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

## GREECE

Version of 24 October 2014

Centre for European Constitutional Law (CECL)
Anna Maria Piskopani

# Summary

The summary shall provide information on the following three issues:

1. 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:

[1]. The surveillance legal framework by state actors in Greece has three aspects: a) lawful interceptions of communications following the conditions and procedures laid down by the Executive Laws of art. 19 of the Hellenic Constitution[1] which protects the freedom of communication and communications' secrecy. According the main Executive Law 2225/1994, communications secrecy may only be waived: i) for national security reasons and ii) in order to investigate particularly serious crimes; b) video surveillance; Art. 3 of Data Protection Law 2472/1997[2] exempts from the scope of the law personal data processing by state authorities via camera installations in public areas for a closed number of purposes such as the protection of state security. Art. 14 of Law 3917/2011[3] amended this provision and fully integrated any video surveillance system in the data protection law, but will come to force with the enactment of a foreseen Presidential Decree and c) mass surveillance in the context of the data retention law 3917/2011. In the context of a legal framework for mass surveillance in communications the first and third aspect will mainly be analysed.

a. types of security services and bodies involved,

[2]. The Greek state authorities with a core mission to collect, store and analyse intelligence information in order to prevent terrorist attacks and protect national security are: a) the National Intelligence Service (*Εθνική Υπηρεσία Πληροφοριών)* (EYP) b) the Intelligence Management and Analysis Division (I.M.A.D.)

---

[1] Greece, Law 2225/1994. For the protection of freedom of correspondence and communication and other Provisions *('Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις'),* (O.G. A΄ 121/20.07.1994) as amended.

[2] Greece, Law 2472/1997, 'On the protection of Individuals with regard to the processing of personal data' (as amended). *('Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα')* An English version of the law is available at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%2024 72-97-NOV2013-EN.PDF (Last accessed: 8 September 2014).

[3] Greece, Law 3917/2011, 'Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the obtaining or recording of sound or image at public areas and relative provisions' (articles 1 to 13) *('Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις')* (O.G. A΄ 22/21.02.2011). Available in Greek at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/N_3917_11_TROPOP_APRIL13.PDF (Last accessed: 8 September 2014).

(Διεύθυνση Διαχείρισης και Ανάλυσης Πληροφοριών)[4] and c) the Special Violent Crime Squad of Hellenic Police (*Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας και εγκληματολογικής έρευνας*). The National Intelligence Service (EYP) is an independent organisation which is not part of the ordinary police force and is subject to the authority of the Minister for Civil Protection (Act of Legislative Content *Πράξη Νομοθετικού Περιεχομένου* 215/2009 validated by Law 3817/2010)[5]. Although earlier National Intelligence Service' legal framework raised serious concerns about ministerial competence[6], it is now based on parliamentary legislation [Law (*Νόμος)* 3649/2008][7]. The mission of EYP is to seek, collect and process information and notify the competent authorities about protecting and promoting the country's political, economic, military and national strategic interests, preventing threats against the democratic regime, fundamental rights, territorial integrity, national security and national wealth, preventing and dealing with activities of terrorist organizations and organized crime groups (art. 2 of Law 3649/2008).

[3]. The Special Violent Crime Squad and the Intelligence Management and Analysis Division of the Hellenic police are part of the Hellenic Police (art. 15 of Law 4249/2014)[8]. The mission of the Intelligence Management and Analysis Division is

---

[4] Article 22 of law 4249/2014 which is amended by law 4281/201, as applicable, provides for the establishment of the Intelligence Management and Analysis Division in the form of an independent central Service under the Head of the Hellenic Police Headquarters. The Division started operating on 29.08.2014; the presidential decree defining the internal organizational structure and operation of the Division is expected to be issued. The Intelligence Management and Analysis Division is responsible for collecting, evaluating, filing, analyzing and providing elaborated or unelaborated information in order to address any form of crime, especially terrorism and organized crime, as well as for maintaining, updating and securing special data bases, which record and store information material, in accordance with the applicable legislation. Under the current legislative framework all services of the Hellenic Police must, during the period of time strictly necessary to this effect, send to the Intelligence Management and Analysis Division the information material collected within the framework of their mission, taking, at the same time, the necessary steps for the immediate and operational use of it, as the case may be.
The information material collected by the Intelligence Management and Analysis Division, in application of the previous paragraph, is classified on the basis of its content and importance, taking the relevant classification level and being used exclusively for carrying out the mission of the Greek Police Force, in accordance with the provisions of law 2472/1997.

[5] Greece, Act of Legislative Content 215/2009 'Classification of National Intelligence Service to Minister of Citizen Protection' *('Πράξη νομοθετικού Περιεχομένου Υπαγωγή της Εθνικής Υπηρεσίας Πληροφοριών στον Υπουργό Προστασίας του Πολίτη')* (O.G. Α΄ 215/13.10.2009). An English version of the Act is available at: www.nis.gr/npimages/docs/215-2009en.pdf (Last accessed: 8 September 2014). Law 3817/2010 'Validation of the 13 October 2010 Act of Legislative Content 215/2009 Classification of National Intelligence Service to Minister of Citizen Protection' *('Κύρωση της από 13 Οκτωβρίου 2010 Πράξης Νομοθετικού Περιεχομένου 'Υπαγωγή της Εθνικής Υπηρεσίας Πληροφοριών στον Υπουργό Προστασίας του Πολίτη')* (O.G. Α΄ 16 /16.02.2010).

[6] Apostolidis P., (2007) *Intelligence services in the National Security System. The case of NIS*, (*Υπηρεσίες πληροφοριών στο Εθνικό Σύστημα Ασφάλειας. Η περίπτωση της ΕΥΠ)*. Occasional Paper, Hellenic Foundation for European and Foreign Policy, 2007, p.18. An English version of the Paper is available at: www.eliamep.gr/wp-content/uploads/en/2008/10/op07_03_eng.pdf. (Last accessed: 8 September 2014).

[7] Greece, Law 3649/2008, 'National Intelligence Service and other provisions', ('*Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις'*) (O.G. Α΄ 39/03.03.2008). As amended.

[8] Greece, Law 4249/2014 'Reorganising Hellenic Police, Fire Department, General Secretary for Civil Protection, upgrade of services at the Minister for Public Order and Citizen's protection and regulation of issues for competence for Minister of Public Order and Citizen's protection and other provisions. ('*Αναδιοργάνωση της Ελληνικής Αστυνομίας, του Πυροσβεστικού Σώματος και της Γενικής Γραμματείας*

to collect and analyse information to counter any form of criminal action, especially terrorism, and keep up to date databases of information collected (art. 22 of Law 4249/2014). All directorates of the Hellenic Police are obliged to send all information to this directorate. This directorate is supervised by a public prosecutor who is the President of the Scientific Council for Analysis, Research and Programming to deal with organised crime.

b. the extent of their powers in case of surveillance of individuals and also vis-à-vis the private sector (right to access to data held by telecom or internet providers, right to refuse access),

[4]. For the purposes of investigation, detection and prosecution of crimes and national security purposes law enforcement bodies can request access to communications (as provided for by special legal laws and the Greek Procedural Penal Code).

[5]. In order for EYP to fulfil its abovementioned mission, it can request the lifting of confidentiality of communication and record the activities of individuals using special technical media, especially audiovisual devices, outside residences (art. 5 of Law 3649/2008). The legal requirements and procedure for the lawful interception required by NIS are described in arts 3 and 5 of Law 2225/1994.

[6]. The communications covered by the scope of confidentiality are described in Law 3471/2006[9], Presidential Decree 47/2005[10] and article 370A of the Penal Code. According to Law 3471/2006, any use of electronic communications services offered through a publicly available electronic communications network, as well as any pertinent traffic and location data, as described in art. 2 of the present law, shall be protected by the principle of confidentiality of telecommunications. Presidential Decree 47/2005 provides the details for the technical and organizational measures for any lawful interception. Law enforcement agencies can also have access to traffic and location data already retained as described in Law 3917/2011 only for the purpose of combating serious crimes according to the procedure described in art. 4 of Law 2225/1994. The Law has transposed Directive 2006/24/EC (Data Retention Directive) into national law.

[7]. Although Law 3917/2011 and Law 3471/2006 state that traffic and location data fall under the constitutional protection of freedom of communication and communications secrecy, there is an ongoing dispute regarding this issue. The Hellenic Authority for Communication Security and Privacy (A.D.A.E. Decision 1/2005), Courts [Council of State *(Συμβούλιο της Επικρατείας)* EA 456/2007] and

---

*Πολιτικής Προστασίας, αναβάθμιση Υπηρεσιών του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη και ρύθμιση λοιπών θεμάτων αρμοδιότητας Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη και άλλες διατάξεις'*) (O.G. A΄ 73/24.3.2014) as amended.

[9] Greece, Law 3471/2006 'Protection of personal data and privacy in the electronic telecommunications sector and amendment of Law 2472/1997'*, ('Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του 2472/1997'),* (O.G. A΄ 133/28.06.2006).

[10] Greece, Presidential Decree 47/2005. 'Procedure, technical and organizational guarantees for ensuring lawful interception' ('*Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του'*) (O.G. A΄ 64/10.03.2005).

the scientific community[11] support that external elements of communication including traffic and location data are constitutionally protected by Article 19 of the Hellenic Constitution. The Public Prosecutor's Office for the Supreme Civil and Criminal Court *(Άρειος Πάγος)* expresses the opposite opinion (in Opinion 9/2009, 12/2009, 9/2011, Circular 1/2013). According to the Public' Prosecutor Office, judicial authorities and law enforcement agencies are entitled to request that providers provide access to traffic and location data of both internet and telecom communications (such as IP addresses and names and addresses of telecom users in case of malicious calls and messages, Opinion 12/2009) without the requirements and procedure set out in Law 2225/1994. In order for this to happen, there should be in place a judicial investigation, or preliminary examination or investigation following Prosecutor's Order.

[8]. Regarding the right of telecom and internet providers to refuse: a) according to article 8 of the Presidential Decree 47/2005, providers of services and networks of communication are obliged to respond directly to every request to lift confidentiality communicated to them by competent authorities, b) according to article 5 para 11 of Law 2225/1994, employees of services requested to lift confidentiality shall be punished if they do not provide the necessary information relating to the content of the order and respective technical support, c) according arts 1 and 4 of Law 3917/2011 providers of electronic communications services or public network of communications are obliged to provide any retained traffic and position data to competent authorities for the purpose of verifying serious crimes. Access can be refused if there is no judicial order.

[9]. EYP can request from state authorities such as the police and coastguard information in the context of preliminary investigations and interviews in order to fulfil its above mentioned mission (art. 6 of Law 3649/2008). According to the a recent Opinion of the Supreme Civil and Criminal Court Public Prosecutor's Office[12], EYP authorized officers can request from investigating officers, orally or in writing, information from the case file (Opinion 7/2014). The investigating officers provide the requested information after they inform orally the Public Prosecutor who supervises the preliminary investigation.

c. control/oversight mechanisms

[10]. The National Intelligence Service (EYP) is supervised by a public prosecutor, specially appointed to the service, who controls the legality of its special operational activities as set out in art. 5 of Law 3649/2008. Parliamentary control is directed at the political supervisor of EYP, the Minister for Public Order and Civil

---

[11] Nouskalis G. (2012), The processing of external telecommunications position and traffic data traffic as inquisition act of investigation under L.3911/2011 *(Η επεξεργασία των εξωτερικών τηλεπικοινωνιακών δεδομένων θέσης και κίνησης ως ανακριτική πράξη έρευνας κατά τον Ν. 3917/2011),* Penal Chronicles p. 247, (In Greek).

[12] Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) Opinion 7/2014, (*Γνωμοδότηση 7/2014*). Available at: http://eisap.gr/sites/default/files/consulations/ΓΝΩΜΟΔΟΤΗΣΗ%2070001.pdf .(in Greek) (last accessed 23/10/2014).http://eisap.gr/sites/default/files/consulations/ΓΝΩΜΟΔΟΤΗΣΗ%2070001.pdf .(in Greek) (last accessed

Protection, according to the Standing Orders of the Hellenic Parliament (questions, interpellations, updated questions). Additionally, parliamentary control is exercised by the Special Permanent Committee on Institutions and Transparency of the Hellenic Parliament which is responsible for supervising the EYP, as stated in art. 43 A para. 2 point (b) of the Standing Orders of the Hellenic Parliament (paragraph 3 of the article 11 of the Decision 693/2008). Among its powers are to call and examine persons and invite the Director General of EYP for a hearing in the presence of the Minister (paragraph 3 of the article 11 of Decision 693/2008). The Special Permanent Committee on Institutions and Transparency of the Hellenic Parliament can also collect information and documents (art.43 of Standing Orders of the Hellenic Parliament).

