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

AUSTRIA

Version of 22 September 2014

European Training and Research Centre for Human Rights and Democracy
ETC Graz

Summary

Preliminary remark on data retention in Austria:

1. Data retention, as large-scale communication surveillance, was in place in Austria between 1 April 2012 and 30 June 2014. Data retention was annulled by the Constitutional Court on 27 June 2014 and the relevant legal norms were repealed as of 1 July 2014 as being unconstitutional. The Constitutional Court ruled that the laws on data retention are unconstitutional and are against the fundamental right to data protection and Art. 8 European Convention on Human Rights (ECHR). A time period for reforming the laws was not granted, the repeal was ordered immediately. The reasons of the judges to repeal data retention were the following[1]:

- A massive infringement of fundamental rights, such as data retention, has to be established in such a way that it is in line with the Data Protection Act 2000 *(Datenschutzgesetz 2000, DSG 2000)* and the ECHR.

- Whether such interference is constitutionally allowed depends on the conditions for data retention and the safeguards regarding access and deletion. The norms in the Telecommunications Act 2003 *(Telekommunikationsgesetz 2003, TKG 2003)*, the Criminal Procedures Act *(Strafprozeßordnung 1975, StPO)* and the Security Police Act (*Sicherheitspolizeigesetz, SPG)* do not meet those requirements.

- Many precise legal safety conditions, such as the precise shaping of mandatory storage, conditions for access to this data and the obligation to delete this data are missing.

- The "spread width" (*Streuweite)* of data retention exceeds the infringements of the right to data protection dealt with in the jurisprudence of the Constitutional Court so far; regarding the affected persons – almost the entire population is affected – and also regarding the affected data and the modality of data usage.

[1] Austria, Constitutional Court (*Verfassungsgerichtshof)* (2014), available at: http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20140627_12G00047_00/JFT_20140627_12G00047_00.pdf (English extract available at: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/erwaegungeneng28082014.pdf). According to media reports, the Austrian Minister of Justice considers the reintroduction of data retention, albeit only in cases of most severe forms of crime. Austria, derStandard (2014), Vorratsdaten: Abgeschafft, doch nicht erledigt, 21 September 2014, available at: http://derstandard.at/2000005845186/Vorratsdaten-Abgeschafft-doch-nicht-erledigt.

- The right to data protection in a democratic society is directed to the facilitation and safeguarding of confidential communication among persons. The freedom as claim of the individual and as condition of society is defined by the quality of information-relationships.

- The Constitutional Court acknowledged that new communication technologies bear new challenges for the fight against crime, which is a public interest. This was kept in mind by the Constitutional Court.

- Rules like data retention may be legal for the fight against severe forms of criminality, but only if they are in conformity with laws on data protection and the ECHR. The norms on data retention are a disproportionate infringement and therefore a violation of the right to data protection.

2. The Constitutional Court did not deal with the question on how legislation on data retention could look like to be in line with constitutional rights.

3. According to information presented in the media, in 2013 354 requests to providers were made regarding data retention by the Austrian judicial authorities, but most of them did not prove to be helpful during investigations. None was linked to terrorism.[2]

4. As data retention, as the only means of mass surveillance is no longer in place, the following information is given regarding data acquisition by intelligence services in Austria in a broader understanding. This also includes the collection of data regarding suspected individuals and safeguards installed in this regard.

Legal framework of surveillance

a. Types of security services and bodies involved

5. The intelligence services (*Nachrichtendienste)* in Austria are part of the public administration and built into the Austrian structure of authorities.[3] There are three organisations conducting intelligence services: The Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, BVT),* the Military Defence Agency (*Heeresabwehramt)* and the Military Intelligence Service (*Heeresnachrichtenamt).* [4]

[2] Heise (2014), Austria: 354 requests to data, non regarding terrorism (*Österreich: 354 Anfragen nach Vorratsdaten, keine wegen Terrorismus),* available at: www.heise.de/newsticker/meldung/Oesterreich-354-Anfragen-nach-Vorratsdaten-keine-wegen-Terrorismus-2219648.html.

[3] Schätz, A. (2007), 'Nachrichtendienste im Transformationsprozess?' (Intelligence services in transformation process?), *Österreichische Militärische Zeitschrift* 4/2007, p. 395.

[4] Austria, Parliament (2013), Parliament Correspondence Nr. 813 of 20 November 2013 – European Solutions on data security and espionage defence necessary (*Parlamentskorrespondenz Nr. 813 vom 20*

6. The BVT is part of the General Directorate for Public Security of the Ministry of the Interior, and part of the police. Its main tasks are the collection of information, analysis and investigations for the protection of the state and its constitutional facilities, the fight against extremism, international arm trade, espionage, trade with nuclear material and organized crime in this regard. A key task is the fight against international terrorism within Austria.[5]

7. The other two agencies are military agencies and therefore part of the Federal Ministry of Defence and Sports. The Military Intelligence Service is the external intelligence service, whereas the Military Defence Agency is the homeland intelligence service of the military.

b. Extent of power

8. The Federal Agency for State Protection and Counter Terrorism is competent for the protection of the citizens and of the constitutional principles, as well as for the institutions of the state.

9. § 21 (3) SPG provides the legal basis for so-called "extended danger research" (*erweiterte Gefahrenforschung).* This rule allows the police to observe potentially dangerous groups and individuals way before criminal acts take place. According to § 54 SPG this may be done by way of surveillance, covert investigations, as well as by way of video and audio records. There are further restrictions in § 54 SPG regarding the specific methods of investigations (e.g. covert investigations and usage of video or audio records are only allowed, if a crime subject to considerable (*beträchtlich)* punishment is expected). Since April 2012 extended danger research has also been possible regarding individuals, if this person publicly speaks or writes for violence against persons or constitutionally safeguarded institutions and procures things to be able to endanger property or people in an extensive way.[6]

10. Through the amendment of the Security Police Act (*Sicherheitspolizeigesetz,* SPG)[7] in 2007, the police forces got extended powers regarding the surveillance of the internet (§ 53 (3a) SPG) and the detection of telecommunication equipment (*Endeinrichtung)* of persons (§53 (3b) SPG). Those tasks are conducted in secrecy without ex-post information of the persons, where there was suspicion that there is present

---

November 2013 - Europäische Lösungen bei Datensicherheit und Spionageabwehr nötig), available at: www.parlament.gv.at/PAKT/PR/JAHR_2013/PK0813/index.shtml.

