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

POLAND

Version 1 October 2014

Helsinki Foundation for Human Rights
Dorota Głowacka
Adam Ploszka

Summary

I. Legal framework

I.A Surveillance bodies, legal basis, material and territorial scope of surveillance

[1]. There are several intelligence services in Poland that have competences with regard to surveillance of communication of all individuals that fall within Polish jurisdiction on the Polish territory. These are Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne*), Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrzego*), Border Guard (*Straż Graniczna*), Military Counter-Intelligence Service (*Służba Kontrwywiadu Wojskowego*), Military Police (*Żandarmeria Wojskowa*), Treasury Control (*Kontrola Skarbowa*) and Customs Service (*Służba Celna)*[1]. Additionally, the Police (*Policja*) also has certain competences in this respect within its investigative and operational actions.

[2]. The legal basis and conditions under which intelligence services can conduct surveillance and the purposes of surveillance are defined in a number of legislative acts defining the powers of relevant institutions, such as the Act on Central Anti-Corruption Bureau[2], Act on Internal Security Agency and Foreign Intelligence Agency[3], Act on Military Counter-Intelligence Service and Military Intelligence Service[4], Act on the Border Guard[5], Act on Customs Service[6], Act on Military Police and Military Law Enforcement Agencies[7], Act on Treasury Control[8] and Act on the Police[9]. The surveillance can be carried out for the purposes of recognition, prevention and control of threats affecting the national security of the state and its constitutional order, in particular sovereignty and international standing, independence and integrity of its territory, and national defence. Moreover, it can be carried out for crime prevention and investigation purposes (in the case of particular intelligence services, it may be limited to certain types of crimes that fall within the competences of a given institution, including espionage, terrorism, crimes affecting economic interests of the State, corruption crimes, tax offences, border and migration crimes, illegal arms trafficking etc.). Surveillance carried out

[1] Military Intelligence Service and Foreign Intelligence Agency also have competences regarding the communication surveillance, but limited only to the operating surveillance (intercepting content of communication). Moreover, on the Polish territory they can conduct the surveillance only indirectly, via the Counter-Intelligence Military Service and the Internal Security Agency (when it comes to MIS) or via the Internal Security Agency (FIA).

[2] Poland, Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym*), 9 June 2006.

[3] Poland, Act on Internal Security Agency and Foreign Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), 24 May 2002.

[4] Poland, Act on Military Counter-intelligence Service and Military Intelligence Service (*Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*), 9 June 2006.

[5] Poland, Act on the Border Guard (*Ustawa o Straży Granicznej*), 12 October 1990.

[6] Poland, Act on Customs Service (*Ustawa o Służbie Celnej*), 27 August 2009.

[7] Poland, Act on Military Police and Military Law Enforcement Agencies (*Ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych*), 24 August 2001.

[8] Poland, Act on Treasury Control (*Ustawa o kontroli skarbowej*), 28 September 1991.

[9] Poland, Act on the Police (*Ustawa o policji*), 6 September 1990.

by particular intelligence services must always be related to the tasks that fall within their specific competences prescribed in the above-mentioned legislative acts[10].

[3]. The surveillance of communication can be conducted by intelligence services in Poland through:

1) interception of the content of communication within operating surveillance (for example wiretapping)[11];
2) accessing telecommunications data (traffic and location data) stored by telecom providers and Internet service providers (ISPs)[12].

[4]. Interception of the content of communication in the case of intelligence services can be ordered within criminal proceedings (in a non-procedural manner). It is limited in time (it can be ordered only for a specific period) and is always subject to judicial control (requires *ex ante* or, exceptionally, *ex post* judicial warrant). In general, these regulations do not allow for mass surveillance, as telecom providers cannot retain the content of communication indiscriminately and on a regular basis. For these reasons, the question of interception of the content of communication has not been elaborated on in this report.

[5]. Unlike data which includes the content of communication, telecommunication data which do not reveal the content of communication are stored in an indiscriminate, blanket manner by private sector telecom providers and Internet service providers (such as hosting operators). The intelligence services have broad access to these data with very few limitations, which poses a risk of mass surveillance of communication and will be presented in the following parts of the report.