[11]. The Hellenic Authority for Communication Security and Privacy" (A.D.A.E.) is the independent administrative authority responsible for overseeing the lawful interception of communications (Law 3115/2003). One of the Hellenic Authority for Communication Security and Privacy's competences is to inquire, conduct inspections and audits at the premises, equipment, archives, databases and documents of the Hellenic National Intelligence Service (EYP) (art. 6 para. 1a of Law 3115/2003).

[12]. The additional obligation of the Hellenic Authority for Communication Security and Privacy is to publish and submit to the Ministry of Justice Transparency and Human Rights and Parliament (Special Permanent Committee on Institutions and Transparency) annual reports about its function, acts and the statistical data regarding requested interceptions (art. 1 para 2 of Law 3115/2003). According to A.D.A.E Annual Report 2013, 23,655 interceptions were accepted by judicial authorities, and 2,371 were rejected[13]. According to A.D.A.E. Annual Report 2012, 29,523 interceptions were accepted by judicial authorities and 676 were rejected[14]. In addition, according to A.D.A.E. Annual Report 2013, 4,141 prosecutors' orders were requested for national security purposes, against 2,634 orders requested in 2012[15]. According to art. 6 para 1 of Law 3115/2003, the A.D.A.E. can only monitor the procedure for waiving confidentiality in compliance with the procedure and requirements of articles 3, 4, 5 of Law 2225/1994 but is not allowed to assess the judgment of competent judicial authorities. On the occasions described in articles 3, 4 and 5 of Law 2225/ 1994, the A.D.A.E only monitors compliance with the terms and the procedures for waiving of communication confidentiality, without taking into consideration the judgment of the competent judicial authorities. The A.D.A.E. can only monitor the procedure not the substance of the applicant waiving of confidentiality. Only the competent judicial authority can decide on the necessity for the waiving of confidentiality.

[13]. According to the Data Retention Law, The Hellenic Data Protection Authority has responsibilities regarding the protection of personal data according to a set of data protection principles and rights (Law 2472/1997) while A.D.A.E. has to ensure the

---

[13] Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών) (*2013). Annual Report 2013 (*Ετήσια Έκθεση 2013)*, p.56.

[14] Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών) (*2012). Annual Report 2012 (*Ετήσια Έκθεση 2012)*, p.51.

[15] Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών) (*2011). Annual Report 2011 (*Ετήσια Έκθεση 2011)*, p.49.

application of the legal framework for the protection of confidentiality of communications and for the lawful interception (Law 3115/2003). But as traffic and location data are considered communications and personal data the law allocates shared competences (articles 7 para 2, 9 and 12 para 2) and overlapping responsibilities (articles 7 para 2, 8 para 2 and 9) to two independent administrative authorities. Common supervision by two understaffed authorities may result in inconsistencies and a lack of efficiency of the oversight mechanism[16]. It took more than 2 years for these two Authorities to issue a Joint Act regarding the obligations of providers for the protection and security of retained data.

d. geographical scope of surveillance

[14]. The geographical scope of surveillance is defined by the application and is included in the judicial order and the report compiled by the service that performed the waiving of confidentiality (Law 2225/1994 and Pres. Dec. 47/2005). The data retention law covers all data produced and stored by natural means on Greek territory for a limited duration of 12 months (art. 6 of Law 3917/2011). Therefore the addressees of the obligation are providers established in Greece that operate under a General Authorisation regime and are registered on the Registry of Electronic Communication Network and Service Providers kept by the Hellenic Communications and Post Commission according to Law 4070/2012[17].

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

[15]. In general, as mentioned above, in order to lawfully conduct surveillance of communications, law enforcement agencies have to follow the procedures described by Executive Law 2225/1994 for art. 19 of the Hellenic Constitution. The investigating judge, or prosecutor or law enforcement agencies such as the police can waive confidentiality in order to verify specific criminal offences (mainly felonies). Lawful interception is ordered by the Judicial Council (consisting of three judges). In case of emergency the prosecutor or investigating judge issues an order which has to be confirmed by the Judicial Council within three (3) days. The particular conditions for lawful interception in this context are justified suspicions of a crime having been committed, the need to trace the location of the suspect and prior exhaustion of all other means (art. 4 of Law 2225/1994). Lawful interception can request information or other elements which lead to the estimation of danger for national security purposes, and in this case the order is issued by the Prosecutor of Court of Appeals (arts. 3 and 5 of Law 2225/1994). The law does not define national security or specify circumstances of surveillance. According to Law 2225/1994, when public authorities such as law enforcement agencies request the waiver of confidentiality for the purpose of verifying crimes, the judicial order should include the suspect's name, address (if

---

[16] Tsiftsoglou A. /Spyridon Flogaitis, (2012), 'Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe, Values and Freedoms in Information Law & Ethics', p. 10. Available at: http://works.bepress.com/anna_tsiftsoglou/1/ (Last accessed: 8 September 2014).

[17] Greece, Law 4070/2012 'Regulation of Electronic Communications, Transportations, Public works and other provisions, *('Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων έργων και άλλες διατάξεις')*, (O.G. A82/10.04.2012), available at: gnto.gov.gr/sites/default/files/N_4070_2012.pdf

known) and the judge's reasoning. The law does not include a specific provision for national security purposes. According to art. 3 para. 2, following a request by the competent authority, the Prosecutor of the Court of Appeals can decide to omit other elements of the issuing order for national security reasons[18].

[16]. According to recently amended art. 22 para. 6 of Law 4249/2014, in exceptional cases in the course of preliminary investigations and interviews conducted in the context of the competences of the Intelligence Management and Analysis Division of the Hellenic police or/and Special Violent Crimes Squad. In these cases, a Public Prosecutor who is the President of a Scientific Council of Analysis, Research and Programming to deal with organised crime can submit the application for the waiving of confidentiality to the Council of Appeals which has to decide on the waiving of confidentiality within 48 hours (art.6 of Law 2713/1999 and art. 3 of Law 2225/1994). In extremely exceptional cases, the waiver can be decided by the Public Prosecutor himself. Its order only details: a) the Authority issuing the warrant, b) the applicant public authority and c) the date the order was issued.

[17]. According to the data retention law, traffic and location data for communications are retained by telecom and internet providers for a period of 12 months (including unsuccessful call attempts). Law enforcement agencies such as the police can access this data under the provisions of art. 4 of Executive Law 2225/1994. They can access this data for limited purposes (mainly felonies) and Art. 3 of Law 2225/1994 provides for the lifting of privacy/waiving of confidentiality for national security purposes.

[18]. According to article 5 para. 1 of Law 3649/2008, the procedure that NIS personnel have to follow in order to waive confidentiality by order of the public prosecutor for correspondence and telephone calls or other communications and record the activities of individuals using special technical media, especially audiovisual devices outside residences, is described in detail in compliance with Law 3115/2003 that has amended Law 2225/1994. The order is issued by the supervising public prosecutor, and must be submitted for approval within twenty-four hours to the competent public prosecutor for the Court of Appeals. The order shall enter into force when approved by the public prosecutor for the Court of Appeals. Also, EYP may collect information on matters of national security by infiltration, following an order issued by the Director General of the National Intelligence Service and with the approval of the supervising public prosecutor. In this case, the National Intelligence Service has to comply with the provisions of Law 3115/2003 that amended the Law 2225/1994.

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

[19]. As a public authority, the National Intelligence Service (NIS) (art 5. para.1a of Law 3649/2008) is obliged to comply with the provisions for protecting privacy set out in Law 2472/97, Law 3471/2006 and Law 3115/2003 when collecting and

[18] According to investigative journalism, this leads to time and place judicial orders and massive interceptions. Greece, Enet, 'Massive interceptions', *('Μαζικές άρσεις απορρήτου')*, 10 May 2010, available in Greek at: www.enet.gr/?i=news.el.article&id=160538 (Last accessed: 8 September 2014).

processing personal data. A.D.A.E. supervises the waiving of secrecy for the communication and the Hellenic Data Protection Authority (H.D.P.A supervises compliance with the data protection law. It performs files audits, examines complaints, reports violations and issues decisions regarding right of access. NIS as controller has the obligations of controllers described in data protection law 2472/1997 and law 3471/2006 protecting data protection in electronic communications. Therefore the EYP has to comply with the principles of collection, processing and destroying of data set out by those laws. The EYP is obliged to delete data when processing is no longer necessary for legitimate purposes or classify them. Regarding the declassification of information, according to art. 3 para. 4b. of Law 3649/2008, the EYP Historic Archives Service classifies and develops documents and audiovisual material. Such material can be declassified after 50 years on the decision of the EYP Director unless it expires or may harm national interests or privacy rights.

[20]. Regarding video surveillance conducted by state authorities, as a consequence of a dispute that took place between the Data Protection Authority and the Police Authority that planned to use CCTV cameras (originally installed to monitor traffic during the Athens Olympics) to monitor public gatherings such as protests, the Data Protection Law was amended so as to exclude surveillance via CCTV cameras from its scope. According to article 3 of Law 2472/1997 video surveillance is defined as a sound or image recording using special technical devices with a view to verifying crimes against life, sexual freedom, crimes involving the economical exploitation of sexual life, crimes against personal freedom, property and violations regarding drugs plotting against public order as well as crimes against minors is excluded from the scope of the law. In addition, the processing of personal data carried out by a public authority using special technical devices for the recording of sound or image in public areas with the aim of safeguarding the security of the state, national defence, public security, the protection of persons and property, the management of traffic is also excluded from its scope. The purpose of national security is not included.

[21]. Before the amendment, the H.D.PA. was asked to review the proposed legislation. It drafted Opinion 1/2009 arguing that the law does not provide sufficient safeguards by exempting police surveillance in public places from the supervision of H.D.P.A. As a response to H.D.P.A. (Opinion 2/2010) and scientific community' concerns regarding the constitutionality of the amendment[19], art. 14 of Law 3917/2011 was introduced and fully reintegrates any video surveillance system into the general data protection law 2472/1997. The Law states that after H.D.P.A. has expressed its opinion a Presidential Decree will specify the competent state authorities, procedure and circumstances of surveillance and criteria for compliance with the principle of proportionality. The foreseen Presidential Decree shall substitute the above mentioned provisions of Law 2472/1997 but is still has not been enacted and therefore art.3 of Law 2472/1997 still applies.

[19] Anthopoulos Ch. (2010), 'The electronic surveillance of public assemblies. Political privacy and public anonymity in Greece' in Akrivopoulou C./Psyfkas A., *Personal Data Privacy and Protection in a surveillance era. Technologies and Practices*, IGI Global, p. 61.

[22]. Regarding the access of law enforcement agencies to retained data: after the 12 months period of storage of data retention data, an automated destruction procedure is followed by service providers. Data that has been legally accessed is excluded and preserved. When service providers are notified by the competent judicial authority that the purpose of data retention has ceased to exist, they are obliged to destroy this data in a short period of time (10 days).

2. 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.)

[23]. Law enforcement agencies and EYP investigation in communications where confidentiality has been waived, is secret, so the target will not be notified. According to art. 5 para 9 of Law 2225/1994, after the measure of confidentiality has ended, the Hellenic Authority for Communication Security and Privacy can notify the targets of investigations on condition that the initial purpose of investigation is not compromised. Collected material can be used for the prosecution. If the target can be notified, material can be returned to him/her. Otherwise the material is destroyed in the presence of the authority that ordered the interception. Material not associated with the reason for imposing the lift of confidentiality must be destroyed.

[24]. Otherwise former investigation targets will be notified of the interception of their communications and collection of communications data only, if and when they are accused of a crime and during judicial investigation and asked for an apology, then they will be informed about the results of the previously conducted secret investigation against them. They will also have access to the order that enabled the investigation.

[25]. In addition, as mentioned above, the EYP (as provided for in art 5. para.1a of Law 3649/2008) is obliged to comply with the provisions for protecting privacy set by Law 2472/97, Law 3471/2006 and Law 3115/2003 and respect the individuals' rights set out in those laws. So the subjects of investigation are entitled to know whether personal data related to them has been processed and request for it to be corrected, erased or blocked (art.12 of Law 2472/1997). Subjects cannot access those files if they have already been deleted according the procedure described in art. 5 para. 9 of Law 2225/1994. In addition, if the files are not deleted by virtue of a decision by the H.D.P.A., on application submitted by EYP, its obligation to inform may be lifted, provided it proves that the processing of personal data in whole or in part was carried out on grounds of national security reasons or for the detection of serious crimes. In this case the President of the Data Protection Authority or his substitute carries out all necessary acts and has free access to the files (art.12 para. 5 of Law 2472/1997). Also according to art. 4 of Law 2472/1997, by virtue of a decision by the H.D.P.A. the obligation to inform may be lifted in whole or in part provided that the data processing is carried out for reasons of national security or for the detection of particularly serious crimes. In a stage of emergency said obligation may be lifted by way of provisional, immediately enforceable judgement by the President of H.D.P.A. who shall convene as soon as possible the Board in order that a final judgement on the matter may be issued.