[5] Schätz, A. (2007), 'Nachrichtendienste im Transformationsprozess?' (Intelligence services in transformation process?), *Österreichische Militärische Zeitschrift* 4/2007, p. 397.

[6] Salimi, F. (2013), 'Terrorbekämpfung durch Straf- und Sicherheitspolizeirecht' (*The fight against terror by Criminal Law and Security Police Law*), *Juristische Blätter* 2013, pp. 698 et seqq.

[7] Austria, Security Police Act (*Sicherheitspolizeigesetz),* BGBl Nr. 662/1992, last amended by BGBl I Nr. 44/2014, available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792.

endangerment for the live, health or freedom of this person, and without ex-ante control by the judiciary.[8]

11. According to § 53 (3a) Security Police Act (and analogously according to § 90 (7) Telecommunications Act) security police authorities are entitled to request public telecommunication providers and other service providers to give information regarding:

- Name, address and telephone number of a connection, if this is necessary to fulfil tasks according to this act.

- IP addresses regarding a specific message and the time of transmission, if they need this data as a relevant prerequisite to defend against a) concrete danger against life, health or freedom of a person (in the course of obligation of first aid); b) a dangerous attack or c) criminal organisations.

- Name and address of a user, who a certain IP address was assigned to, if this is needed as a relevant prerequisite to defend against a) concrete danger against life, health or freedom of a person (in the course of obligation of first aid); b) a dangerous attack or c) criminal organisations.

- Name, address and telephone number of a specific connection connected to a certain call and specific time frame and the passive number assigned, if this is necessary to fulfil general first aid or defence of dangerous attacks.

12. According to § 53 (3b) information on location data and the International Mobile Subscriber Identity (IMSI) of the endangered person or a person accompanying this person can be requested from public telecommunication services (*öffentliche Telekommunikationsdienste)* if it is to be assumed according to specific facts, that there is an imminent danger to life, health or freedom of a person. Furthermore technical tools to localise can be used.

13. The tasks of the Military Defence Agency are laid down in the Military Authority Act (*Militärbefugnisgesetz, MBG).*[9] Military self-protection is a task comprising also intelligence defence (*nachrichtendienstliche Abwehr)* according to § 2 (1) 2 MBG. According to § 4 MBG the principle of proportionality applies; i.e. in case an infringement of the rights of persons is necessary, it may only be made in so far proportionality regarding the reasons and the outcome is guaranteed. The measure which infringes the rights of the person the least is to be chosen according to § 4 (3) 1

[8] Zankl, W. (2009), *Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie* (On the way to a surveillance – state? New surveillance measures in the area of information and communication technology, Facultas/WUV, p. 25.

[9] Austria, Military Authority Act (*Militärbefugnisgesetz),* BGBl I Nr. 103/2002, last amended by BGBl I Nr. 181/2013, available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000864.

MBG. The second section (*Hauptstück*) of the MBG on military intelligence services mentions the powers of the service in §§ 21 et seqq. MBG. § 22 MBG deals with processing of data. § 22 (3 until 7) MBG describes the special data processing procedures and their preconditions. Observation and video- and audio surveillance is allowed, to defend against intentional attacks on military goods, to preventive protection of military goods, in case of danger of intentional attacks is probable because of specific reasons; for the reason of intelligence, if otherwise the fulfilment of intelligence would be hindered. Those actions have to be authorised by the Legal Protection Officer, as laid down in a constitutional stipulation in § 22 (8) MBG.

14. According to § 22 (2a) MBG military authorities may request public providers of telecommunication services to provide them with the name, address and telephone number of a specific connection, if this is needed as a relevant prerequisite to fulfil tasks of military intelligence or defence. The requested provider is obliged to give information immediately and free of charge.

c. Control and oversight mechanisms

15. Two permanent Sub-Committees to control intelligence services are installed in parliament according to § 32b Rule of Procedure Act 1975 (*Geschäftsordnungsgesetz 1975).*[10] One is installed to control the Federal Agency for State Protection and Counter Terrorism and is set up as sub-committee to the committee on the interior (*Ausschuss für innere Angelegenheiten),* the other one to control military intelligence services is set up as a sub-committee to the committee on defence (*Landesverteidigungsausschuss).* The committees are composed of 18 members each. The members of the committees are entitled to ask members of government for information. A request to look into documents requires a decision by the respective sub-committee. Members of government are obliged to grant access to documents, except when this is not possible or might endanger national interests or the security of persons.[11] The work of the sub-committees is confidential, so no information is available to the public or the media.

16. In December 2013 voices were raised, that the Federal Minister of Defence refused to provide information to the sub-committee on suspected collaboration with the NSA without any justification why no information is provided.[12]

---

[10] Austria, Rule of Procedure Act 1975 (*Geschäftsordnungsgesetz 1975),* BGBl Nr. 410/1975, last amended by BGBl I Nr. 6/2014, available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000576.

[11] Austria, Parliament (*Parlament),* Permanent sub committees to control intelligence services (*Ständige Unterausschüsse zur Kontrolle der Nachrichtendienste),* available at: www.parlament.gv.at/PERK/KONTR/POL/6STAEND_UNTERAUSSCHUESSE/index.shtml.

[12] Austria, The Press (*Die Presse)* (2013), Pilz: Klug paralyses parliamentary control (*Pilz: Klug legt "parlamentarische Kontrolle lahm")*, available at: http://diepresse.com/home/politik/innenpolitik/1494196/print.do.

d. Geographical scope of surveillance

17. The Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung)* works on the national level and is also responsible for cooperation with foreign police and intelligence services.[13]

18. The Military Defence Agency (*Heeresabwehramt)* is the homeland intelligent service, operating within Austria. The Military Intelligence Service (*Heeresnachrichtenamt)* is the foreign intelligence service operating abroad, for example for gathering important information about regions where the Austrian military is deployed.[14] Media reported in July 2014, that the *Königswarte* in Lower Austria is used to collect data. A journalist reported that it mainly targets civil satellites.[15]

d. Condition of surveillance and purposes

19. As already stated above, the military services may start observance, video and audio surveillance to hold off intentional attacks against military goods, to protect military goods, if attacks are awaited and to conduct intelligence, if otherwise intelligence is hindered (see § 22 (3) and (5) MBG). An ex-ante authorization by the Legal Protection Officer is needed.