[6]. Access to telecommunication data stored by telecom providers (*przedsiębiorca telekomunikacyjny*[13]) is possible on the grounds of the Telecommunications Law[14] in conjunction with particular legislative acts concerning relevant intelligence services listed

[10] Articles 17-18 of the Act on Central Anti-Corruption Bureau; Articles 27-28 of the Act on Internal Security Agency and Foreign Intelligence Agency; Articles 31-32 of the Act on Military Counter-intelligence Service and Military Intelligence Service; Articles 9e and 10b of the Act on Border Guard; Article 75d of the Act on Customs Service; Article 30-31 of the Act on Military Police and Military Law Enforcement Agencies; Article 36b - 36c of the Act on Treasury Control; Article 19 and 20c of the Act on the Police.

[11] Article 17 of the Act on Central Anti-Corruption Bureau; Article 27 of the Act on Internal Security Agency and Foreign Intelligence Agency; Article 31 of the Act on Military Counter-intelligence Service and Military Intelligence Service; Article 9 e of the Act on Border Guard; Article 31 of the Act on Military Police and Military Law Enforcement Agencies; Article 36c of the Act on Treasury Control; Article 19 of the Act on the Police.

[12] Article 18 of the Act on Central Anti-Corruption Bureau; Article 28 of the Act on Internal Security Agency and Foreign Intelligence Agency; Article 32 of the Act on Military Counter-intelligence Service and Military Intelligence Service; Article 10b of the Act on Border Guard; Article 75d of the Act on Customs Service; Article 30 of the Act on Military Police and Military Law Enforcement Agencies; Article 36b of the Act on Treasury Control; Article 20c of the Act on the Police.

[13] The definition of 'telecom providers' is prescribed in Article 2. 27 of the Telecommunications Law. Telecom providers provide access to telephone, internet and related communications networks. Their activities are governed by the Telecommunications Law.

[14] Poland, Telecommunications Law (*Prawo telekomunikacyjne*), 16 July 2004.

above in paragraph 2 (and references no. 2-9), which provide detailed regulations (these regulations transpose the EU Data Retention Directive[15] to the domestic legal order). Telecommunication data have to be mandatorily stored by telecom providers for 12 months from the date of communication. Access to the data stored by ISPs (*usługodawca świadczący usługi drogą elektroniczną[16]*), including especially hosting operators, is possible on the grounds of the Act on providing electronic services[17] (APES). This Act imposes on all ISPs the obligation to "disclose information on the processed data to government authorities for the purposes of proceedings conducted by them" (Article 18 paragraph 6). However, there is no legal obligation under APES for ISPs to store the data for any specific period.

I.B Oversight bodies

[7]. There are no oversight bodies which specifically exert control over mass surveillance of communication. There are only oversight bodies which control the general activity of intelligence services, sometimes in a non-binding way (i.e. they have only advisory competences with regard to their current actions, future policies or draft law proposals concerning their competences and cannot question particular activities or impose any sanctions). There are governmental oversight institutions, such as the Prime Minister (*Prezes Rady Ministów*) and Collegium for Intelligence Services (*Kolegium do Spraw Służb Specjalnych*), as well as a parliamentary oversight body – the Parliamentary Commission for Intelligence Services (*Sejmowa Komisja ds. Służb Specjalnych*). The Prime Minister has a general competence of supervision of the functioning of intelligence services, determining their objectives (for example by accepting the annual action plan for the upcoming year in the case of Central Anti-Corruption Bureau[18]) as well as appointing and dismissing their heads. The Prime Minister has the most far-reaching competences with regard to the oversight of intelligence services out of all oversight institutions, but – as shown by the latest report of the Supreme Audit Office – in practice his oversight lacks efficacy[19]. The Collegium is an advisory body with non-binding competences, supporting the Prime Minister in matters of programming, monitoring and coordination of intelligence services. The Parliamentary Commission provides, in particular, opinions on draft law proposals concerning intelligence

[15] European Commission (2011), *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225 final, Brussels, 18 April 2011, available at: http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf.

[16] For the purposes of this report, the term 'ISPs' refers to the 'entities that provide electronic services' defined in Article 2.6 of the Act on providing electronic services (which is based on the so called EU's E-commerce Directive). These companies do not provide access to the communications networks, but offer online services, such as hosting or searching. Their activities are governed by the Act on providing electronic services.

[17] Poland, Act on providing the electronic services (*Ustawa z dnia 18 lipca 2002 oświadczeniu usług drogą elektroniczną*), 18 July 2002.