[26]. As a public authority, the Hellenic Police has the obligations provided by Law 2472/1997 and Law 3471/2006 to respect data protection and privacy rights. According to art. 22 of Law 4249/2014, the Intelligence Management and Analysis Division of the Hellenic police has to comply with Law 2472/1997 regarding the data analysis of information for combating crime. The police's obligation to respect Law 2472/1997 during and after surveillance deferred on two occasions: A) According to current legal framework, state authorities as law enforcement agencies can conduct video surveillance in public areas, for the limited purposes defined by the law such as security of the state only after receipt of an order issued by the public prosecutor representative and provided a serious danger to the public order and security is imminent. The processing of data which is not necessary for the verification of those crimes shall be prohibited and destroyed following an order by the Public Prosecutor (art. 3 of Law 2472/1997). Those safeguards might be amended after the foreseen Presidential Decree as analysed above, B) In addition, the police conduct surveillance under the supervision of judicial and public prosecution authorities in the framework of attributing justice. In this case and only when the aim is to verify crimes which are punished as felonies or misdemeanours with intent and especially with the aim of verifying crimes against life, against sexual freedom, crimes involving economic exploitation, crimes against personal freedom, property, violations of regulation regarding plotting against public order as well as crimes against minors, those activities are excluded from the scope of Law 2472/1997. The main safeguard in this case is the supervision of the procedure by judicial and public prosecutor authorities (art.3 of Law 2472/1997).

[27]. Regarding the Data Retention Law safeguards, in accordance with art. 7, the H.D.P.A. and A.D.A.E. have issued a Joint Act No 1/2013 specifying the obligations of the providers in relation to the security measures in accordance with article 7 of Law No 3917/2011 (O.G. B 3433/ 31.12.2013). According to this Act the providers have to respect the following data security principles: a) retained data shall be of the same quality and subject to the same security and protection as data on the network, b) the data shall be subject to appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure, c) the data shall be subject to appropriate technical and organizational measures to ensure that it can be accessed by specially authorised personnel only and d) the data, except for that accessed and preserved, shall be destroyed at the end of the period of retention.

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

[28]. Individuals subject to surveillance can lodge a complaint with the oversight body, the Hellenic Authority for Communication Security and Privacy, requesting it to monitor the legality of the interception. If EYP's personnel has violated the confidentiality of communications or the conditions and procedure of lawful interception, penal sanctions include punishment by imprisonment for up to 2 years and a fine of at least 30,000 euros (art.10 of Law 3115/2003). EYP's personnel are subject to duty of confidentiality (article 4 of law 3649/2008). The violation of the confidentiality duty shall be punished by imprisonment of at least one (1) year and a monetary fine ranging from € 20.000,00 to € 500.000,00, provided that the act is not punished more severally pursuant to any other provision (art.14 of law

3649/2008). The individual can also request compensation for damages caused (based on art. 105 of the Civil Law Code). In addition, the A.D.A.E. can impose administrative sanctions on liable individuals or legal entities (art.11 of Law 3115/2003). The definition of legal entities is not provided by this law and the courts have not decided whether the A.D.A.E. can impose administrative sanctions on the EYP and law enforcement agencies. Only the Law 3674/2008 "Reinforcement of the institutional framework for the assurance of privacy of telephone communications and other provisions", which aims to guarantee the secrecy of fixed and mobile telephony services, specifies that the A.D.A.E. can impose administrative sanctions only on telecom providers (art.11).

[29]. In case of an illegal interception, the individual can appeal to civil courts according to art. 105 of the Civil Code and art. 23 of Law 2472/1997 and art. 14 of Law 3471/2006. There are penal sanctions by courts according to: art. 10 of Law 3115/2003, art. 11 of Law 3917/2011, art. 15 of Law 3471/2006, and arts. 292 A and 370 A of the Penal Code.

[30]. Lastly, Law 3917/2011 regulating retained data provides strict criminal sanctions for data security breaches (art. 11). Those who illegally collect and process retained data can be charged with felonies and financial penalties by administrative authorities and courts. Specifically, the A.D.A. E. can impose fines on providers for the violation of arts 3, 4, 5, 6, 7, 8 of Law 3917/2011 (art.12). There are provisions for civil liability for possible damages caused (art. 13). In its Judgment on joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others (8 April 2014), the European Union Court of Justice has declared the Data Retention Directive invalid. The declaration of its invalidity takes effect from the date on which the Directive entered into force. According to the Statement on the ruling of the court adopted by 29 Working Group on 1 August 2014, the national measures based on the invalid directive were not directly affected by this ruling, So member states of the European Union such as Greece need to evaluate the consequences of the court decision in national law. In July 2014, a scientific committee was appointed by a decision of the Greek Minister for Justice, Transparency and Human Rights to review Law 3917/2011 and propose the necessary amendments.

*BIBLIOGRAPHY*

Anthopoulos H. (2010), 'The electronic surveillance of public assemblies. Political privacy and public anonymity in Greece' in Akrivopoulou C./Psyfkas A., *Personal Data Privacy and Protection in a surveillance era. Technologies and Practices*, IGI Global, pp.59-68.

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών) (*2011). Annual Report 2011 (*Ετήσια Έκθεση 2011)*. available in Greek at: www.adae.gr/ektheseeis-pepragmenon/leptomereies/article/ekthesi-pepragmenon-toy-etoys-2011-tis-adae/(Last accessed: 8 September 2014).

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών)* (2012). Annual Report 2012, (*Ετήσια Έκθεση 2012),* available in Greek at: www.adae.gr/ektheseeis-pepragmenon/leptomereies/article/ekthesi-pepragmenon-toy-etoys-2012-tis-adae/(Last accessed: 8 September 2014)

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης Απορρήτου Επικοινωνιών)* (2014). Annual Report 2013, (*Ετήσια Έκθεση 2013)*, available in Greek at: www.adae.gr/ektheseeis-pepragmenon/leptomereies/article/ekthesi-pepragmenon-toy-etoys-2013-tis-adae/(Last accessed: 8 September 2014).

Greece, Hellenic Data Protection Authority and Hellenic Authority for Communication Security and Privacy, Joint Act regarding the obligations of providers for the protection and security of data according the provisions of article 7 of Law 3917/2011 as it remains in effect. *('Κοινή πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και της Αρχής Διασφάλισης των Επικοινωνιών ως προς τις υποχρεώσεις των παρόχων για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του Νόμου 3917/2011 όπως ισχύει')* (O.G. B΄ 3433/31.12.2013) available at: www.adae.gr/fileadmin/docs/nomoi/prakseis/koini_praxi_ADAE_DPA_FEK_3433_B_31_12_2013.pdf8 September 2014 (Last accessed: 8 September 2014).

Apostolidis P., (2007) 'Intelligence services in the National Security System. The case of NIS', ('*Υπηρεσίες πληροφοριών στο Εθνικό Σύστημα Ασφάλειας. Η περίπτωση της ΕΥΠ')*. Occasional Paper, Hellenic Foundation for European and Foreign Policy, 2007. An English version of the Paper is available at: www.eliamep.gr/wp-content/uploads/en/2008/10/op07_03_eng.pdf.( Last accessed: 8 September 2014)

Kaiafa-Gbanti M. (2010), *Surveillance Models in the Security State & Fair Criminal Trial* [in Greek], (*Μοντέλα Επιτήρησης στο κράτος ασφάλειας και δίκαιη ποινική δίκη)* Nomiki Vivliothiki Publications.

Mitrou L.(2008), 'Data retention: a Pandora's Box for Rights and Liberties?' in A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis, C. Lambrinoudakis (eds), *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications pp. 410-433.

Mitrou L. (2010), 'The Impact of Communications Data Retention on Fundamental Rights and Democracy – The Case of the EU Data Retention Directive' in: Haggerty D. & Samatas M. (eds.), *Surveillance and Democracy*, Routledge.

Greece, Enet, 'Massive interceptions', *('Μαζικές άρσεις απορρήτου')*, 10 May 2010, available in Greek at: www.enet.gr/?i=news.el.article&id=160538 (Last accessed: 8 September 2014).

Nouskalis G. (2012), 'The processing of external telecommunications data traffic as an act of investigation under Law 3911/2011' *('Η επεξεργασία των εξωτερικών τηλεπικοινωνιακών δεδομένων θέσης και κίνησης ως ανακριτική πράξη έρευνας κατά τον Ν. 3917/2011'*, Penal Chronicles, pp. 246-249 (In Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 9/2009' *('Γνωμοδότηση 9/2009')*, Penal Chronicles, 2010 p. 498 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 12/2009' *('Γνωμοδότηση 12/2009'),* Mass Media & Communication Law Review, 2 /2009 p. 393 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 9/2011' ('*Γνωμοδότηση 9/2011'*), Penal Chronicles, 2011 p. 714 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) Circular 1/2013 (Εγκύκλιος 1/2013) Penal Chronicles, 2013 p.307 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) Γνωμοδότηση 7/2014. Available at: http://eisap.gr/sites/default/files/consulations/ΓΝΩΜΟΔΟΤΗΣΗ%2070001.pdf .(in Greek) (last accessed 23/10/2014).

Tsiftsoglou A. / Spyridon Flogaitis, (2012), 'Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe, Values and Freedoms in Information Law & Ethics'. Available at: http://works.bepress.com/anna_tsiftsoglou/2/ (Last accessed: 8 September 2014).

Tsolias G. (2008), 'Personal data in electronic communications domain and reverse investigation for reasons of certification of particularly serious crimes', *(Δεδομένα προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών και «αντίστροφη αναζήτηση» αυτών για λόγους διακρίβωσης ιδιαίτερά σοβαρών εγκλημάτων. Εξ αφορμής της υπ. Αρ. 19/2008 απόφασης ΑΠΔΠΧ Προσωπικά Δεδομένα* '), Mass Media & Communication Law Review, 2 [in Greek], pp. 175-183.

Tsolias G. (2010) *'Protection of confidentiality and personal data in the telecommunications sector' ('Προστασία του απορρήτου και των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών')* in C. Lambrinoudakis, L. Mitrou, S. Gritzalis, S. K. Katsikas, (eds), *Privacy and Information and Communication Technologies: Technical and Legal Issues. (Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών. Τεχνικά και Νομικά Ζητήματα),* Papasotiriou Pubs. (in Greek), pp. 679-701.

Tsolias G. (2013), 'Privacy, Data Retention And Data Protection In The Electronic Communications Sector - Providers Of Publicly Available Electronic Communications Services - Competent Supervisory Independent Administrative Authorities' in Greek Lawyers' digest, available at: www.greeklawdigest.gr/topics/technology-media-electronic/item/84-privacy-data-retention-and-data-protection-in-the-electronic-communications-sector-providers-of-publicly-available-electronic-communications-services-competent-supervisory-independent-administrative-authorities (Last accessed: 8 September 2014).

Fountedaki P., Tsolka O., Chanos A. (eds), (2010), *Freedoms, Rights & Security in EU ('Ελευθερίες, δικαιώματα και ασφάλεια στην Ε.Ε.')* [in Greek], Nomiki Vivliothiki.