20. § 21 (3) SPG provides the legal basis for so-called "extended danger research" (*erweiterte Gefahrenforschung).* This rule allows the police to observe potentially dangerous groups way before criminal acts take place (surveillance, covert investigations, image and audio records). As of April 2012 extended danger research is also possible regarding individuals, if this person publicly speaks or writes for violence against persons or constitutionally safeguarded institutions and procures things to be able to endanger property or people in an extensive way and it is to be expected that this person effectuates ideological or religious violence that pose a threat to public security. [16]

21. Through the amendment of the SPG in 2007, the police forces got extended powers regarding surveillance of the internet (§ 53 (3a) SPG) and detection of

[13] Austria, Federal Ministry of the Interior (*Bundesministerium für Inneres),* Protection of the constitution (*Verfassungsschutz),* available at: www.bmi.gv.at/cms/bmi_verfassungsschutz/.

[14] Federal Ministry of Defence (*Bundesministerium für Landesverteidigung)* (2013), Military – Military intelligence service important for actions abroad (*Bundesheer: Nachrichtenamt wichtig für Auslandseinsätze),* Press release, 14 June 2013, available at: www.ots.at/presseaussendung/OTS_20130614_OTS0168/bundesheer-nachrichtenamt-wichtig-fuer-auslandseinsaetze.

[15] Austria, The Standard (*der Standard)* (2014), Königswarte – Austria listens until the Middle East (*Köngiswarte: Österreich lauscht bis in den Nahen Osten),* 7 July 2014, available at: http://derstandard.at/2000002770626/Koenigswarte-Oesterreich-lauscht-bis-in-den-Nahen-Osten?dst=l.facebook.com.

[16] Salimi, F. (2013), 'Terrorbekämpfung durch Straf- und Sicherheitspolizeirecht', *Juristische Blätter* 2013, pp. 698 et seqq.

telecommunication equipment (*Endeinrichtungen)* of persons (§53 (3b) SPG). Those tasks are conducted in secrecy without ex post information of the persons, where there was suspicion that there is present endangerment for the live, health or freedom of this person and without ex-ante control of the judiciary.[17] According to § 53 (3a) SPG the police is entitled to request the name, address and telephone number, IP addresses and name and address of persons who are linked to a certain IP address from public telecommunication services providers according to § 92 (3) Z1 TKG 2003 or other service providers according to § 3 Z2 ECG, if this information is necessary for the police to perform their legal tasks or if it is necessary for certain, further specified tasks in fighting crime.

22. In case of § 21 (3) SPG the Legal Protection Officer has to be informed ex-ante according to § 91c (3) SPG. He then has to authorise the measures. For other measures, e.g. those of § 53 SPG the Legal Protection Officer also has to be informed as soon as possible (*ehestmöglich)*, providing the main reasons for those actions (§ 91 c (1) SPG).

e. Different stages of surveillance

23. As data retention is no longer in place in Austria, there is no pertinent information on the procedures for collection, analysis, storing or destruction of such surveillance data.

Safeguards

Parliamentary Sub-Committees

24. Permanent Sub-Committees to control intelligence services *(Ständige Unterausschüsse zur Kontrolle der Nachrichtendienste)* are installed at the Parliament according to § 32 b Rule of Procedure Act (*Geschäftsordnungsgesetz 1975*[18]). Detailed information on them is provided above at 1c and in Annex 2.

Legal Protection Officers

25. There are Legal Protection Officers established in Austria. The idea behind the Legal Protection Officers is to provide sufficient legal protection for persons, who are affected by secret investigations. As those persons do not know about those investigations, the Legal Protection Officer shall administer their rights as a

[17] Zankl, W. (2009), *Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie* (On the way to a surveillance – state? New surveillance measures in the area of information and communication technology, Facultas/WUV, p. 25.

[18] Austria, Rule of Procedure Act 1975 (*Geschäftsordnungsgesetz 1975),* BGBl Nr. 410/1975, last amended by BGBl I Nr. 6/2014, available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000576.

substitute.[19] The Legal Protection Officer is entitled to file complaints in front of the data protection authority according to § 57 (6)2 MBG and § 91 d (3) SPG, when he notices that personal rights of persons have been affected through the use of personal data. In case of the Military Authority Act this is linked to the prerequisite that the knowledge of the affected person regarding the existence or the content of the data set would endanger or hinder the assurance of the operational readiness of the military or would endanger or hinder the interests of the comprehensive defence of the country. In case of the Security Police Act, the competence of the Legal Protection Officer is given, if informing the affected person is not possible because of the reasons of § 26 (2) DSG. This is the case, if there are predominant public reasons speaking against informing the affected person (such as protection of constitutional institutions of the republic, assuring the readiness of the military, assuring the interests of defence of the country, protection of external, economic or financial interests of the republic or the EU and prevention, hindrance or prosecution of criminal acts).

26. It has to be noted that the Legal Protection Officers is obliged to inform the person in question according to §91d (3) Security Police Act.

27. Regarding the military defence agency an independent and not-bound by directives Legal Protection Officer (*Rechtsschutzbeauftragter,* see also § 57 MBG) is entitled to control all measures of the intelligence defence (*nachrichtendienstliche Abwehr)* (§ 22 (8) MBG – this is a constitutional law provision). The Legal Protection Officer gives an annual report to the Federal Minister of Defence and Sport. The permanent sub-committee of the defence committee of the parliament is entitled to gain access to the annual report upon request, as far as granting access does not endanger national security or the security of individuals (Article 52a of the Federal Constitution).

28. There is a Legal Protection Officer also established for the Security Police Act (§ 91 SPG). He is responsible regarding matters to identify person-related data, which are mentioned in an exhaustive list in § 91 c (1) SPG. There are three intensity steps for control:[20]

    - notification for ex-post control (§ 91 c (1) SPG)

    - notification for ex-ante statements (§ 91 c (2) SPG)

    -Asking for authorisation regarding extended danger research (§ 91 c (3) SPG).