[18] Article 12 of the Act on Anti-Corruption Bureau.

[19] This is the main conclusion from the Supreme Audit Office's report which was revealed to the public opinion. The full content of the report is secret. See: Poland, Supreme Audit Office (*Naczelna Izba Kontroli*) (2014), Nadzór nad służbami specjalnymi, Press release, 26 August 2014, available at: www.nik.gov.pl/aktualnosci/nadzor-nad-sluzbami-specjalnymi.html (accessed on 9 September 2014).

services and evaluates proposals for the appointment and dismissal of individual persons as heads of these services. The activities of the intelligence services can also be subject to control by the general national audit institution (Supreme Audit Office, *Najwyższa Izba Kontroli*). The roles and competences of particular institutions with respect to intelligence services are described in detail in Annex 2.

[8]. The only tool that can be used in order to control the way the data retention regime operates specifically is the reporting obligation imposed on telecom providers. Telecom providers have to annually report the total number of requests received from institutions entitled to use the retained data to the Office for Electronic Communications (*Urząd Komunikacji Elektronicznej*). According to the statistics provided by the OEC in 2014, there were 1.75 mln such requests in 2013[20] (same number as in 2012[21]). According to the statistics from previous years, the number of requests was rising from 2009 (1 million requests) up to 2011 (1.85 million requests). Since 2012, the number of requests has slightly decreased to 1.75 (which is 100,000 fewer than in 2011, but still 750,000 more than in 2009 when the European Commission placed Poland at the very top of the list of European countries using data retention[22]). The data published by OEC do not indicate, however, how often and for what purposes the data were accessed by particular institutions, making it impossible to fully assess the use of this measure.

I.C Ongoing legislative reforms

[9]. The current legal framework and practice of intelligence services with regard to the use of telecommunication data has been criticized by Polish human rights NGOs and other bodies, such as the Human Rights Defender[23] (*Rzecznik Praw Obywatelskich*), who is *inter alia* authorized to apply for a constitutional review of legislative acts and participate in the

[20]Poland, Office of Electronic Communications (*Urząd Komunikacji Elektronicznej*) (2013), 'Udostępnianie danych telekomunikacyjnych w 2012 r.', Press release, 14 March 2014, available at: http://www.uke.gov.pl/informacja-o-rocznym-sprawozdaniu-dotyczacym-udostepniania-danych-telekomunikacyjnych-13495.

[21]Poland, Office of Electronic Communications (*Urząd Komunikacji Elektronicznej*) (2013), 'Udostępnianie danych telekomunikacyjnych w 2012 r.', Press release, 2 April 2013, available at: www.uke.gov.pl/udostepnianie-danych-telekomunikacyjnych-w-2012-roku-12248.

[22] European Commission (2011), *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM(2011) 225 final, Brussels, 18 April 2011, available at: http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf.

[23] Poland, Human Rights Defender (*Rzecznik Praw Obywatelskich*), Wniosek do Trybunału Konstytucyjnego, RPO-662587-II-ll/ST, 1 August 2012.

proceedings before the Constitutional Court[24], the Supreme Bar Council[25] (*Naczelna Rada Adwokacka*), Prosecutor General[26] (*Prokurator Generalny*) or the Supreme Audit Office[27] (*Najwyższa Izba Kontroli*). Despite many government declarations made in the last 3 years to restrict the extensive powers of intelligence services with regard to data retention, there have not been any significant developments or legislative changes enforced in this respect. The only improvement has so far included a legislative amendment to the Telecommunication Law which reduced the data retention period from 24 months to 12 months and imposed a prohibition on the use of data retention in the course of civil proceedings (the amendment entered into force on 31 January 2013).[28] The last legislative proposal from the Ministry of Interior,[29] aiming at restricting access and use of data retention, was subject to another round of public consultations in 2013, but has still not been referred to the Parliament for further legislative works. At the moment, there are 2 draft law proposals pending focused on increasing the control over the conduct of intelligence services. First of all, there is a Senate proposal for draft law amending, specifically, the regulations concerning access of public authorities to telecommunication data retained by telecom providers.[30]The draft law proposal includes in particular: (1) imposing the obligation on the intelligence services to obtain consent from the court to acquire telecommunication data in accordance with a procedure which is currently applicable to the operating surveillance (that allows *inter alia* wiretapping); the court's consent would not be mandatory only with regard to the data concerning the identity of subscribers; (2) introduction of a closed catalogue of offenses in case of which intelligence services would be authorized to use the data retention regime; (3) obligation to destroy the collected data which are no longer necessary for the criminal proceedings purposes; (4)

