Works, reccommendations, as well as mediating for dispute resolution regarding disputes between providers of communications and post networks and services.

[23] http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/office_gr/office_gr?OpenDocument. Accessed 12 August 2014.

		to any other form of surveillance committed through the communications network and the electronic services available to the public. The only case an intervention to the telecommunications can be possible is when provided by the Law and with a Court permission. Article 98(2): The Commissioner acts accordingly so that the providers of public communication networks take all appropriate measures to assure the integrity of their networks. Article 98(3): The Commissioner acts accordingly so that the providers of public communication networks notify every		industry, politics, public economy and economic science in general, finance, engineering, accounting, commerce or law. Apart from the Commissioner and the Assistant Commissioner, the Office of the Commissioner for Electronic Communications and Post Regulation is staffed by 38 officers: the director, three higher officers for communications and post, three A' class officers, 14 officers for electronic communications and post regulation, 12 secretarial officers, three technical engineers and two accounting officers.[24]	

[24] Office of the Commissioner for Electronic Communications and Post Regulation, 'Budget for year 2014' (*Προϋπολογισμός για το έτος 2014*), p. 23. http://www.ocecpr.org.cy/media/documents/General/EC_Regulation_Budget_2014_Gr_14-04-2014_AV.pdf. Accessed 12 August 2014.

		breach of their security measures or loss of their networks' integrity with essential impact on their services' or networks' functioning.			
House of Representatives and Parliamentary Committees (Βουλή των Αντιπροσώπων και Κοινοβουλευτικές Επιτροπές)	Parliamentary	According to article 3 of the Submission of Data and Information to the House of Representatives and the Parliamentary Committees Law {Ο περί Καταθέσεως Στοιχείων και Πληροφοριών στη Βουλή των Αντιπροσώπων και τις Κοινοβουλευτικές Επιτροπές Νόμος [N. 21/1985 και 12(I)/1993]}, Parliamentary Committees, during the execution of their works in the context of their powers as defined by the law, are authorized to request information – written or oral- from the	Parliamentary.	The House of Representatives is elected by universal, direct, secret and compulsory vote for a five-year term of office, called a parliamentary term. Elections are general and are held on the same day throughout the state's territory. Under the Constitution, the President of the House is elected by the Representatives at the beginning and for the whole period of the above mentioned term. The House is composed by 56 Greek Cypriot MPs and 3 representatives, one representing the Armenians, another the Latins and another representing the Maronites living in Cyprus. Each MP	Amendment of the Constitution, enactment of legislation, confirmation or rejection of a proclamation of emergency, investiture of the President of the Republic, parliamentary scrutiny, co-formulation of economic and financial policy.[26]

[26] http://www.parliament.cy/easyconsole.cfm/id/146/lang/en/. Accessed on 2 September 2014.

		various public services of the Republic, from legal persons and legal entities of public law, from legal persons and legal entities of private law and from individuals and ask for the presentation of documents, public or private, which, in their opinion, could facilitate the work of a committee in the examination of a subject. Due to the lack of a law, for the time being, regulating the CIS functioning, there is no clarity about whether the CIS can be considered as a public service or not. At this stage, CIS is directly accountable to the President of the Republic. In relation to the discussion of an issue titled "The institutional role of the Central Intelligence		is supported by one assistant. Furthermore, the House is staffed by approximately 120 administrative officers, secretaries, messengers and other employees.[25]	

[25] http://www.parliament.cy. Accessed on 2 September 2014.

		Service, potential surveillance of citizens and subsequent responsibilities", which took place on the 17th of September 2013, the Parliamentary Committee on Institutions, Merit and the Commissioner for Administration (Ombudsman) invited the Director of the CIS in his capacity as the political head of the Service. Nevertheless, the bill which is currently under scrutiny by the Parliamentary Committee on Institutions, Merit and the Commissioner for Administration (Ombudsman) provides for the establishment of an independent authority which will be headed by a Commander who will be appointed by the President of the Republic and will be			

		accountable directly to him/her.			