[19] Zankl, W. (2009), *Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie* (On the way to a surveillance – state? New surveillance measures in the area of information and communication technology, Facultas/WUV, pp. 113 et seqq.

[20] Further information on the actions of the Legal Protection Officer is provided on the Website of the Ministry of the Interior at: www.bmi.gv.at/cms/BMI_Rechtsschutzbeauftragter/aufgaben/start.aspx.

29. The Legal Protection Officer has to inform the persons affected or can file – in specific cases – a complaint in front of the Data Protection Authority.

Judicial or non-judicial remedies

30. Generally speaking, the data protection authority is competent for complaints against public and private entities regarding the right to obtain information (§ 1 (3) Z1 and § 26 Data Protection Act 2000, *Datenschutzgesetz 2000,* DSG 2000), for complaints against public entities regarding the right to secrecy and the right to rectification or erasure (§ 1 (1, 2) (3 Z 2) and § 27 DSG). Apart from that, the Data Protection Authority is competent to investigate proprio motu in the private and public sector if it is of the opinion that rules on data protection have been infringed. 2000).

31. § 54 (4) Military Authority Act foresees, that the Data Protection Authority is competent regarding the violation of rights through data procession against the norms of this law.

32. According to § 90 SPG the Data Protection Authority decides on claims because of the violation of rights because of data processing through the security administration (*Sicherheitsverwaltung)* according to § 31 DSG 2000. According to § 90 second sentence SPG the assessment of legality of processing of data through exercise of power of command or power of enforcement is exempted. In this case the Federal Administrative Court decides on appeals, allowing for judicial review. The Committee on the Interior as well as the Committee on Defence of the Parliament established permanent sub-committees on controlling of intelligence services. The members of the sub-committees can ask any members of the government on information. The meetings of the sub-committees are confidential; no public reports on these meetings are available.[21] According to § 32 d (2) Rule of Procedure Act *(Geschäftsordnungsgesetz)*[22] the sub-committees have to be held once every three months.

33. Any person who wants to complain about public administration may file an informal claim free of charge at the Austrian Ombudsman Board (*Volksanwaltschaft).*

34. Furthermore, the parliamentary military commission *(parlamentarische Bundeesheerkommission)* and the data protection authority, the administrative courts,

[21] Austria, Parliament (*Parlament)* (2014), Ständige Unterausschüsse zur Kontrolle der Nachrichtendienste, available at: www.parlament.gv.at/PERK/KONTR/POL/6STAEND_UNTERAUSSCHUESSE/index.shtml.

[22] Austria, Rules of Procedure Act (*Geschäftsordnungsgesetz),* BGBl Nr. 302/1979, last amended by BGBl I Nr. 6/2014, available at: www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000576.

the Ombudsman Board and the courts can be addressed by the persons affected.[23] According to § 54 MBG, the Federal Administrative Court decides on complaints against power of command or power of enforcement (*Befehls- und Zwangsgewalt).*

35. **Additional note**: There is a recent discussion in Austria regarding espionage in Germany by US agents and links to Austria. According to various experts, Austria and especially Vienna has always been a centre for espionage since the Cold War. There is only low profile counter-espionage (*Spionageabwehr)* according to the former head of the Federal Agency for State Protection and Counter Terrorism.[24] In its annual report 2014 the Federal Agency for State Protection and Counter Terrorism states that "the geopolitical central position, the location of several international organisations, good infrastructure, low criminal sanctions and short statutory limitations (*Verjährungsfristen)* seem to favour intelligence actions in Austria".[25] The spokesperson on security of the green party asks for the establishment of a counter-espionage system in Austria in July 2014.[26]

36. Regarding cooperation with other intelligence services, the Federal Ministry of Defence stated in 2013 that cooperation is only conducted to guarantee security in Austria. It is strongly limited, only based on assignments and always in line with Austrian laws, especially data protection laws. Data on Austrians is not provided and there is no mass-exchange of data.[27]

37. According to § 25 (1) 4 Military Authority Act, data may be transferred to foreign authorities or international organisations or other inter-state organisations if this is based on an international law obligation or is a relevant prerequisite to fulfil the tasks of intelligence or defence.

---

[23] Austria, Federal Ministry for Defence (*Bundesministerium für Landesverteidigung),* The military defence agency – competent-reliable-safe (*Das Abwehramt, kompetent – verlässlich-sicher),* available at: www.bmlv.gv.at/organisation/beitraege/n_dienste/pdf/abwa.pdf.

[24] Austria, ORF (2014), ZIB 2 interview with Dr. Polli, former Head of the Federal Agency for State Protection and Counter Terrorism on 14 July 2014, available at: http://tvthek.orf.at/program/ZIB-2/1211/ZIB-2/8189420/Gert-Rene-Polli-zu-Spionage-in-Oesterreich/8189424.

[25] Austria, Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusnekämpfung)* (2014), Constitutional Protection Report 2014 *(Verfassungsschutzbericht 2014),* available at: www.bmi.gv.at/cms/BMI_Verfassungsschutz/BVT_VSB_2014_V20140613_online.pdf, p. 54 et seq.

[26] Austria, ORF Futurezone (2014), Pilz wants to strengthen counter-espionage in Austria (*Pilz will Spionageabwehr in Österreich forcieren),* 16 July 2014, available at: http://futurezone.at/netzpolitik/pilz-will-spionageabwehr-in-oesterreich-forcieren/75.221.216.

[27] Federal Ministry of Defence (*Bundesministerium für Landesverteidigung)* (2013), Military – Military intelligence service important for actions abroad (*Bundesheer: Nachrichtenamt wichtig für Auslandseinsätze),* Press release, 14 June 2013, available at: www.ots.at/presseaussendung/OTS_20130614_OTS0168/bundesheer-nachrichtenamt-wichtig-fuer-auslandseinsaetze.

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance[28]

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

[28] **Please note**, that the relevant norms on data retention in the telecommunications act, the criminal procedures act and the security police act are no longer in place but repealed by the Constitutional Court as being unconstitutional (for the detailed list on norms repealed see www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf, p.3.).
De facto data retention was the only tool of real broad scale mass surveillance in Austria.