# 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<br>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 |
| Greece, Law 2225/1994 For protection of freedom of correspondence | Individuals whose confidentiality has been lifted by a judicial order. | A) Investigation for reasons of national security (arts.3 and 5 para.1). | A) For national security (arts.3 and 5).<br>B) To verify serious crimes | A) A judicial order for national security purposes must have been issued by the | A) In the course of surveillance for national security purposes the first steps are: a) an | According to article 5 para 6, the time duration of the waiving of confidentiality | No, there is no such reference in the law. |

| 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)? |
|---|---|---|---|---|---|---|---|
| and communications and other provisions. *('Για την προστασία της ελευθερίας της ανταπόκρισης και άλλες διατάξεις')* (O.G.A' 121/20.07.1995). As amended | According to art. 4 para.3 and article 5 para. 2, the judicial order shall specify the targeted individuals. Therefore includes: a) name, b) address (in case is known) and c) the Judge's reasoning for ordering the lifting for the | B) During pre-trial and during trial criminal procedure to combat serious crimes. The particular conditions for lawful interception in this context are justified suspicions of committing the crime, need to trace the location | (art.4).[20] | Prosecutor of Court of Appeals (art.3 and 5).<br>B) In case of serious crimes competent to issue the order is a judicial council. In case of emergency the prosecutor or the investigating judge issues an order which has to be confirmed by the judicial council within three days | application by the judicial, military public authority and police, b) the prosecutor of Court of Appeals must decide whether to lift confidentiality or not within 24 hours .<br>B) In the course of surveillance for verifying serious crimes, the first steps are: a) an application by investigating judge, prosecutor, or | cannot extend beyond two months. Any extension of this duration cannot exceed every time two months. Extensions may be ordered using the same procedure on the condition that the reasons for the lift are still valid. In any case the extension cannot | |

[20] The list of crimes for which lawful interception is permitted includes: 1) crimes provided for in the by penal code such as: a) crimes against the constitution, as high treason, treason and preparatory acts, damage to the integrity of the country, military service for the enemy, violation against of international peace in the country, violation of state secrets, spying, b) crimes against political parties and the government, such as violence against a political party or Government and bribery, c) threats to public order such as criminal organization and terrorist acts, d) offences relating to currency such as forgery, d) offences relating to bribery service for lawful acts, e) commonly dangerous crimes such as arson, explosion, f) crimes against life such as intentional homicide, g) crimes against personal freedom such as abduction, human trafficking, h) crimes against sexual freedom and crimes of economic exploitation of sexual life such as rape, child pornography, pimping, trafficking and i) crimes against property such as distinguished theft, robbery and property rights such as extortion, 2) Also includes crimes provided for in special penal laws such as possession of weapons in prisons, drug dealing, smuggling, and special penal laws protecting the environment, the antiquities and the cultural heritage. (Last amended with by art. 15 of Law. 4267/2014 'Combating sexual abuse and exploitation of children and child pornography and other provisions', *('Καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις'*) (O.G. A΄ 137/12.6.2014).

| 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)? |
|---|---|---|---|---|---|---|---|
| | purpose of investigating serious crimes. The law does not include such specific requirement for issuing an order for national security purposes. According to art. 5 para. 1, in the event that an order is issued, it should include elements regarding who decided the lift, who requested the lift, the purpose, the medium of correspondence or communication | of the suspected defendant and prior exhaustion of all other means (art.4). | | (art.4). | law enforcement agencies, b) an order by a judicial council or a prosecutor (in this case has to be confirmed by the judicial council within three days). The next steps in both occasions are: an official copy of the order is delivered in a closed envelope to a) the president, administrative council, general director or representative of the responsible legal entity responsible for waiving confidentiality In the event of the order referring to an individual enterprise, it is given to an | exceed 10 months. This absolute maximum time limit does not apply in cases where the lifting of confidentiality is ordered for reasons of national security. The time duration and geographical scope of the lift is described in the issuing order according to article 5 para.1. These elements can be omitted for national security purposes (art.3). In addition, time duration and | |

| 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)? |
|---|---|---|---|---|---|---|---|
| | on which the lift is imposed, the geographical scope and time duration and the publication's date of the order. In addition according to art. 3 para.2, after an application by the Authority the Prosecutor of the Court of Appeals can decide to omit or quote concisely other elements of the issuing order in special circumstances of national security. | | | | individual the entrepreneur and lastly a full text is given to the Hellenic Authority for Communication Security and Privacy. After the confidentiality has been lifted, one or more reports are compiled by the service that performed the lifting of the confidentiality. Copies of these reports are delivered to the applicant judicial authority, and Hellenic Authority for Communication Security and Privacy. After the end of the | geographical scope are included in the report of the service performing the lift of confidentiality (art. 5 par.5). | |

| 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)? |
|---|---|---|---|---|---|---|---|
| | | | | | surveillance the individual can be notified by the A.D.A.E. | | |
| Greece, Presidential Decree 47/2005 'Procedure, technical and organizational guarantees for ensuring lawful interception'. (*'Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του')* (O. G.A' 64/10.03.2005) | Individuals whose confidentiality has been lifted by a judicial order. | Investigation for national security purposes and to verify serious crimes (Law 2225/1994). | For purposes of national security and to verify serious crimes (Law 2225/1994). | Yes, as provided for by arts. 3, 4, 5 of Law 2225/1994. | The law provides details on the procedure for waiving confidentiality. According to article 7, the judicial order must define the specific form and elements of communication and identify those elements as the identity of subscriber or user, the number calls and elements of leased lines, and codes of access to data networks or network. The order is sent by the competent authority | There is no specific time and geographical limit. | There is no such reference at the Law. |

| 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)? |
|---|---|---|---|---|---|---|---|
| | | | | | to the service provider and performed by corporation between the provider and competent authority. According to article 8, providers of services and communication networks are obliged to respond directly to every request for the waiving of confidentiality that is communicated to them by competent authorities. | | |
| Greece, Law 3649/2008, National Intelligence Service (EYP)and other provisions *('Εθνική Υπηρεσία Πληροφοριών και* | Individuals whose confidentiality of communications has been lifted by a judicial order. | The National Intelligence Service (EYP) seeks, collects and processes information and notify the competent | Lawful interception of communications is allowed for national security purposes (art.3 and 5 of Law 2225/1994). | Approval must have been obtained from the Public Prosecutor of the Court of Appeals (art. 5). | An order is issued by the Public Prosecutor who is assigned to the EYP by decision of the supreme judicial council. The EYP shall lift the confidentiality of | There is no specific reference to time limit or geographical scope as provided for by this law. However, the | There is no such specific reference at the Law. |

| 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)? |
|---|---|---|---|---|---|---|---|
| *άλλες διατάξεις'*) (O.G.39/ 3.03. 2008). | | authorities in order to fulfil its mission[21.] | | | letters and telephone or other communication and record the activities of persons using special technical media, especially audiovisual devices, outside residences. The said order shall be submitted for approval within twenty-four hours to the competent public Prosecutor of the | Law refers to Law 3115/2003 that amended Law 2225/1994 and provides time limits for the issuing of the judicial order. National Intelligence Service (EYP) personnel are subject to confidentiality Any violation of | |

[21] Its mission is a) to protect and promote the country's political, economic, military and overall national strategic interests.
b) to prevent and deal with activities constituting threats against the democratic regime, the fundamental human rights, the territorial integrity and the national security of the Greek State, as well as the country's national wealth, c) prevent and deal with activities of terrorist organizations and other organized crime groups. In times of war, mobilization or direct threat to national security, the National Intelligence Service shall come under the Chief of the National Defence General Staff who, via the NIS Director General, shall have full control on any matters relating to the National Intelligence Service contribution to the country's defence and security. In the event of any action aimed at violently abolishing the democratic regime, the NIS shall, by a resolution of the Government Council for Foreign Affairs and Defence (KYSEA), operate as central service for the management of the country's intelligence (article 2). Among its competences are to 1) to collect and provide information and data, make evaluations and submit recommendations to the Minister of Interior and other competent Ministers about the prevention or aversion of threats toward national security or the democratic regime, as well as the protection of the country's national interests. 2 To seek, collect, process and provide intelligence, in the context of the preceding para, mainly about matters relating to the activities of terrorist organizations or other organized crime groups in the fields of trafficking of human beings, human organs, weapons, drugs or other prohibited substances, mainly nuclear, radiobiological and chemical substances (NBRC) as well as about matters relating to money laundering (art.4).

| 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)? |
|---|---|---|---|---|---|---|---|
| | | | | | Court of Appeals. The order shall enter into force when approved by the Public Prosecutor of the Court of Appeals (art.5 b). According to art. 5 par.1c of Law 3649/2008, the National Intelligence Service (EYP) may collect information in accordance with the provisions of Law 3115/2003, as currently in force, for matters of national security by infiltration, following an order of the Director General of the National Intelligence Service (EYP) and with the approval of the supervising Public | the confidentiality duty shall constitute a disciplinary offence (art.14) | |

| 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)? |
|---|---|---|---|---|---|---|---|
| | | | | | Prosecutor. (art.5). | | |
| Law 4249/2014. Reorganising the Hellenic Police, Fire Department, General Secretary for Civil Protection, upgrade of services at the Minister for Public Order and Civil protection and regulation of issues for competence for Minister of Public Order and Civil protection and other provisions. *('Αναδιοργάνωση της Ελληνικής Αστυνομίας, του Πυροσβεστικού Σώματος και της Γενικής* | Individuals whose confidentiality of communications has been lifted by a judicial order that shall include only: a) the authority issuing the order, b) the applicant public authority and c) the date of issue of the order (art.22 para.6). | In exceptional cases in the course of preliminary examinations or interviews by the Directorate for Managing and Analysing Information of the Hellenic police or/and the Special Violent Crime Squad (art 22 para.6). | In exceptional cases in the context of the competences of Special Violent Crime Squad and Directorate for Managing and Analysing Information of the Hellenic police which is to collect, analyse, organise, disseminate and utilise processed or not information about every form of criminality and mostly terrorism and organized crime and to keep and inform special databases | Yes, according art. 3 of Law 2225/1994 and art. 22 of Law 4249/2014. | A Public Prosecutor who is the President of a Scientific Council of Analysis, Research and Programming to deal with the organised crime can submit the application of lift of confidentiality to Council of Appeals which has to decide on the waiving of confidentiality within 48 hours. Its order shall include only: a) the Authority issuing the order, b) the applicant public authority and c) the date of issuing the order In extremely exceptional cases the lift can be decided by | Law 2225/1994 applies and provides time limits for the issuing judicial order. | According art. 11, Hellenic Police has local competence the entire Greek state except the areas of the coastguard competence. |

| 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)? |
|---|---|---|---|---|---|---|---|
| *Γραμματείας Πολιτικής Προστασίας, αναβάθμιση Υπηρεσιών του Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη και ρύθμιση λοιπών θεμάτων αρμοδιότητας Υπουργείου Δημόσιας Τάξης και Προστασίας του Πολίτη και άλλες διατάξεις')* (O.G. A'73/24.3.2014) as amended. | | | where information is stored (art. 22). | | the Public Prosecutor himself. (art.22 para.6 refers to art. 6 of Law 2713/1999 and art. 3 of Law 2225/1994). | | |
| Greece Law 3917/2011 'Retention of data generated or processed in connection with | Subscribers and registered users of telecom and internet services. | According to article1 para. 1 and article 3 para.1, providers of publicly available | According to articles 1 and 4, the retained data can be provided to competent authorities in | Article 1 and 4 of the Law provides for the lifting of confidentiality for communication according to the | According to article 1 para. 1, traffic and location data as well as identification data are protected by the article 19 of the | According to article 6, data is retained for a period of 12 months from the date of | There is no such reference at the Law. |

| 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)? |
|---|---|---|---|---|---|---|---|
| the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the obtaining or recording of sound or image at public areas and relative provisions' (articles 1 to 13). *('Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την* | | electronic communications services or of a public communications network are obliged to retain data generated or processed by them. But according to art.4, they will provide this data to pubic authorities only under the procedure, requirements and conditions described in Law 2225/1994. | order to verify serious criminal offences. There is a closed number of crimes provided for in the penal law and special penal laws (such as crimes against the Constitution, political parties and the government, threats to public order) for which lawful interception is permitted according art.4 of Law 2225/94[22] | procedure stated at article 4 of Law 2225/1994. | Greek Constitution. Only this data can be retained and only for verifying serious criminal offences as stated under the provisions of Executive Law 2225/1994 governing the lifting of confidentiality (arts1 and 4). The retention of data that can reveal the content of communication is prohibited (art.3). Data must be destroyed after a storage period of 12 months by the providers using an automated | communication. Data must be stored in physical means within the borders of Greek state. Surveillance is conducted to providers that are established in Greece operating under a General Authorisation regime and registered in the Registry of Electronic Communication Network and Service Providers kept by Hellenic Communications and Post | |

[22] The crimes are enumerated in the Law 2225/1994 as mentioned above.