[24] Other main competences of the Human Rights Defender include: 1) examination of individual complaints and, in case citizen rights or freedoms have been infringed, HRD may refer the request to the competent authority, organisation or institution whose actions led to the infringement, or to a superior authority to ensure redress for the infringement; HRD then monitors the implementation of the recommended actions; 2) lodging a last resort appeal with the Supreme Court and Supreme Administrative Court; 3) presenting advisory opinions on draft laws. Legal basis: Articles 191.1 and 208-212 of the Polish Constitution and the Act on the Human Right Defender (*Ustawa o Rzeczniku Praw Obywatelskich*), 15 July 1987. The Human Rights Defender is an A-status institution according to the Paris Principles. It is a high prestige constitutional body.

[25] Poland, Supreme Bar Council, Conference entitled Data Retention: attention of security or surveillance of citizens? Polish citizen- the most controlled citizen of Europe.(*Konferencja pt. Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli? Polak najbardziej inwigilowanym obywatelem Europy?*) 6 May 2011, available at: http://archiwum.adwokatura.pl/?p=3396.

[26] Poland, Prosecutor General (*Prokurator Generalny*), PG VII TK 62/11, 28 October 2011.

[27] Poland, Supreme Audit Office (*Naczelna Izba Kontroli*), 'Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne', Report, 8 October 2013.

[28] Poland, the Act amending the Act on telecommunication law and certain other acts (*Ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*), 16 November 2012.

[29] Poland, Ministry of Interior (*Ministerstwo Spraw Wewnętrznych)*, The draft Project onThe Draft Act amending the certain other acts on obtaining and processing telecommunications data, (*Projekt założeń projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych)*, 28 May 2012, available at: bip.kprm.gov.pl/portal/kpr/46/1889/Projekt_zalozen_projektu_ustawy_o_zmianie_niektorych_ustaw_w_zwiazku_z_pozyskiwa.html

[30] Poland, Senate, the Draft Act amending the certain other acts on obtaining and processing telecommunications data by authorized entities, (*Ustawa o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjncyh),* December 2012.

obligation to provide statistical data by every intelligence service in an uniform manner; (5) establishing internal agents for the control of processing personal data within every intelligence service (currently such agent operates only in the Central Anti-Corruption Bureau).This proposal is at the very initial stage of the legislative procedure though (still labelled as a working document). Secondly, there is a governmental draft law proposal for establishing a Commission for the control of intelligence services[31] (improving general oversight of the activities of intelligence services). This draft law proposal has not yet been adopted by the Council of Ministers.

[10]. Most probably, the real breakthrough for the legislative process will only be brought by the Polish Constitutional Court's judgment which was delivered in July 2014.[32] The Court challenged some of the regulations concerning the grounds for operating surveillance (allowing *inter alia* wiretapping) as well as, to some extent, the current data retention regulations. The Court found the latter to be incompatible with the constitutional right to privacy, including the information autonomy rights and correspondence secrecy (the judgment is described in more detail in Annex 4). The ruling, however, will become effective in 18 months from the publication of the judgment. After that period, the current provisions will expire. Before this expiry date, new regulations will have to be adopted which will implement the Court's guidelines (the Court did not go as far in its critical approach towards the current regulations as CJEU in the "Digital Rights Ireland" ruling. The Polish Court focused mainly on one element, namely the lack of independent oversight with regard to the use of data retention regime by intelligence services). The Ministry of Interior already announced that a new draft law proposal should be prepared within the next 12 months.[33] One can, therefore, expect in the upcoming months an intense public debate and legislative works on the data retention regulation reform in Poland.

II. Safeguards protecting the right to privacy

[11]. Although the Polish Constitution grants the right to privacy, secrecy of communication and informational autonomy (Articles 47, 49, 51), the Polish legal order lacks adequate safeguards against abusing the competences of intelligence agencies with regard to mass surveillance of communication.