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)?**
					etc.		
Military Authority Act (*Militärbefugnis gesetz)*, act of parliament	Anybody suspected	If there are threats for military security	Military security	According to § 22 (8) Military Authority Act the Legal Protection Officer is only responsible regarding observation and audio- and video surveillance (his previous approval has to be acquired), but not for those information requests to telecommunication providers.	Military authorities may ask providers of public telecommunication services on information about name, address and number of a connection, if they need it as a prerequisite to fulfil their intelligence tasks. The provider has to provide information immediately and free of charge.	Limited to providers of telecommuniatio n services in Austria regarding § 22 (2a) MBG.	No
Security Police Act (*Sicherheitspolizei gesetz)*	Anybody suspected	Defence against criminal connections or dangerous attacks and to prevent dangerous attacks	Defence against criminal connections or dangerous attacks and to prevent dangerous	In the case of extended danger research the approval of the Legal Protection Officer has to be acquired according	The police is allowed to request information from public telecommunication service providers according to § 92 (3) Z1 TKG 2003 and	Providers of telecommunicati on services in Austria	No

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)?
			attacks.	to § 91 c (3) SPG, it can only be issued for a maximum of thee months and be renewed only once.	other service providers according to the E-Commerce Act, e.g. in case this data is needed to prevent dangerous attacks (§53 (3a) SPG).		

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

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
Include a reference to specific provision and describe their content	*e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.*	*Please, provide details*	*Please, provide details*
Data Protection Act 2000 (Datenschutzgesetz 2000)	Right to be informed, right to rectification/erasure, right to challenge (§§ 26-28 DSG).	The law applies to processing of personal data within Austria and applies for everybody (nationals, EU nationals, third country nationals). Furthermore when data is used in another member state of the EU for the reason of a branch of a controller within Austria. According to § 57 (6) Military Authority Act the Legal Protection Officer is entitled to inform the individual OR file a complaint at the data protection authority. He/she might only file this complaint, if the knowledge about the existence or about the content	Inside and sometimes EU (see section left of this colum).

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
		of the data would endanger the safeguard or readiness of the military or would endanger the interest of national defense or hinder it and therefore providing this information to the individual is not to be conducted. A similar provision can be found in the Security Police Act § 91 d (3). Yet, this provision obliges the Legal Protection Officer, while the provision in the Military Authority Act only entitles him/her: if the Legal Protection Officer obtains knowledge about the fact that personal data of individuals is used without their knowledge, he is obliged to inform them, or if this is not possible according to § 26 (2) Data Protection Act 2000, he is obliged to file a complaint at the Data Protection Authority if he notices a violation of rights of the	

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
		affected person. § 26 (2) Data Protection Act states, that (amongst others) information is not to be given to the individuals, if overarching public interests speak against it. Such public interests are the protection of constitutionally safeguarded institutions of the Republic of Austria, securing the readiness of the military, securing the interests of national defense, the protection of foreign affairs, economic or financial interests of the Republic of Austria or the EU and the prevention, hinderance or prosecution of crimes. A refusal to give information on these grounds is subject to a special supervisory procedure before the Data Protection Authority (§ 31a DSG 2000)	

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**
European Convention of Human Rights	Right to privacy (Art. 8).	The ECHR is a constitutional law and applies to all persons – EU citizens and third country nationals	
Basic Law on the General Rights of Nationals (*Staatsgrundgesetz)*	Secrecy of communication via telecommunication. Does only apply for messages sent to a specific person, not for public messages (blogs, message boards, etc). It's not clarified whether secrecy of communication is valid only for content data or also for traffic data.[29] This was clarified by the Constitutional Court in 2012, stating that it applies to content	On Austrian nationals according to the law. Because of the anti-discrimination rules of the EU also EU nationals can refer to the right to secrecy of communication based on the Staatsgrundgesetz.	Austria

[29] Zankl, W. (2009), *Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie* (On the way to a surveillance – state? New surveillance measures in the area of information and communication technology, Facultas/WUV, p. 65 et seq.

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
	data but not the entire traffic of telecommunication.[30]		

[30] Austria, Constitutional Court (2012), B 1031/11, VfSlg. 19.657/2012, www.ris.bka.gv.at/Dokumente/Vfgh/JFT_09879371_11B01031_00/JFT_09879371_11B01031_00.pdf.

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.*
Permanent Sub-Committees to controll intelligence services (*Ständige Unterausschüsse zur Kontrolle der Nachrichtendienste)*	Parliamentary, one sub-comittee is organised as a sub committee of the committee on the interior (*Ausschuss für innere Angelegenheiten)*, one is organised as a sub committee to the committee on defence	§ 32 b Rule of Procedure Act *(Geschäftsordnungsgesetz 1975)*	Ex-post	Each sub-committee has to comprise one member of the parties which are also present in the main committee. Both sub committees have 18 members.[31] Regularly the sub-committees are assisted by one member of staff of each faction (*Fraktion)* as well as two members of staff	Each member of the sub-committees is entiteled to ask members of governemnt for information. The request to look into documents requires a decision by the relevant sub-committee. Members of governemnt are obliged to grant access to documents, except when

[31] Austria, Parliament (*Parlament),* Permanent sub-committee to the committee on defence, list of members (*Ständiger Unterausschuss des Landesverteidiungsausschusses, Mitglieder),* available at: www.parlament.gv.at/PAKT/VHG/XXV/SA-LV/SA-LV_00001_00357/MIT_00357.html; Austria, Parliament (*Parlament),* Permanent sub-committee to the committee on the interior, list of members (*Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten, Mitglieder),* available at: www.parlament.gv.at/PAKT/VHG/XXV/SA-IA/SA-IA_00001_00355/MIT_00355.html.