| 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)? |
|---|---|---|---|---|---|---|---|
| *παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις')* (O.G. A'22/21.02.2011). | | | | | procedure. When the lifting of confidentiality is ordered, the provider has to deliver this data within 5 days of notification (art.8). Where public authorities have gained legal access, the provider shall delete the data in his own system within a period of 10 days after the providers have been notified by the competent judge or council that the reason that their preservation has been ordered has ceased to exist. | Commission according to Law 4070/2012 (O.G. A'82/10.04.2012 ). | |
| Law 3471/2006 Protection of personal data and privacy in the | Subscribers and users of public networks of electronic | According to art. 4 para.1, the withdrawal of confidentiality | For purposes of national security and to verify serious crimes | Yes, according art. Executive Laws of Hellenic Constitution as | Article 4 of Law 3471/2006, provides the lifting of confidentiality for | Law 2225/1994 applies and provides time limits for the | There is no such reference in the law. |

| 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)? |
|---|---|---|---|---|---|---|---|
| electronic telecommunications sector and amendment of Law 2472/1997 *('Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του 2472/1997')* (O.G A'133/28.06.2006). | telecommunications. | shall only be allowed under the procedures and conditions provided for in Art. 19 of the Hellenic Constitution. State authorities can request access to Communications data as well as the pertinent traffic and location data available to providers of public networks of electronic telecommunications according the procedure stated at Executive Laws of art. 19 of Hellenic | (Law 2225/1994). | Law 2225/1994. | communication is allowed according to the conditions and procedure stated at Executive Laws of art. 9 of Hellenic Constitution as Law 2225/1994. | issuing judicial order. | |

| 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)? |
|---|---|---|---|---|---|---|---|
| | | Constitution as Law 2225/1994. | | | | | |

## 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:**<br><br>**only to nationals or also to EU citizens and/or third country nationals** | **Indicate whether rules on protection of privacy and data protection apply:**<br><br>**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* |
| Greece Law. 3115/2003, 'Hellenic Authority for Communication Security and Privacy' *('Ελληνική Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών')* (O.G. Α΄ 47/27.2.2003). The Law provides the legal framework relating to the constitution, the operation and the functions of the A.D.A.E. monitoring the protection of | According to article 6 para 1, the Hellenic Authority for Communication Security and Privacy investigates relevant complaints from members of the public when their rights of freedom of communication and communications secrecy are violated from the mode and the procedure of the withdrawal of confidentiality. In case of violation, the Hellenic Authority for Communication Security and Privacy can impose administrative sanctions and financial penalties on liable individuals or legal entities | The rules apply to nationals, EU citizens and third country nationals. The Hellenic Authority for Communication Security and Privacy was established pursuant to the constitutional revision of 2001 in the paragraph 2 of Article 19 of the Hellenic Constitution. So its founding law protects everyone's freedom of communication and communications secrecy. | The rules on data protection apply for personal data processed by providers established in Greece. |

| | | | |
|---|---|---|---|
| confidentiality of communications, procedure of lawful interception and access to communications data. | (art. 11 of Law 3115/2003). The Law does not provide definition of legal entities. According to art. 11 of Law 3674/2008 and art. 12 of Law 3917/2011 the A.D.A.E. can impose administrative sanctions on communications providers. The Hellenic Authority for Communication Security and Privacy's decisions are enforceable and can be appealed before the Council of State and the administrative courts (art.6 par.4 of Law 3115/2003, art. 11 of Law 3674/2008, art. 12 of Law 3917/2011 and Council of the State Decision 3319/2010). | | |
| Greece Law 3917/2011 'Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, use of surveillance systems with the obtaining or recording of sound or images in public areas and relative provisions', *('Διατήρηση δεδομένων* | The Law refers to Law 2225/1994 and provides the safeguard of a judicial council that decides upon the lift of confidentiality. Article 5 of Law 2225/1994 provides that subjects could be informed by A.D.A.E. after the surveillance in case that the purpose of surveillance is not threatened. | The rules apply to nationals, EU citizens and third country nationals. | The rules apply for processing retained data by providers established in Greece. |

| | | | |
|---|---|---|---|
| *που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις')* (O.G. A΄ 22/21.02.2011).<br>According to article 1 para. 1, traffic, location data and identification data are protected by article 19 of the Greek Constitution.<br>Only this data can be retained and only for verifying serious criminal offences as stated under the provisions of Executive Law 2225/1994 governing the lifting of confidentiality (arts.1 and 4). | | | |

| | | | |
|---|---|---|---|
| The retention of data that can reveal the content of communication is prohibited (art. 3).<br>In accordance to art. 7, H.D.P.A. and A.D.A.E. have issued a Common Act regarding the obligations of providers for protection and security of retained data. | | | |
| Law 3471/2006 Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997. *('Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του 2472/1997')*, (O.G. A΄ 133/28.06.2006).<br>The Law has implemented Directive 2002/58/EC. The provisions of the law | The Law defines the scope of confidentiality. According to art. 4 para.1, any use of electronic communication services offered through a publicly available electronic communications network, as well as the pertinent traffic and location data, shall be protected by the principle of confidentiality of telecommunications. The withdrawal of confidentiality shall only be allowed under the procedures and conditions provided for in Art. 19 of the Hellenic Constitution. | The rules apply to nationals, EU citizens and third country nationals. | The rules on data protection and privacy apply for personal data processed by providers established in Greece. |

| | | | |
|---|---|---|---|
| institute a set of obligations in the sector of personal data protection in the sector of electronic communications.[23.] According to art. 4 para.2, Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic and location data is prohibited, except when legally authorised. | | | |
| Law 2472/1997 'On the protection of individuals with regard to the processing of personal data (as amended)'. *('Για την προστασία των δεδομένων προσωπικού χαρακτήρα')*, (O.G. A΄ 50/ 1997)[24] (The Law has implemented Directive 95/46/EC. The | Art 5 para.1a of the Law 3649/2008 provides for the applicability of Law 2472/1997 to the activities of NIS when collecting and processing personal data. Art. 12 of Law 2472/1997, provides that the data subjects have the right to access and challenge the processing. There are limitations to those rights for purposes of national security and for the detection of serious crimes. By virtue of a | The rules apply to nationals, EU citizens and third country nationals. The law refers to everyone's rights. | According to art. 1 para 3, the law applies to any processing of personal data, provided that such processing is carried out: a) by a controller or a processor established in Greek territory or in a place where Greek law applies by virtue of public international law. b) by a controller who is not established in the territory of a member-state of the European Union or of a member of the European |

[23] Available in English at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF (Last accessed: 8 September 2014).
[24] An English version is available at : www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF (Last accessed: 8 September 2014)

| | | | |
|---|---|---|---|
| provisions of the Law institutes a set of principles of data processing, a set of obligations for those ones who process personal data and respective rights of the people to whom the data processed relate).<br>The Law provides data protection principles for data controllers and processors and the right to be informed (art.11), right to access to data (art. 12), right to challenge, rectify, delete and block (art. 13) and temporal judicial protection (art.14) to data subjects. | decision by the H.D.P.A., on application submitted by NIS, its obligation to inform was carried out on grounds of national security reasons or for the detection of serious crimes. In this case the President of the Data Protection Authority or his substitute carries out all necessary acts and has free access to the files.<br>Also according to art. 11 par. 4 of Law 2472/1997, by virtue of a decision by the H.D.P.A. the obligation to inform may be lifted in whole or in part provided that the data processing is carried out for reasons of national security or for the detection of particularly serious crimes. In a stage of emergency said obligation may be lifted by way of provisional, immediately enforceable judgement by the President of H.D.P.A. who shall convene as soon as possible the Board in order that a final judgement on the matter may be issued<br>Law enforcement agencies are also obliged to respect data protection principles and data subjects' rights provided by Law 2472/1997.<br>But according art. 3, the Law exempts from its scope state | | Economic Area (EEA) but in a third country and who, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the Greek territory, unless such equipment is used only for purposes of transit through such territory. |

| | | | |
|---|---|---|---|
| | authorities collection and processing of personal data when acting under supervision by a judicial authority in the framework of attributing justice. In addition excepts personal data processing by state authorities via camera installations in public areas for a closed number of purposes as the protection of state security ([25]) Art 14 of Law 3917/2011 fully re-integrates any video surveillance system into the general data protection law 2472/1997. Art, 3 still applies, since the amendments of art. 14 of Law 3917/2011 will | | |

[25] According to article 3 of L. 2272/1997 the following are excluded from the scope of this Law: A) data processing by judicial-public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operation needs with the aim of verifying crimes which are punished as felonies or misdemeanors with intent, and especially with the aim of verifying crimes against life, against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, against property, against the right to property, violations of legislation regarding drugs, plotting against public order, as well as crimes against minors. With regard to the above, the current essential and procedural penal provisions shall apply (art. 3 para.1 b). ,B) In cases where citizens exercise their right to assemble, in accordance with Article 11 of the Constitution, the simple operation of sound or image recording devices or other technical means is allowed with a view to recording, subject to the conditions mentioned below. The recording of sound or image using special technical devices with a view to verifying the perpetration of crimes mentioned above shall only be allowed following an order by a public prosecutor representative and provided a serious danger to the public order and security is imminent. The aim of such a recording shall solely be to use the data to verify the perpetration of crimes as evidence in front of any public investigative authority, prosecution authority or court of law. The processing of data which are not necessary for the verification of crimes shall be prohibited, while the recordings shall be destroyed following an order by the public prosecutor (art.3 para.1b), C) by a public authority using special technical devices for the recording of sound or image in public areas with the aim of safeguarding the security of the state, national defense, public security, the protection of persons and property, the management of traffic for which they are competent. The material collected through the above mentioned devices (as long as it does not fall under point b of the present article) is stored for a period of seven (7) days, after which it is destroyed by the order of the public prosecution authority. Any breach of the above provisions shall be punished by imprisonment for a period of at least one year, a stricter punishment is provided for in some other law (Art. 3 para.1c).

| | | | |
|---|---|---|---|
| | come into force with the enactment of a foreseen Presidential Decree [26] | | |
| Greek Penal Law Code[27] | Law 3784/2008 has introduced two articles to the Greek Penal Law Code:<br>Art 370A 'Breach of confidentiality of telephone conversation and verbal communication' provides criminal sanction in case of illegal interception. The sentence is at least 1 year.<br>Article 292A, 'Crimes against the security of telephone communications', provides criminal sanctions in case of data security breaches. Users illegally accessing a network or software system used for telecommunications purposes will be sentenced to at least two years and subject to a fine of from Euro 20,000 to Euro 50,000. | The rules apply to nationals, EU citizens and third country nationals. | This law applies inside the country. |

[26] According to art. 14 of Law 3917/2011 after the expressed opinion of H.D.P.A. a Presidential Decree will specify the competent state authorities, the procedure and circumstances of surveillance and criteria of compliance to the principle of proportionality. The foreseen Presidential Decree shall substitute art. 3 para. 2b last three passages and art.3 para.2c of Law 2472/1997 but has still not been enacted.

[27] The text of the Penal Code can be accessed in Greek at: www.ministryofjustice.gr/site/kodikes/%CE%95%CF%85%CF%81%CE%B5%CF%84%CE%AE%CF%81%CE%B9%CE%BF/%CE%A0%CE%9F%CE%99%CE%9D%CE%99%CE%9A%CE%9F%CE%A3%CE%9A%CE%A9%CE%94%CE%99%CE%9A%CE%91%CE%A3/tabid/432/language/el-GR/Default.aspx)(Last accessed: 8 September 2014).

# Annex 2 – Oversight bodies and mechanisms

| **Name of the body/mechanism** | **Type of the body/mechanism** | **Legal basis** | **Type of oversight** | **Staff** | **Powers** |
|---|---|---|---|---|---|
| *in English as well as in national language* | *e.g. parliamentary, executive/government, judicial, etc.* | *name of the relevant law, incl. specific provision* | *ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated* | *including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body* | *e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.* |
| Hellenic Authority for Communication Security and Privacy (A.D.A.E.). *(Αρχή Διασφάλισης Απορρήτου Επικοινωνιών)* | Independent Administrative Authority not subject to any Administrative control. It is subjected to parliamentary control by the Special Commitee of Institutions and Transparency (43 para. 1 of Standing Orders of Hellenic Parliament). | Art. 101 A. of Hellenic Constitution. Law 3051/2002[28] According to art. 6 para. 1 of Law 3115/2003, the Hellenic Authority for Communication Security and Privacy has the duty to put into | Oversees the lawful interception of communications activities by the EYP and law enforcement agencies and investigates complaints by the public. Monitoring may take place before/during and after any type of surveillance, whether lawful or unlawful. | According art. 101 A of Hellenic Constitution, Independent Administrative Authorities' members such as A.D.A.E. shall be appointed for a fixed tenure and shall enjoy personal and functional independence. Their selection is by a decision of the Conference of Parliamentary Chairmen. The Head of the Hellenic Authority for Communication Security | The Hellenic Authority for Communication Security and Privacy has the powers to: a) monitor the procedure for waiving confidentiality in compliance with the procedure and requirements of articles 3, 4, 5 of Law 2225/1994 but is not allowed to assess the judgment of competent judicial authorities, b)issue regulations regarding the assurance of the |

[28] Greece, Law 3051/2002 'Constitutionally established authorities, amending and supplementing the system in the public sector and related regulations', *('Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος στον δημόσιο τομέα και συναφείς ρυθμίσεις')* (O.G. A΄ 220/20.9.2002).