Annex 3 – Remedies[27]

Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[Ι]/2001)				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	Yes[28]	Yes[29]	Claims lodged with the oversight body (Office of the Commissioner	Violation of data protection, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού

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

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

[28] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[Ι]/2001), article 12.

[29] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[Ι]/2001), article 12.

			for Personal Data Protection, government)[30]	Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), articles 4(1), 5(1).
Analysis*	Yes[31]	Yes[32]	Claims lodged with the oversight body (Office of the Commissioner for Personal Data Protection, government)[33]	Violation of data protection, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), articles 4(1), 5(1).
Storing*	Yes[34]	Yes[35]	Claims lodged with the oversight body (Office of the Commissioner for Personal Data Protection, government)[36]	Violation of data protection, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του

30 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12 (3).

31 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

32 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

33 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12 (3).

34 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

35 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

36 Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12 (3).

				Ατόμου) Νόμος 138[I]/2001), articles 4(1), 5(1).
Destruction *	Yes[37]	Yes[38]	Claims lodged with the oversight body (Office of the Commissioner for Personal Data Protection, government)[39]	Violation of data protection, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), articles 4(1), 5(1).
After the whole surveillance process has ended	Yes[40]	Yes[41]	Claims lodged with the oversight body (Office of the Commissioner for Personal Data Protection, government)[42]	Violation of data protection, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), articles 4(1), 5(1).

[37] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

[38] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

[39] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12 (3).

[40] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

[41] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12.

[42] Cyprus, Processing of Personal Data (Protection of Individuals) Law (Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος 138[I]/2001), article 12 (3).

Cyprus, Regulation of Electronic Communications and Post Services of 2004 (*O Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]*), 30 April 2004.				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	Yes[43]	Yes[44]	Claims lodged with the oversight bodies (Office of the Commissioner for Electronic Communications and Post Regulation, Office of the Commissioner for Personal Data Protection, government)[45]	Violation of data protection and private life, Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N.

* 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

43 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

44 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

45 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 107(2).

				112(I)/2004]), 30 April 2004, article 97(1).
Analysis*	Yes[46]	Yes[47]	Claims lodged with the oversight bodies (Office of the Commissioner for Electronic Communications and Post Regulation, Office of the Commissioner for Personal Data Protection, government)[48]	Violation of data protection and private life, Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 97(1).
Storing*	Yes[49]	Yes[50]	Claims lodged with the oversight bodies (Office of the Commissioner for Electronic Communications and Post Regulation, Office of the Commissioner for Personal Data Protection, government)[51]	Violation of data protection and private life, Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N.

46 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

47 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

48 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 107(2).

49 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

50 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 99(2).

51 Cyprus, Regulation of Electronic Communications and Post Services of 2004 (Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004 [N. 112(I)/2004]), 30 April 2004, article 107(2).

				112(I)/2004]), 30 April 2004, article 97(1).
Destruction *	N/A[52]	N/A[53]	N/A[54]	N/A[55]
After the whole surveillance process has ended	N/A[56]	N/A[57]	N/A[58]	N/A[59]

52 The law does not include any reference to such cases.
53 The law does not include any reference to such cases.
54 The law does not include any reference to such cases.
55 The law does not include any reference to such cases.
56 The law does not include any reference to such cases.
57 The law does not include any reference to such cases.
58 The law does not include any reference to such cases.
59 The law does not include any reference to such cases.

Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	Not defined[60]	Not defined[61]	Claims lodged with the courts. Disctrict Courts, judicial body.	Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.

* 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

[60] According to article 17(1), the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus) in a reasonable time limit not exceeding 90 days after the issue of the judicial warrant. The report includes notification of the issue of the warrant, the date the warrant was issued and the period of the authorized surveillance and information whether the surveillance took place or not.

[61] According to article 17(2) after an application submitted by the person subject to surveillance the court may decide to order the delivery of excerpts of the content of the private communication surveilled to the person subject to surveillance or his/her advocate.