	(*Landesverteidigungs ausschuss).* This is due to the division of Austrian intelligence services.			of the directorate of the parliament.[32]	this is not possible or might endanger national interests or security of persons.[33] The work of the sub-committees is confidential, so no information is available for the media or public.
Legal Protection Officer (Security Police Act)	Public Authority staff	§ 91a et seqq. Security Police Act;	ex-ante and ex-post (for details see column on powers)	According to the Security Police Act one Legal Protection Officer with two substitutes. They are appointed by the Federal President, after proposal by the federal government und after hearing the president of the national assembly (*Nationalrat)*, the president of the constitutional court and the highest administrative court for a period of five years. Re-appointment is possible. He is assisted by his two substitutes and two other	Ex-ante authorisation of extended danger research (foreseen in § 21 3 SPG) As § 91c (3) states this ex ante authorisation applies to all measures of § 21 (3) SPG. The same applies, if special investigation methods are planned in the course of extended danger research according to § 54 (2, 2a, 3 and 4) (i.e. observation, covered investigations, video and audio surveillance) or if gathered data should be processed according to § 53 (5) (i.e. data gathered by

[32] Information received from the Directorate of the Parliament – citizen service, on 1 September 2014.

[33] Austria, Parliament (*Parlament),* Permanent sub committees to control intelligence services (*Ständige Unterausschüsse zur Kontrolle der Nachrichtendienste),* available at: www.parlament.gv.at/PERK/KONTR/POL/6STAEND_UNTERAUSSCHUESSE/index.shtml.

				persons (one head of bureau and one legal assistant). Furthermore he may – on demand – be assisted by Section III/7 of the Federal Ministry of the Interior on legal issues and data protecton.[34]	legal subjects of the public and private sphere by use of audio or video equipment). Has to be informed ex-ante or at least as soon as possible (*ehestmöglich)* about any investigation of personal data. Is entitled to observe the actions of the police authorities in scope of his mandate according to § 91 c SPG. Has to inform persons affected or file a complaint to the Data Protection Authority, if the person affected is not to be informed according to § 26 (2) Data Protection Act. Annual report to the Federal Ministry of the Interior until 31 March each year. According to § 91 c (1) SPG security authorities are obliged to inform the Legal Protection Officer about any investigation of personal data through

[34] Information received from the Federal Ministry of the Interior on 5 September 2014.

					observation (§ 54 (1), covered investigations (§ 54(3)), covered usage of video- and audio recorders (§ 54 (4)), procession of data which was gathered by others via video- and audio recorders (§ 53 (5)) with information of the main reasons. Furthermore, the Legal Protection Officer is to be informed about the request for information (§ 53 (3a) Z 2 to 4 und 3b), the information of individuals affected (§ 53 (3c)), the usage of technical devices to locate terminal equipment (§ 53 (3b), as well as the usage of license plate detection devices (54 (4b) as soon as possible. Security authorities which plan the surveillance of public places with video and audio equipment according to § 54 (6 and 7), data usage according to § 53 (1) Z7 or a data usage according to §53 a (2 and 6) have to immediately

					inform the Federal Minister of the Interior. He has to give the Legal Protection Officer the possibility to make a statement within three days. Actual use of video- and audio surveillance or start of data procession is only allowed to start after those three days or after the Legal Protection Officer has made his statement (§ 91 c (2)).

Legal Protection Officer (Military Authority Act)	Public Authority staff	§ 57 Military Authority Act	Both (for detail see column on powers)	According to the Military Authority Act one Legal Protection Officer with two substitutes. They are appointed by the Federal President, after proposal by the federal government und after hearing the president of the national assembly (*Nationalrat)*, the president of the constitutional court and the highest administrative court for a period of five years. Re-appointment is possible. The Legal Protection Officer and his substitutes have three persons as supporting staff.[35]	Ex-ante approval of data investigation (§ 22 (8) Military Authority Act). Access to all relevant information, official secrecy cannot be invoked. Might observe those actions he is entiteled to control at any time. Has to observe the obligations regarding rectification or deletion of data according to the Data Protection Act 2000. Has to inform persons affected or file a complaint to the Data Protection Authority, if the person affected is not to be informed because this would endanger or hinder the readiness of the military or endanger the interests of national defence. Annual report to the Federal Minister of Defence and Sport until 31 March each year

[35] Information received from the Federal Ministry of Defense on 2 September 2014.

Data Protection Authority	Public authority	§§ 30, 31, 35, 36 Data Protection Act 2000	Ex post	The head of the data protection authority is appointed by the Federal President (*Bundespräsident)* for five years according to § 36 DSG 2000. The proposal has to be preceded by a biding to general application. This has to be arranged by the Federal Chancellor. The Data Protection Authority has all together a staff of 24 persons, 6 of them working part-time.[36]	Issues legally binding decisions on individual complaints. Issues (non-binding) recommendations in certain cases (§ 30 DSG 2000), e.g. in cases of investigations that are initiated proprio motu.

[36] Information received by the Data Protection Authority on 13 August 2014 via E-Mail.

Annex 3 – Remedies[37]

Security Police Act				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	The person affected does not have to be informed obligatory, but the Legal	No, as there is not even an obligation to inform the subject, there is also not right to access the data.	The Legal Protection Officer is the relevant safeguard. He has to be informed regarding any investigation of personal data through observation, audio or video, etc. (§ 91 c). In case public	§§ 88 et seqq. Security Police Act.

[37] 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.

	Protection Officer is entitled to do so. So this question cannot clearly be answered using yes/no.		places should be investigated using audio or video equipment, the Federal Ministry of the Interior has to be informed and the Legal Protection Officer has to have the possibility to comment within 3 days. In case a person is informed about collection of data, he/she might address the Data Protection Authority.	
Analysis*	See above		See above	
Storing*	See above		See above	
Destruction*	See above		See above	
After the whole surveillance process has ended	See above		See above	

Military Authority Act				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection[*]	No	No	The Legal Protection Officer is the relevant safeguard. He is entitled to request all relevant data and information. Only if the information regarding the identity of persons or sources would endanger national security or the security of persons this does not apply according to § 57(4) Military Authority Act. In case he notices, that the rights of persons were violated through data procession	According to § 54 (1) Military Authority Act each persons may address the Federal Administrative Court in cases of direct orders or coercive measures (*Befehls und Zwangsgewalt*) or other measures, insofar these were not issued as decisions (§ 54 (2)). The Data Protection Authority decides in cases of violation of the rights through data

[*] 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.