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | effect scheduled and emergency auditing procedures, ex officio or upon complaint, of installations, equipment, files data bases and documents of the Hellenic National Intelligence Service (NIS), other civil services, providers of electronic communications services and providers of postal services. Monitoring is executed by a member (or members) of the Hellenic Authority for Communication Security and Privacy. The | The Authority performs scheduled but also ad hoc audits on providers of electronic communications services, providers of postal services, the NIS and other public services. (art. 6 par.1 a L.3115/2003). | and Privacy is appointed by the Conference of Parliamentary Chairmen seeking unanimity or in any case by the increased majority of four fifths of its members. (Art. 2 para 2 of Law. 3115/2003, article 101A of Hellenic Constitution and art. 13 & 14 of the Greek Standing Orders of the Hellenic Parliament). Law 3051/2002 provides issues relating to the appointment and service status of the Scientific and other staff. The Head and the members need to have broad social acceptance and specific legal and technical expertise and they are appointed by the Minister of Justice, Transparency and Human rights. Hellenic Authority for Communication Security and Privacy's staff consists of its President, Vice President and his/her | confidentiality of communications, c) to perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service, d) to hold hearings of the aforementioned entities, d) to investigate relevant complaints from members of the public and e) to collect relevant information using special investigative powers as against NIS (article 6). In addition it publishes and submits to the Parliament an annual report giving detailed information about its functioning and acts, underlying cases of negligence, presenting key observations and suggesting appropriate legislative changes in the field of securing the confidentiality of communications subject to the provisions of the |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | presence of ADAE'S President is mandatory when the audit concerns files which are maintained for national security purposes. According to art. 10 of Law 3917/2011 Hellenic Authority for Communication Security and Privacy' shares supervision of implementation of data retention law with the Hellenic Data Protection Authority. | | substitute and 5 other members and their substitutes (art.2 par. 1 Law 3115/2003).<br>The total number of staff is thirty eight positions. Eighteen of those positions are permanent civil servants, one is a private law contract, seventeen are Special Scientific staff, and there are two positions for lawyers and one legal counsel. Their competences are defined by art. 8 of Law 3115/2003. According to A.D.A.E' Annual Report 2013, the budget is reduced every year. The President and some members of A.D.AE. have resigned and must be replaced. | founding law (art.1.para. 2 Law 3115/03).Law 3471/2006, which transposes Directive 2002/58/EC into the national legal order, designates ADAE as the competent authority for the implementation of article 5 of the Directive ("confidentiality of the communications"), as well as for the implementation of the articles of the Directive which refer to the presentation of calling line identification for the tracing of malicious or nuisance calls and for emergency calls. The same Law (art.12) designates ADAE, together with the national DPA, as the competent national authority to receive data breach notifications.<br>Article 8 of Law 3674/2008 also includes provisions for the immediate notification of communication secrecy breaches or risk of such breaches to ADAE. Law 4070/2012 (art.37), which transposes Directive 2009/140/EC (art.13A) into the national legal order, provides that ADAE issues |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | | | regulations regarding the appropriate technical and organisational measures to be taken by undertakings providing public communications networks or publicly available electronic communications services in order to appropriately manage the risks posed to security of networks and services and to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.<br>A.D.A.E. can impose administrative sanctions and financial penalties to liable individuals or legal entities (art.1 of Law 3115/2003). The definition of legal entities is not provided by this law. ADAE may also impose administrative sanctions and financial penalties to providers in accordance with art.13 of Law 3471/2006, art. 11 of Law 3674/2008 and art.12 of Law 3917/2011.<br>According to 10 art. 3917/2011, A.D.A.E. has |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | | | the obligation to send statistics regarding retained data of the previous year to the European Committee via the Ministry of Justice. |
| Hellenic Data Protection Authority (DPA). *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)* | Independent Administrative Authority is not subjected to any Administrative control. It pertains and answers to the Minister of Justice for budgetary purposes (article 15 of 2472/1997). It is subjected to parliamentary control by the Committee of Institutions and Transparency (43 para. 1 of the Standing Orders of the Hellenic Parliament). | Art. 101 A. of the Hellenic Constitution. Law 3051/2002. According art 5. para. 1a of Law 3649/2008, NIS has to comply with Law 2472/1997. According to art. 22 of Law 4249/2014, the Directorate for Managing and Analysing Information of the Hellenic police has to comply with Law 2472/1997. According art. 3 of Law 2472/1997, state authorities when they collect and | During and post the surveillance According to art. 19 para 1 h of Law 2472/1997, H.D.P.A. shall proceed ex officio or following a complaint to administrative reviews in the framework of which the technological infrastructure and other means, automated or not, supporting the processing of data are reviewed. It shall have the right of access to personal data and the right to collect any kind of information for the purposes of such review, notwithstanding any | According to art. 3 para 2 of Law 3051/2002, the Head of the Hellenic Data Protection Authority is appointed by the Conference of Parliamentary Chairmen. Besides the President of the Hellenic Data Protection Agency and his/her substitute there are also 6 more members and their substitutes (art.16 of Law 2472/1997). According to H.D.P.A. Annual Report 2013, the total staff consisted of 77 organic positions. In Auditors department consisted of informatics auditors and legal auditors, there were 21 unfilled organic auditor positions and 25 filled. In the Department of Communication, there were 2 unfilled organic positions | The D.P.A. powers are to a) be responsible for file audits, b) to issue regulatory acts arising from legislation on data protection, c) to provide information and recommendations to data controllers d) to examine complaints, e) to report violations and f) to issue decisions related to the right of access. In general is responsible to ensure compliance with the data protection regulations. D.P.A. may impose administrative sanctions on controllers or their representatives. The DPA grants permits for the collection and processing of sensitive personal data and grants permits for the interconnection of files, |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | process personal data under supervision by a judicial authority and conduct video surveillance for a closed number of purposes as the protection of state security they are not obliged to comply to Law 2472/1997.[29] Art 3 still applies, since the amendments of art. 14 of Law 3917/2011 that fully reintegrated video surveillance to data protection law will come into force with the enactment of | kind of confidentiality. Exceptionally the H.D.P.A. shall not have access to identity data relating to associates and contained in files kept for reasons of national security or for the detection of particularly serious crimes. Such review is carried out by one or more members of the H.D.P.A. or an employer of the Secretariat, duly authorised to that effect by the President of the H.D.P.A. In the course of reviewing files kept for reasons of national security, the President of H.D.P.A. shall be present in person. | and 5 filled. In the Department of Administrative and Financial Affairs, there were 8 unfilled organic positions and 16 filled. | including sensitive data, and the trans-border flow of personal data. |

[29] See in detail above Annex 2 Law 2472/1997. Column 2

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | a foreseen Presidential Decree. According to art. 9 of Law 3917/2011 the H.D.P.A. shares supervision of implementation of data retention law with the A.D.A.E. According to article 7 para. 2 the Hellenic Data Protection Authority and the Hellenic Authority for Communication Security and Privacy issue a Joint Act regarding the obligations of providers for protection and security of retained data. According to art.9, the | | | |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | Hellenic Data Protection Authority has responsibilities regarding the protection of personal data according to a set of data protection principles and rights (Law 2472/1997) while the A.D.A.E. has to ensure the application of the legal framework for the protection of confidentiality of communications and for the lawful interception (Law 3115/2003). The A.D.A.E. also imposes fines in case of violation | | | |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | of arts 3, 4, 5, 6, 7, 8 of Law 3917/2011 (art.12 of Law 3917/2011). | | | |
| Special Standing Committee for Institutions and Transparency | Parliamentary Committee | Article 43A of Standing Orders of Hellenic Parliament | Parliamentary control of Independent Administrative Authorities. Oversees the parliamentary control policies, administration, management and legitimacy of the activities of the EYP. | Appointed by the President of the Parliament. (Art.31 of Standing Orders of Hellenic Parliament). Proportional representation Two Vice-Chair persons and one Secretary of the Committee are elected from the first, second and third, respectively, parliamentary parties of the opposition. The total number of members of the Committee is 13 (art. 43A. para.4. of the Standing Orders of the Hellenic Parliament). | The Committee on Institutions and Transparency exercises parliamentary control over the activity and the overall planning of the National Intelligence Service. The Government, either at its own initiative or following a request by the Committee, ought to inform the Committee on the National Intelligence Service's activity, except for reasons of overriding public interest or personal data protection, presented to the Committee by the competent Minister of Public Order and Citizen's Protection. The Director General of the National |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | | | Intelligence Service may be invited to a hearing by the Committee, in the presence of the competent Minister. Regarding the issue of confidentiality, "Discussions on National Intelligence Service's activity are confidential, and the Committee members have a confidentiality duty extending even after the expiration of their tenure. The Committee may publicize the findings of its control, always taking into account the aforementioned confidentiality duty" (Standing Orders of the Parliament-Article 43 A paragraph 2a) The Committee has the power to collect information and documents, as well as to summon and examine persons, by application of Articles 146 and 147 (Standing Order of Parliament, Article 43A paragraph 2a, subparagraph |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | | | 10). |
| Public Prosecutor. Public Prosecutor of Court of Appeals and/or Judicial Council. | Judicial Authority | Article 5 of L.3649/2008. Articles 3, 4, 5 of Law 2225/1995. Article 22 of Law 4249/2014. Greek Procedural Penal Code. | The National Intelligence Service (EYP) is supervised by a public prosecutor, specially appointed to the service, who controls the legality of its special operational activities as set out in art. 5 of Law 3649/2008. The order is issued by the supervising public prosecutor. It shall be submitted for approval within twenty-four hours to the competent public prosecutor for the Court of Appeals. The order shall enter into force when approved by the public prosecutor for | 1) The National Intelligence Service (EYP) is supervised by a public prosecutor, specially appointed to the service by decision of the Supreme Judicial Council. A public prosecutor for the Court of Appeals (Law 3649/2008).<br><br>2) According Law 2225/1994: a) judicial order for national security purposes must have been issued by the Prosecutor of Court of Appeals (art.3 and 5).<br>b) In case of serious crimes competent to issue the order is a judicial council. In case of emergency the prosecutor or the investigating judge issues an order which has to be confirmed by the judicial council within three days | Issues orders to lift the confidentiality. |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | the Court of Appeals. Also, the EYP may collect information on matters of national security by infiltration, following an order issued by the Director General of the National Intelligence Service (EYP) and with the approval of the supervising public prosecutor. Also in this case the National Intelligence Service has to comply with the provisions of Law 3115/2003 that amended Law 2225/1994According to recently amended art. 22 para. 6 of Law 4249/2014 in exceptional cases during preliminary investigation and interviews conducted by Directorate of Managing and Analysing | (art.4). Public Prosecutor of Court of Appeals and Judicial Council.<br><br>3) Public prosecutor who is the president of a Scientific Council of Analysis, Research and Programming (Article 22 of Law 4249/2014) | |

| Name of the body/mechanism | Type of the body/mechanism | Legal basis | Type of oversight | Staff | Powers |
|---|---|---|---|---|---|
| | | | Information of Hellenic police or/and Special Violent Crime Squad, a public prosecutor who is the president of a Scientific Council of Analysis, Research and Programming to deal with the organised crime can submit the application of lift of confidentiality to the Council of Appeals | | |

# Annex 3 – Remedies[30]

| [Law 3115/2003] | | | | |
|---|---|---|---|---|
| **Stages of surveillance process** | **Is the subject informed?** | **Does the subject have a right of access to the data collected on him/her?** | **List remedies available to an individual concerned** | **Legal basis for using the available remedies** |
| | Yes/No | Yes/No, please provide details if needed | Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc. AND please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies. | Violation of data protection, private life, specific legislation, etc. |
| Collection* | No | There is no such provision to this law. See Law 2472/1997 | If the individual becomes aware of the surveillance and considers that the waive of interception has not been properly followed, he/she can lodge a request with the A.D.A.E. (Oversight body) in order to investigate. According art. 6 of Law 3115/2003, the Hellenic | Violation of freedom of communication and communications secrecy art. 19 of the Hellenic Constitution. |