Analysis*	Not defined[62]	Not defined[63]	Claims lodged with the courts. Disctrict Courts, juducual body.	Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.
Storing*	Not defined[64]	Not defined[65]	Claims lodged with the courts. Disctrict Courts, juducual body.	Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.
Destruction *	Not defined[66]	No[67]	Claims lodged with the courts. Disctrict Courts, juducual body.	Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του*

[62] According to article 17(1), the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus) in a reasonable time limit not exceeding 90 days after the issue of the judicial warrant. The report includes notification of the issue of the warrant, the date the warrant was issued and the period of the authorized surveillance and information whether the surveillance took place or not.

[63] According to article 17(2) after an application submitted by the person subject to surveillance the court may decide to order the delivery of excerpts of the content of the private communication surveilled to the person subject to surveillance or his/her advocate.

[64] According to article 17(1), the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus) in a reasonable time limit not exceeding 90 days after the issue of the judicial warrant. The report includes notification of the issue of the warrant, the date the warrant was issued and the period of the authorized surveillance and information whether the surveillance took place or not.

[65] According to article 17(2) after an application submitted by the person subject to surveillance the court may decide to order the delivery of excerpts of the content of the private communication surveilled to the person subject to surveillance or his/her advocate.

[66] According to article 17(1), the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus) in a reasonable time limit not exceeding 90 days after the issue of the judicial warrant. The report includes notification of the issue of the warrant, the date the warrant was issued and the period of the authorized surveillance and information whether the surveillance took place or not.

[67] According to article 17(2) excerpts cannot be delivered to the person subject to surveillance or his/her advocate if the surveillance content has been destroyed according to the providence of the law.

				Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996), 18 November 1996.
After the whole surveillance process has ended	Not defined[68]	Yes[69]	Claims lodged with the courts. Disctrict Courts, juducual body.	Cyprus, Law that Provides for the Protection of Private Communications (*Νόμος που Προνοεί για την Προστασία του Απόρρητου της Ιδιωτικής Επικοινωνίας 92(I)/1996*), 18 November 1996.

[68] According to article 17(1), the Attorney General sends a report to the person that is subject to the surveillance (in case he/she lives or resides in the Republic of Cyprus) in a reasonable time limit not exceeding 90 days after the issue of the judicial warrant. The report includes notification of the issue of the warrant, the date the warrant was issued and the period of the authorized surveillance and information whether the surveillance took place or not.

[69] According to article 17(2) after an application submitted by the person subject to surveillance the court may decide to order the delivery of excerpts of the content of the private communication surveilled to the person subject to surveillance or his/her advocate.

Annex 4 – Surveillance-related case law at national level

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

Case title	*Attorney General of the Republic v. Andrea Isaia and others*, Civil Appeal No. 402/2012, 7/7/2014.
Decision date	7 July 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Supreme Court of Cyprus (Ανώτατο Δικαστήριο Κύπρου)
Key facts of the case (max. 500 chars)	Cyprus Police asked for a judicial warrant for the revelation of an internet user's personal data, Mr. Evagoras Isaia, as he was recognised through his IP address to have hacked a Facebook account owned by Ms Kiki Polemitou without her consent. Mr. Isaia and his father, who owned the house where the computer that was used for hacking Ms Polemitou's account was positioned, appealed to the Supreme Court for a Certiorari Writ. The Certiorari Writ was issued based on two arguments: 1. That the Police should have asked for a judicial warrant before obtaining the IP address. By having obtained the IP address without a prior warrant the Police violated the applicants' rights. 2. That the IP address comprises personal data per se. An appeal was submitted to dispute both arguments.