			and this subject does not know about it, he is entitled to inform the subjec or file a complaint at the data protection authority. This complaint is only allowed, if the knowledge of the subject about the existence or content of the data set would endanger or hinder the assurance of the operational readiness of the military or would endanger or hinder the interests of the comprehensive defence of the country. In case a person is informed about collection of data, he/she might address the Data Protection Authority.	processing according to § 54 (4).
Analysis*	See above	No	See above	
Storing*	See above	No	See above	
Destruction *	See above	No	See above	
After the whole surveillance process has ended	See above	No	See above	

Data Protection Act 2000 (*Datenschutzgesetz 2000)*				
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[*]	Depends, cannot clearly be answered using yes/no. There is no legal obligation in the Military Authority Act or the Security Police Act to inform the subject. But the	Depends, cannot clearly be anwered using yes/no. Generally, the subject has a right to disclosure according to the § 26 Data Protection Act 2000. The information provided has to include the data processed, the	As laid down in § 54(4) Military Authoriy Act and § 90 Security Police Act, the Data Protection Authority is compentent on complaints regarding the violations of rights through procession of personal data. Regarding intelligence services, it has to be kept in mind, that the individuals might not receive knowledge of this procession of data, so the way to the Data Protection Authority	§ 54 (4) Military Authority Act, § 90 Security Police Act, Data Protection Act 2000.

[*] 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.

	Legal Protection Officers are obliged to do so (specific information provided in the two tables above in this Annex 3).	information on where the data came from and who it received, the reason for data usage and the legal basis for it. However, according to § 26 (2) the information is not to be provided, if there are predominant public reasons speaking against informing the affected person (such as protection of constitutional institutions of the republic, assuring the readiness of the military, assuring the interests of defence of the country, protection of external, economic or financial interests of the republic or the EU and prevention, hindrance or prosecution of	might not be open for them. As laid down in the Military Authority Act, the Legal Protection Officer is not obliged to inform the individual but is only "entitled" to do so (under the conditions mentioned above). The Data Protection Authority is competent to decide on claims regarding disclosure (against public and private sector entities), confidentiality or correction or deletion of information (regarding public entities). For these claims the Data Protection Authority is able to conduct legally binding decisions on the issues. The decisions against private sector entities are executable, while those against public entities are purely declaratory (*Feststellungsbescheid).* Public sector entities are bound by law to immediately follow the legal interpretation, so no remit is needed (*Leistungsauftrag).*[38] Appeals against decisions of the Data Protection Authority can be brought to the Federal	

[38] Austria, Data Protection Authority (*Datenschutzbehörde),* Legal Protection regarding violations of data protection (*Rechtsschutz bei Datenschutzverletzungen),* available at: www.dsb.gv.at/site/6189/default.aspx.

		criminal acts).	Administrative Court according to § 38 (3) DSG 2000. The Federal Administrative Court decides as a senate, comprising one judge and two lay judges. According to § 32 Data Protection Act 2000 claims against private sector entities regarding confidentiality or correction or deletion of information have to be brought to the civil courts. According to § 32 (2) the claimaint has a right to ommission, irrespective of culpability. The Regional Courts act as courts of first instance in cases of data protection claims according to § 32 (4) DSG 2000, so representation by an attorney is obligatory according to § 27 Civil Procedures Act (*Zivilprozessordnung, ZPO).* Appeals can be brought to the Higher Regional Courts.	
Analysis*	See above	See above	See above	See above
Storing*	See above	See above	See above	See above
Destruction *	See above	See above	See above	See above
After the whole surveillance process has ended	See above	See above	See above	See above

Annex 4 – Surveillance-related case law at national level

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

Note:

There is no case law available on surveillance related cases regarding surveillance by intelligence services since 2006. The database of the Data Protection Authority was checked at ris.bka.gv.at using the search term "surveillance". Only cases regarding complaints against surveillance by police forces were identified (e.g. Cases K121.862/00012-DSK/2012 and K121.637/0009-DSK/2010). In 2002 there was a case in front of the Data Protection Commission regarding the Intelligence Service, but it was rejected due to formal reasons and therefore not included in a table here, as it did not provide any information on material issues (K120.758/003-DSK/2002). According to information received by the Data Protection Authority inquiries regarding the right to information increased in 2013, related to the discussion on NSA and data transfer in Austria. Independent of these inquiries three procedures were launched against the Federal Agency for State Protection and Counter Terrorism. One procedure was started against the Military Defence Agency. No further detailed information was provided on these procedures.[39] Looking into the Public Registry of the Courts no law suits linked to the Snowden relevations could be found.[40] Ex-officio investigations by the Data Protection Authority were started regarding the Federal State Agency for State Protection and Counter Terrorism, the Military Defence Agency and the Military Intelligence Service. The procedure against the State Agency for State Protection and Counter Terrorism was already suspended, the procedure against the other two institutions is close to being suspended.[41]

Case title	G 47/2012
Decision date	27 June 2014

[39] Information received by the Data Protection Authority on 13 August 2014.

[40] An additional information request was sent to the Data Protection Authority on 1 September 2014.

[41] Information received by the Data Protection Authority on 2 September 2014. No details on the procedures were provided.

Reference details (type and title of court/body; in original language and English [official translation, if available])	Constitutional Court (*Verfassungsgerichtshof),* full text judgment available at: http://www.ris.bka.gv.at/Dokumente/Vfgh/JFT_20140627_12G00047_00/JFT_20140627_12G00047_00.pdf ; English extract available at: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/erwaegungeneng28082014.pdf).
Key facts of the case (max. 500 chars)	In 2012, 11.139 persons filed an individual complaint to the Constitutional Court against data retention (of which all but one complaints were rejected by the Constitutional Court). Several norms of the Telecommunications Act *(Telekommunikationsgesetz 2003, TKG 2003*), the Criminal Procedures Act *(Strafprozeßordnung 1975, StPO)* and the Security Police Act (*Sicherheitspolizeigesetz, SPG)* were named as being unconstitutional.
Main reasoning/argumentation (max. 500 chars)	Data retention in this form violates the right to data protection and Art. 8 ECHR. It is an inproporationate infringement of those rights.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Data protection, proporationality of interference with fundamental rights.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The norms on data retention in the Austrian laws (Telecommunication Act, Criminal Procedures Act, Security Police Act) were repealed.