[30] 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

| | | | | |
|---|---|---|---|---|
| | | | Authority for Communication Security and Privacy" investigates relevant complaints from members of the public when their rights of freedom of communication and communications secrecy are violated from the mode and the procedure of the withdrawal of confidentiality.<br>The National Intelligence Service is controlled by the A.D.AE. (art.6 par.1a of Law 3115/2003).<br><br>The A.D.AE. can conduct regular and ad hoc controls on facilities, technical equipment, archives, databases and NIS documents (art.6 par.1 of Law 3115/2003).<br>If National Intelligence service personnel has violated the confidentiality of communications or the conditions and the procedure of lawful interception, penal sanctions include punishment by imprisonment for up to 2 years and a fine of at least 30.000 euros (art.10 of Law 3115/2003). EYP's personnel are subject to duty of confidentiality. The violation of the confidentiality duty shall constitute a disciplinary offence (article 14 of law 3649/2008).<br>In case of violation, the Hellenic | |

| | | | | |
|---|---|---|---|---|
| | | | Authority for Communication Security and Privacy can impose administrative sanctions and financial penalties on liable individuals or legal entities (art.11 of Law 3115/2003). The Law does not provide definition of legal entities.<br>According to art. 11 of Law 3674/2008 and art. 12 of Law 3917/2011 the A.D.A.E. can impose administrative sanctions on communications providers. In case of illegal interception, the individual can appeal to civil courts according to art. 105 of the Civil Code, art. 23 of Law 2472/1997, art. 14 of Law 3471/2006 and 13 of Law 3917/2011. There are penal sanctions by courts according to: art. 10 of Law 3115/2003, art. 22 of Law 2472/1997, art. 11 of Law 3917/2011, art. 15 of Law 3471/2006, and arts. 292 A and 370 A of the Penal Code. | |

| | | | | |
|---|---|---|---|---|
| **Analysis*** | No | | | |
| **Storing*** | | | | |
| **Destruction *** | | | | |
| **After the whole surveillance process has ended** | According to art 5 para.9 of Law 2225/1994. The A.D.A.E. can notify the targets of investigations under the necessary condition that the initial purpose of investigation is not threatened. | There is no such provision to this law. See Law 2472/1997 | | |
| **[Law 2472/1997]** | | | | |
| **Stages of surveillance process** | **Is the subject informed?** | **Does the subject have a right of access to the data collected on him/her?** | **List remedies available to an individual concerned** | **Legal basis for using the available remedies** |

| | | | | |
|---|---|---|---|---|
| | Yes/No | Yes/No, please provide details if needed | Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc. **AND** please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies. | Violation of data protection, private life, specific legislation, etc. |
| **Collection*** | No. According to art. 11 par. 4 of Law 2472/1997, by virtue of a decision by the Authority the obligation to inform may be lifted in whole or in part provided that the data processing is carried out for reasons of national security or for | Yes, if they are related to him/her according to art.12 of Law 2472/1997 and Law 3471/2006 by requesting them from the surveillance authority. Individuals cannot access files already deleted according to the procedure described in art. 5 par. 9 of Law 2225/1994. In addition in case the files are not deleted by virtue of a decision by the H.D.P.A., on application submitted | Data subject can petition to civil courts according to article 23 of Law 2472/1997. H.D.P.A. can impose administrative sanctions according to art.21 of Law 2472/1997. Penal sanctions can be imposed by penal courts according to art. 22 of Law 2472/1997. | Violation of information privacy art. 9A of Hellenic Constitution Arts 21,22,23 of Law 2472/1997. |

* 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

| | | | | |
|---|---|---|---|---|
| | the detection of particularly serious crimes. In a stage of emergency said obligation may be lifted by way of provisional, immediately enforceable judgement by the President of H.D.P.A. who shall convene as soon as possible the Board in order that a final judgement on the matter may be issued. | by the NIS, its obligation to inform may be lifted, provided that proves that the processing of personal data in whole or in part was carried out on grounds of national security reasons or for the detection of serious crimes. In this case the President of the Data Protection Authority or his substitute carries out all necessary acts and has free access to the files (art.12 par. 5 of L. 2472/1997). | | |
| **Analysis*** | No | | | |
| **Storing*** | No | The individual can ask his data to be deleted. | | |
| **Destruction *** | No | | | |
| **After the whole surveillance process has ended** | No | | | |

# 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** | Council of State decisions No. 3319 and No. 3320/2010. |
| **Decision date** | 13.2.2009. and 11.3.2009 |
| **Reference details (type and title of court/body; in original language and English [official translation, if available])** | The Hellenic Council of State (Συμβούλιο της Επικρατείας) is the Supreme Administrative Court of Greece. |
| **Key facts of the case (max. 500 chars)** | After the illegal interception using Ericsson software of a number of Vodafone mobile telephones (over 100) belonging to members of the government, the security services and others, the Hellenic Authority Communication Security and Privacy fined Vodafone 76 million Euro for failing to protect the network from the unknown hackers and fined Ericsson Hellas 7.36 million Euro. The Hellenic Council of the state decided to accept both companies of telecommunication sector's petitions for judicial review (annulment) of those fines imposed by Hellenic Authority Communication Security and Privacy. |
| **Main reasoning/argumentation (max. 500 chars)** | The Hellenic Council of State decided to annul the acts of the Independent authority on the grounds that the relevant administrative procedure was not open to the public and that this constitutes a breach art 6 of Convention of human rights and fundamental freedoms.According to The Hellenic Authority Communication Security and Privacy Regulation, a public hearing is not prescribed by Law, as its founding Law 3115/2003 calls for the implementation of the relevant provisions of the Code of Administrative Procedure, which establishes the rule of closed (not public) board meetings. The Hellenic Authority Communication Security and Privacy should review this case according to the reasoning of this court decision. |

| | |
|---|---|
| **Key issues (concepts, interpretations) clarified by the case (max. 500 chars)** | The court interpreted article 6 of European Convention on Human Rights (fair trial) and case law, considering that the fundamental procedural guarantees for issuing a decision by administration are: the equity of its members, its constant character and publicity of its meetings.<br>Article 6 of the founding Law of the Hellenic Authority for Communication Security and Privacy (3115/2003) calls for the implementation of the relevant provisions of the Code of Administrative Procedure, which establishes the rule of closed (not public) board meetings and does not include exceptions when the Hellenic Authority Communication Security and Privacy decides to impose a fine.<br>So, according to the Court, as the Hellenic Authority for Communication Security and Privacy decided in a closed board meeting its decision is invalid and cannot be implemented. |
| **Results (sanctions) and key consequences or implications of the case (max. 500 chars)** | As key consequence of this case, article 61 par. 5 of L.4055/2012 was introduced so as to amend Law 3051/2002 so as to provide the possibility that Independent Administrative Authorities (such as the Hellenic Authority for Communication Security and Privacy) can have public hearings especially when deciding on fines.<br>It must be noted that with its subsequent decision 1361/2013, the reasoning of decision 3319/2010 was revisited by the Hellenic Council of State, and it held that, following the decision of the European Court of Human Rights of 21.07.2011 on the case of SIGMA RADIO TELEVISION LTD v. CYPRUS (Applications nos. 32181/04 and 35122/05), the hearings of Independent Administrative Authorities may be lawfully held in closed (not public) board meetings.<br>The Hellenic Authority for Communication Security and Privacy issued a new (1/2013) Decision and fined Vodafone 50,6 million Euros. The company has again petitioned the annulment of the fine imposed by The Hellenic Authority for Communication Security and Privacy.<br>The Council of State sat on 9 May of 2014. The publication of its decision regarding this case is still expected.<br>After the increased public concern caused by the scandal of unlawful interceptions, Law 3674/2008 was introduced to reinforce the privacy of |

| | |
|---|---|
| | telephone communications.<br>In addition according to investigative journalism, there are allegations of spying related to these illegal interceptions and there is an ongoing secret penal investigation[31]. |

[31] Greece, TVXS, 'The employee responsible for the interceptions of American Embassy was found' *('Βρέθηκε ο υπάλληλος επικεφαλής υποκλοπών της αμερικανικής πρεσβείας')*, 10 March 2014, available at: http://tvxs.gr/news/ellada/brethike-o-ypallilos-epikefalis-ypoklopon-tis-amerikanikis-presbeias.

| | |
|---|---|
| **Case title** | Administrative Court of Appeals of Athens decision No 1237/2011 |
| **Decision date** | 2. 03. 2011 |
| **Reference details (type and title of court/body; in original language and English [official translation, if available])** | Administative Court of Appeals of Athens (Διοικητικό Εφετείο Αθηνών). |
| **Key facts of the case (max. 500 chars)** | After the Hellenic Authority Communication Security and Privacy decision to impose a fine on Vodafone for the illegal interceptions, the Hellenic Communications and Post Commission also decided to impose a fine of 19.1 million Euros. The company petitioned the judicial review (annulment) of the fine. The Administrative Court of Appeals rejected the company's petition. |
| **Main reasoning/argumentation (max. 500 chars)** | According to the Administative Court of Appeals of Athens, decisions of Hellenic Communications and Post Commission are reviewed by the Administrative Court which has the power to amend and reduce the fine. Therefore the Court provides the guarantees for art 6 of Convention of human rights and fundamental freedoms (fair trial). |
| **Key issues (concepts, interpretations) clarified by the case (max. 500 chars)** | Even in the case that there is an obligation for a public hearing so the Hellenic Communications and Post Commission can issue a fine, the right to fair trial is not violated because the administrative court has the competence to decide upon the substance of the dispute. |
| **Results (sanctions) and key consequences or implications of the case (max. 500 chars)** | A sanction of 19.1 million Euros was imposed on Vodafone by the Hellenic Communications and Post Commission.<br>The Administrative Court of Appeals of Athens rejected the company's petition and decided the forfeiture of the imposed fine.<br>The company appealed against the judgment of Administrative Court of Appeals of Athens at the Supreme Civil and Criminal Court of Greece (Άρειος Πάγος). The Court has not yet sat on this case. |

# 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 |
|---|---|---|---|
| **National Information Service (EYP) (*Εθνική Υπηρεσία Πληροφοριών ΕΥΠ*)** | Public authority | Address: 4, Panagioti Kanellopoulou Str.<br>GR-101 77, Athens.<br>Phone: 30 210 6926210<br>E-mail: nis@nis.gr | www.nis.gr/portal/page/portal/NIS/ |
| **Special Violent Crimes Squad *(Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας Δ.Α.Ε.Ε.Β)*** | Public authority | email ctu@hellenicpolice.gr | www.astynomia.gr/index.php?option=ozo_content&perform=view&id=47&Itemid=38&lang=EN |
| **Ministry of Public Order and Citizen Protection (*Υπουργείο Δημόσιας Τάξης και Προστασίας του Πολίτη*)** | | Address: 4, Panagioti Kanellopoulou Str.<br>GR-101 77, Athens.<br>Phone: +30-210 6977505, 210 6929764.<br>Email pressoffice@yptp.gr | www.mopocp.gov.gr/main.php?lang=EN |

| | | | |
|---|---|---|---|
| **Committee on Institutions and Transparency (*Ειδική Μόνιμη Επιτροπή Θεσμών και Διαφάνειας*)** | Parliament | Address: Parliament Mansion (Megaro Voulis), GR-10021, Athens.<br>Parliament call center: (+3-0210-3707000), Fax: (+3-0210-3707814), | www.hellenicparliament.gr/Koinovouleftikes-Epitropes/CommiteeDetailView?CommitteeId=2b188390-2f24-4d95-b867-912d485fa8cf |
| **The Council of State (*Συμβούλιο Επικρατείας*)** | Court | Panepistimiou 47-49, GR 10564 Athens.<br>E.mail. ste@ste.gr | www.ste.gr/FL/main_en.htm |
| **Supreme Civil and Criminal Court (*Άρειος Πάγος*)** | Court | Av. Alexandras 121 11522 Athens | www.areiospagos.gr/ |
| **Hellenic Authority for Communication Security and Privacy *(Αρχή Διασφάλισης Απορρήτου Επικοινωνιών)*** | Independent Administrative Authority | Address: Ierou Lohou 3, Marousi GR151 24, Athens, Greece.<br>Phone: +30-210 6387600<br>+30-210 6387601 | www.adae.gr/en/ |
| **Hellenic Data Protection Authority (HDPA) *(Αρχή Προστασίας Προσωπικών Δεδομένων)*** | Independent Administrative Authority | Address: Kifissias 1-3,<br>GR 115 23 Athens, Greece.<br>Phone: +30 210 6475600<br>+30 210 6475696<br>+30 210 6475628 (fax).<br>E-mail: contact@dpa.gr | www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL |
| **Hellenic Telecommunication and Post Commission. (*Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων*)** | Independent Administrative Authority | Address:Kifissias Avenue 60,<br>GR 151 25 Marousi, Athens<br>Phone:(+30) 210 6151 000<br>Fax (30) 210 6105049<br>Email: info@eett.gr | www.eett.gr/opencms/opencms/EETT_EN/index.html |