Main reasoning/argumentation **(max. 500 chars)**	An IP address does not comprise personal data per se. It is neutral since by itself it can reveal only the network provider's identity. It could become personal data of the user only if the network provider agreed to provide the details of that specific IP address. In that case a judicial warrant should be issued. That warrant had been provided in the case under discussion, therefore the personal data revelation that followed and led to the identification of the appellees was legitimate.
Key issues (concepts, interpretations) clarified by the case **(max. 500 chars)**	An IP address does not comprise private co2mmunication detail per se, at least not before it is subject to proccessing by the network provider, therefore it is not protected by the Constitution.
Results (sanctions) and key consequences or implications of the case **(max. 500 chars)**	The Supreme Court rejected the appeal and the Certiorari Writ was cancelled. As a result of this Supreme Court decision, a request for possessing an IP address is not necessarily depedent on a prior court decision.

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**
Central Intelligence Service (Κεντρική Υπηρεσία Πληροφοριών)	Government	No contact details are publicly provided Ministry of Justice and Public Order: 125 Athalassas Av., 1461, Nicosia Tel. no. (+357)22805901/9 Fax no. (+357)22518349	No contact details are publicly provided Ministry of Justice and Public Order: www.mjpo.gov.cy
Presidency of the Republic (Προεδρία της Δημοκρατίας)	Government	Presidential Palace, 1400, Nocisia Tel. no. (+357)22661333 Fax no. (+357)22663799	www.presidency.gov.cy
Ministry of Justice and Public Order	Government	125 Athalassas Av., 1461, Nicosia	www.mjpo.gov.cy

(Υπουργείο Δικαιοσύνης και Δημόσιας Τάξης)		Tel. no. (+357)22805901/9 Fax no. (+357)22518349 Email address: minister@mjpo.gov.cy	
Cyprus Police (Αστυνομία Κύπρου)	Government	Police Headquarters, General Evaggelos Florakis St., 1478, Nicosia Tel. no. (+357)22808080 Fax no. (+357)22423217	www.police.gov.cy
Parliamentary Committee on Institutions, Merit and the Commissioner for Administration (Ombudsman) (Κονοβουλευτική Επιτροπή Θεσμών, Αξιών και Επιτρόπου Διοικήσεως)	Parliament	House of Representatives, 1402, Nicosia Tel. no. (+357)22407300 Fax no. (+357)22673066 Email address: vouli@parliament.cy	www.parliament.cy
Office of the Commissioner for Personal Data Protection (Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)	Government	1 Iasonos St., 2nd Floor, 1082, Nicosia Tel. no. (+357)22818456 Fax no. (+357)22304565 Email address: commissioner@dataprotection.gov.cy	www.dataprotection.gov.cy

Office of the Commissioner for Electronic Communications and Post Regulation (Γραφείο Επιτρόπου Ρύθμισης Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων)	Government	12 Ilioupoleos st., 1101, Nicosia Tel. no. (+357)22693000 Fax no. (+357)2222693070 Email address: Info@ocecpr.org.cy	www.ocecpr.org.cy

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

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

Independent Authority for Human Rights, 'Position of the Ombudswoman as and Independent Authority for Human Rights regarding the confrontation of demonstrations by the Police' (Τοποθέτηση Επιτρόπου Διοικήσεως ως Εθνικής Ανεξάρτητης Αρχής Ανθρωπίνων Δικαιωμάτων αναφορικά με την αντιμετώπιση συγκεντρώσεων διαμαρτυρίας από την Αστυνομία), Action 2/2012, 7 September 2012.

3. Non-governmental organisations (NGOs)

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

Tsoumis, G. (2011), *Memoirs and documents of CIS intelligence on Cyprus and the Near East* [Ενθυμήματα και τεκμήρια πληροφοριών της ΚΥΠ για την Κύπρο και την Εγγύς Ανατολή], Athens, Doureios Ippos.

Charalambidou, E. (2011), *The white pages of the Cyprus problem* [Οι λευκές σελίδες του κυπριακού], Nicosia, Parga.

Drousiotis, M. (2009), *Cyprus 1974: The Greek coup and the Turkish invasion*, Nicosia, Alfadi.