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**
Ausschuss für innere Angelegenheiten	Parliamentary committee	Parlament, Dr. Karl Renner-Ring 3 1017 Wien, Österreich	http://www.parlament.gv.at/PAKT/VHG/XXV/SA-IA/SA-IA_00001_00355/index.shtml
Landesverteidi-gungsausschuss	Parliamentary committee	Parlament, Dr. Karl Renner-Ring 3 1017 Wien, Österreich	http://www.parlament.gv.at/PAKT/VHG/XXV/SA-LV/SA-LV_00001_00357/index.shtml
Heeresnachrichten-amt (Military Intelligence Service)	Public authority	Federal Ministry of Defence (*Bundesministerium für Landesverteidiung und Sport)* Roßauer Lände 1 1090 Wien **Tel.:** 050201 - 0	None
Heeresabwehramt (Military Defense Agency)	Public authority	Hetzgasse 2 1030 Wien-Landstraße	None

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Federal Agency for State Protection and Counter Terrorism)	Public Authority	Herrengasse 7 1014 Wien BMI-II-BVT@bmi.gv.at	www.bmi.gv.at/cms/bmi_verfassungsschutz/
Datenschutzbehörde/ Data Protection Authority	Public Authority	Hohenstaufengasse 3 1010 Wien Telefon: +43 1 531 15 / 202525 Telefax: +43 1 531 15 / 202690 E-Mail: dsb@dsb.gv.at	www.dsb.gv.at
Bundesministerium für Landesverteidigung und Sport (Federal Ministry of Defence (Legal Protection Officer))	Public Authority	Roßauerlände 1 1090 Wien Tel.: 050201 - 0	http://www.bmlv.gv.at/
Bundesministerium für Inneres (Federal Ministry of the Interior (Legal Protection Officer))	Public Authority	Herrengasse 7, 1014 Wien Postfach 100 Tel.: +43-(0)1-531 26-0 Fax: +43-(0)1-531 26-108613	www.bmi.gv.at

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

Federal Ministry of Defence (*Bundesministerium für Landesverteidigung)* (2013), Military – Military intelligence service important for actions abroad (*Bundesheer: Nachrichtenamt wichtig für Auslandseinsätze)*, Press release, 14 June 2013, available at: www.ots.at/presseaussendung/OTS_20130614_OTS0168/bundesheer-nachrichtenamt-wichtig-fuer-auslandseinsaetze.

Federal Ministry for Defence (*Bundesministerium für Landesverteidigung)*, The military defence agency – competent-reliable-safe (*Das Abwehramt, kompetent-verlässlich-sicher)*, available at: www.bmlv.gv.at/organisation/beitraege/n_dienste/pdf/abwa.pdf.

Parliament (2013), Parliament Correspondence Nr. 813 of 20 November 2013 – European Solutions on data security and espionage defence necessary (*Parlamentskorrespondenz Nr. 813 vom 20 November 2013 - Europäische Lösungen bei Datensicherheit und Spionageabwehr nötig)*, available at: www.parlament.gv.at/PAKT/PR/JAHR_2013/PK0813/index.shtml.

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

Data Protection Authority (*Datenschutzbehörde)*, Data Retention (*Vorratsdatenspeicherung)*, available at: www.dsb.gv.at/site/cob__47811/7713/default.aspx.

3. Non-governmental organisations (NGOs)

Krisch, A. (2012), data retention vs. Fundmanental rights (*Vorratsdatenspeicherung vs. Grundrechte)*, power point presentation, available at:www.dsb.gv.at/DocView.axd?CobId=48998.

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

The Press (*Die Presse)* (2013), Pilz: Klug paralyses parliamentary control (*Pilz: Klug legt "parlamentarische Kontrolle lahm")*, available at: http://diepresse.com/home/politik/innenpolitik/1494196/print.do.

Eidenberger, H. (2011), nosy computers – on the state of automatic mass surveillance (*Neugierige Computer - Zum Stand der automatisierten Massenüberwachung),* Sachverständige 2011, p. 63.

Fritzl, M. (2010), *Military intelligence service blushes (*Heeresnachrichtenamt: ein Geheimdienst errötet), in Die Presse, 13 July 2010, available at: diepresse.com/home/politik/innenpolitik/580975/Heeresnachrichtenamt_Ein-Geheimdienst-errotet.

Heise (2014), Austria: 354 requests to data, non regarding terrorism (*Österreich: 354 Anfragen nach Vorratsdaten, keine wegen Terrorismus),* available at: www.heise.de/newsticker/meldung/Oesterreich-354-Anfragen-nach-Vorratsdaten-keine-wegen-Terrorismus-2219648.html.

Profil (2013), Heeresnachrichtenamt: was die US-Geheimdienste absaugen, available at: www.profil.at/articles/1328/560/362038/hna-heeresnachrichtenamt-was-us-geheimdienste.

Raschauer N./Wessely W. (2005), Military Authority Act Commentary (*Militärbefugnisgesetz Kommentar)*, NWV.

Salimi, F. (2013), 'Terrorbekämpfung durch Straf- und Sicherheitspolizeirecht' (*The fight against terror by Criminal Law and Security Police Law*), *Juristische Blätter* 2013, pp. 698 et seqq.

Schätz, A. (2007), 'Nachrichtendienste im Transformationsprozess?' (Intelligence services in transformation process?), *Österreichische Militärische Zeitschrift* 4/2007, p. 395-406.

The Standard (*der Standard)* (2014), Königswarte – Austria listens until the Middle East (*Köngiswarte: Österreich lauscht bis in den Nahen Osten),* 7 July 2014, available at: http://derstandard.at/2000002770626/Koenigswarte-Oesterreich-lauscht-bis-in-den-Nahen-Osten?dst=l.facebook.com.

Wiener Zeitung (2013), spies like us (*Spione wie wir*), available at: www.wienerzeitung.at/nachrichten/oesterreich/politik/587681_Spione-wie-wir.html.

Zankl, W. (2009), On the way to a surveillance – state?, new surveillance measures in the area of information and communication technology (*Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie*, Facultas – WUV.