| | | | |
|---|---|---|---|
| **National Commission for Human Rights** ***(Εθνική Επιτροπή για τα Δικαιώματα του Ανθρώπου)*** | Independent Administrative Authority | Neophutou Bamba 6 (3d floor), GR 106 74 Athens<br>Phone: +30 210-7233221, 210-7233216, fax:210-7233217.<br>E-mail: info@nchr.gr, | www.nchr.gr |
| **Hellenic League for Human Rights** ***(Έλληνική Ένωση για τα Δικαιώματα του Ανθρώπου)*** | Human Rights Organisation | Poste Restante. 3119, GR10210, Athens.<br>There is an online form for electronic communication | www.hlhr.gr/ |
| **University of the Aegean Department of Information Systems** (***Πανεπιστήμιο Αιγαίου Τμήμα Πληροφοριακών Συστημάτων)*** | University | Dept. of Information and Communication Systems Engineering Karlovasi, GR 83200 Samos<br><br>Tel.: +30-22730 82200<br><br>Fax: +30-22730 82209<br><br>email: dicsd@icsd.aegean.gr | www.aegean.gr |
| **Democritus University of Thrace** ***(Δημοκρίτειο Πανεπιστήμιο Θράκης)*** | University | Democritus University of Thrace, University Campus,<br>GR 69100 Komotini<br>Phone: +30 25310 39000<br>Email webmaster@duth.gr | http://duth.gr/index.en.shtml |
| **Department of Information Science** | University | Department of Informatics, Ionian University | http://di.ionio.gr/ |

| | | | |
|---|---|---|---|
| **University of Ionion** ***(Ιόνιο Πανεπιστήμιο Τμήμα Πληροφορικής)*** | | 7 Tsirigoti Square<br>GR 49100 Corfu<br><br>Phone : +30 26610 87760 / 87761<br>Fax : +30 2661 0 87766<br>E-mail: cs@ionio.gr | |
| **Panteion University Department of Social Sciences** ***(Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών)*** | University | Av. Syggrou 136,<br>GR 176 71 Athens | www.panteion.gr/ |
| **Hellenic Foundation for European and Foreign Policy** (***Ελληνικό Ίδρυμα Ευρωπαϊκής και Εξωτερικής Πολιτικής)*** | Think Tank | Phone: (+30) 2107257110<br>Vassilisis Sofias 49,<br>Athens, GR 10676.<br>Email: eliamep@eliamep.gr | www.eliamep.gr/ |

# 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.


Greece, Minister of Public Order and Citizen's Protection, (*Υπουργείο Δημόσιας Ασφάλειας και Προστασίας του Πολίτη*), Press release. 'Response of "Press Office of Minister of protection of Public Order and Citizens' protection. N. Dendias to Announcement of Syriza's Press Office regarding interceptions' *(Απάντηση του Γραφείου Τύπου του Υπουργού Δημόσιας Τάξης και Προστασίας του Πολίτη κ. Νίκου Δένδια στην ανακοίνωση του Γραφείου Τύπου του ΣΥΡΙΖΑ σχετικά με τις «υποκλοπές»)*, 9.10.2013. Available in Greek at: www.minocp.gov.gr/index.php?option=ozo_content&perform=view&id=4789&Itemid=581&lang=GR. All references were accessed on 8 September 2014.

Minutes of Scientific Meeting organised by the Panhellenic Federation of Workers of EYP POSEYP in 11.06.2008 (2009). *'State, Security and the Role of Intelligence Services. The case of Greece. Function and Powers of the NIS (Κράτος, Ασφάλεια και ο ρόλος των υπηρεσιών πληροφοριών. Η περίπτωση της Ελλάδας-Αρμοδιότητες και λειτουργία της ΕΥΠ. Πρακτικά Επιστημονικής Ημερίδας)* [in Greek], ed. Sakkoulas.

Greece, Hellenic Parliament Special Committee on Institutions and Transparency (*Βουλή των Ελλήνων, Ειδική Επιτροπή Θεσμών και Διαφάνειας)*. Discussion on the Annual Report of the Hellenic Authority for Communication Security and Privacy (2013) and hearing of its Vice President K. Maravela 8.07.2014. *(Συζήτηση επί της Εκθέσεως Πεπραγμένων της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών [Α.Δ.Α.Ε]), έτους 2013, και ακρόαση του Αντιπροέδρου της Αρχής, κ. Κωνσταντίνου Μαραβέλα).*The video can be accessed at: www.hellenicparliament.gr/Koinovouleftikes-Epitropes/Synedriaseis?met_id=57236dc4-1f65-4afd-83cf-1b425741492c (video).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 9/2009', Penal Chronicles, 2010, p.498 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 12/2009' Mass Media & Communication Law Review, 2 /2009 p.393 (in Greek)

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Opinion 9/2011' Penal Chronicles, 2011 p. 714 (in Greek)

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) 'Circular 1/2013' *('Εγκύκλιος 1/2013')*, Penal Chronicles, 2013 p.307-309 (in Greek).

Greece, Public Prosecutor's Office for the Supreme Civil and Criminal Court (*Άρειος Πάγος*) Opinion 7/2014, (*Γνωμοδότηση 7/2014*). Available at: http://eisap.gr/sites/default/files/consulations/ΓΝΩΜΟΔΟΤΗΣΗ%2070001.pdf .(in Greek) (last accessed 23/10/2014).

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

Greece, Hellenic Data Protection Authority *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)* (2012), Annual Report 2011, (*Ετήσια έκθεση 2011*). Available in Greek at: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2011/ARXH_PROSTASIAS_2011.PDF (Last accessed: 8 September 2014).

Greece, Hellenic Data Protection Authority *(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)* (2013), Annual Report 2012, (*Ετήσια έκθεση 2012*). Available in Greek at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2012/ARXH%20PROSTASIAS%20APOLOGISMOS%202012_%20WEBUSE.PDF (Last accessed: 8 September 2014).

Greece, Hellenic Data Protection Authority (*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*) (2014), Annual Report 2013, *(Ετήσια έκθεση 2013*). Available in Greek at: www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/AR2013/ARXH%20PROSTASIAS_APOLOGISMOS%202013%20WEBUSE.PDF (Last accessed: 8 September 2014).

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2012), Annual Report 2011 (*Ετήσια Έκθεση 2011).* Available in Greek at: Last accessed: 8 September 2014).

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2013), Annual Report 2012 (*Ετήσια Έκθεση 2011)*. Available in Greek at: Last accessed: 8 September 2014).

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2014), Annual Report 2013 (*Ετήσια Έκθεση 2012)*. Available in Greek at: 8 September 2014).

Greece, Hellenic Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2013), Press Release 'Announcement regarding the interceptions' *('Ανακοίνωση σχετικά με την υπόθεση των υποκλοπών')*, 7 January 2013, available in Greek at: www.adae.gr/fileadmin/documents/DELTIO_TYPOU_ADAE.pdf (Last accessed: 8 September 2014).

3. Non-governmental organisations (NGOs).

Greece, Hellenic League for Human Rights *(Ελληνική Ένωση για τα δικαιώματα του Ανθρώπου*) Press Release 'Interceptions of rights', *('Υποκλοπές δικαιωμάτων')* 22 March 2006. available in Greek at: www.hlhr.gr/index.php?MDL=pages&SiteID=485 (Last accessed: 8 September 2014).

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

Apostolidis P., (2007) 'Intelligence services in the National Security System. The case of EYP', ('*Υπηρεσίες πληροφοριών στο Εθνικό Σύστημα Ασφάλειας. Η περίπτωση της ΕΥΠ*') Occasional Paper, Hellenic Foundation for European and Foreign Policy, 2007. Available in English at: www.eliamep.gr/wp-content/uploads/en/2008/10/op07_03_eng.pdf. (Last accessed: 8 September 2014).

Kaiafa-Gbanti M. (2010), *Surveillance Models in the Security State & Fair Criminal Trial* [in Greek], (*Μοντέλα Επιτήρησης στο κράτος ασφάλειας και δίκαιη ποινική δίκη)* Nomiki Vivliothiki Publications.

*Katrougalos G. (2013), Monitoring and Constitution, (Παρακολουθήσεις και Σύνταγμα),* Unfollow, Issue 23 November 2013, pp. 55-57.

Mitrou L. (2008), 'Data retention: a Pandora's Box for Rights and Liberties?' in A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis, C. Lambrinoudakis (eds), *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications, pp. 410-433.

Mitrou L. (2010), 'The Impact of Communications Data Retention on Fundamental Rights and Democracy – The Case of the EU Data Retention Directive', in: Haggerty D. & Samatas M. (eds.), *Surveillance and Democracy*, Routledge.

Nouskalis G. (2012), The processing of external telecommunications position and traffic data traffic as inquisition act of investigation under L.3911/2011. *Η επεξεργασία των εξωτερικών τηλεπικοινωνιακών δεδομένων θέσης και κίνησης ως ανακριτική πράξη έρευνας κατά τον Ν. 3917/2011*, Penal Chronicles pp. 246-249, (In Greek).

Tsiftsoglou A. /Spyridon Flogaitis, (2012), Transposing the Data Retention Directive in Greece: Lessons from Karlsruhe, Values and Freedoms in Information Law & Ethics. Available in English at: http://works.bepress.com/anna_tsiftsoglou/2/ (Last accessed: 8 September 2014).

Tsolias G. (2008), 'Personal data in electronic communications domain and reverse investigation for reasons of certification of particularly serious crimes', *('Δεδομένα προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών και «αντίστροφη αναζήτηση» αυτών για λόγους διακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων. Εξ αφορμής της υπ. Αρ. 19/2008 απόφασης ΑΠΔΠΧ')*, Mass Media & Communication Law Review, 2 [in Greek], pp. 175-183.

Tsolias G. (2010), 'Protection of confidentiality and personal data in telecommunications sector' *('Προστασία του απορρήτου και των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών')* in C. Lambrinoudakis, L. Mitrou, S. Gritzalis, S. K. Katsikas, (eds), *Privacy and Information and Communication Technologies: Technical and Legal Issues, (Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών)*, Papasotiriou Publications, (in Greek), pp. 679-701.

Tsolias G. (2013), Privacy, Data Retention and Data Protection in The Electronic Communications Sector - Providers Of Publicly Available Electronic Communications Services - Competent Supervisory Independent Administrative Authorities. Available in Greek at: Greek Lawyers' digest www.greeklawdigest.gr/topics/technology-media-electronic/item/84-privacy-data-retention-and-data-protection-in-the-electronic-communications-sector-providers-of-publicly-available-electronic-communications-services-competent-supervisory-independent-administrative-authorities.(Last accessed: 8 September 2014).

Fountedaki P., Tsolka O., Chanos A. (eds), (2010), *Freedoms, Rights & Security in EU, (Ελευθερίες, Δικαιώματα και Ασφάλεια στην Ε..Ε.)* [in Greek], Nomiki Vivliothiki.

*Investigative journalism*

Greece, Enet, (2013), 'Crime…the interviews' *('Έγκλημα....οι συνεντεύξεις')*, 23 October 2013, available in Greek at: www.enet.gr/?i=news.el.ellada&id=393947 (Last accessed: 8 September 2014).

Alevizopoulou M. and A. Zenako (2013), Anyone can listen to whoever they want. Is National Intelligence Service a state or secret shadow government? (*Όποιος θέλει ακούει όποιον θέλει. Κράτος ή παρακράτος η ΕΥΠ;* ) Unfollow, Issue 23 November 2013, pp. 58-67.

Greece, Enet, Massive interceptions, 10/5/2010. (*Μαζικές άρσεις απορρήτου*), 10 May 2010, available in Greek at: www.enet.gr/?i=news.el.article&id=160538 (Last accessed: 8 September 2014).

Greece, To Vima, 'Dispute between the National Information Service and the Hellenic Authority for Communication Security and Privacy on for interceptions', (*'Διαμάχη ΕΥΠ και ΑΔΑΕ για τις υποκλοπές'*), 22 November 2011, available in Greek at: www.tovima.gr/society/article/?aid=431544 (Last accessed: 8 September 2014).

Greece, TVXS, 'The employee responsible for the interceptions of American Embassy was found' *('Βρέθηκε ο υπάλληλος επικεφαλής υποκλοπών της αμερικανικής πρεσβείας')*, 10 March 2014, http://tvxs.gr/news/ellada/brethike-o-ypallilos-epikefalis-ypoklopon-tis-amerikanikis-presbeias (Last accessed: 8 September 2014).

Greece, To Vima, (2014), 'Snowden network in Athens', (*'Δίκτυο Σνοουντεν στην Ελλάδα'*), 13 July 2014, available in Greek at: www.tovima.gr/society/article/?aid=615036 (Last accessed: 8 September 2014).