[12]. As regards the use of data stored by telecom providers, the (now invalidated) law does not provide for judicial or any other independent, external control (neither *ex post* nor *ex ante*) over the access and use of such data. The surveillance is possible for a broad range of purposes of performing any statutory duties of particular intelligence services (there is no legal

[31] Poland, Ministry of Interior (*Ministerstwo Spraw Wewnętrznych*), the Draft Act on Commission for the control of intelligence services, (*Projekt ustawy o Komisji Kontroli Służb Specjalnych*), 11 October 2011.

[32] Poland, Constitutional Court (*Trybunał Konstytucyjny*), Judgment of 30 July 2014, K 23/11, available at: http://trybunal.gov.pl/rozprawy/wyroki/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/, (accessed on 18 August 2014).

[33] Poland, Polish Press Agency (*Polska Agencja Prasowa*), Minister of Interior Bartłomiej Sienkieiwcz: two expert teams analyse the Constitutional Court's ruling (*Szef MSW Bartłomiej Sienkiewicz: dwa zespoły analizują wyrok TK ws. Zasad inwigilacji*), available at: http://wiadomosci.wp.pl/kat,1342,title,Szef-MSW-Bartlomiej-Sienkiewicz-dwa-zespoly-analizuja-wyrok-TK-ws-zasad-inwigilacji,wid,16791240,wiadomosc.html?ticaid=113388&_ticrsn=3, 31 July 2014, (accessed on 7 August 2014).

threshold for seriousness of a crime). There is no requirement to notify the person whose data were acquired (even once the proceedings are completed). A data subject's right to access is denied as well, though in a judicial proceeding, a party to the proceeding whose data were collected and made available to Police, has the right to access such data as they become part of the evidence.

[13]. Only in the case of some of the intelligent services (Police, Military Police, Border Guard, Customs Service), there is a specific obligation to destroy data once they are no longer needed for the purpose for which they have been acquired. Moreover, the data retention regulations do not include any specific provisions preventing violations of the guarantees protecting professional secrecy rules (such as journalistic shield laws or legal professional privilege). Intelligence services access telecommunication data at no cost (all costs generated by the data retention regime are covered by telecom providers) and often directly, through simple interfaces established on telecommunication networks. Access to telecommunication data by Police via a telecommunication network can take place only if the telecommunication network provides the possibility to determine the person obtaining the data, type of data and the time in which they were obtained (art. 20c par. 5 point 1 letter a) of the Act on the Police).

[14]. Similar problems arise with regard to the use of data stored by ISPs. Article 18 paragraph 6 of APES causes certain interpretation problems (the law does not precisely specify which "government authorities" can access data, what are the elements which a data request should contain or who should bear the cost of such a disclosure). There are no safeguards preventing arbitrary acquisition of data either – there is no independent oversight of acquiring the data by intelligence services (no need for a judicial warrant) and no obligation to inform the data subject concerned.

III. Legal remedies

[15]. Individuals have very limited possibilities to use legal remedies in case of an abuse of powers of intelligence services with regard to the use of telecommunication data stored by telecom providers or ISPs. The intelligence services may in general collect and process personal data without the knowledge or consent of the data subjects[34]. Since there is no external oversight and no notification obligation, it is difficult to question the conduct of intelligence services, as individuals most often never find out about the fact that their telecommunication data were acquired (and in order to be able to challenge the surveillance, the individual must have concrete evidence to substantiate the probability of surveillance). There are no specific legal remedies prescribed by law against arbitrary surveillance. If an individual somehow finds out that their data were unlawfully acquired, they may only rely on general civil law measures, such as a lawsuit for the protection of personal rights[35] or general criminal law measures

[34]Article 22.1 of the Act on Central Anti-Corruption Bureau; Article 34.1 of the Act on Internal Security Agency and Foreign Intelligence Agency; Article 31.8 of the Act on Military Counter-intelligence Service and Military Intelligence Service Act; Article 9.1a of the Act on Border Guard; Article 7.1 of the Act on Customs Service; Article 29.6 of the Act on Military Police and Military Law Enforcement Agencies; Article 36f.2 of the Act on Treasury Control; Article 20.2 of the Act on the Police.

[35] Poland, Civil Code (*Kodeks Cywilny*), 23 April 1964, Article 23-24.

described in detail in Annex 3 (misconduct of a public official[36] or data protection offences listed in Data Protection Act[37]). It needs to be highlighted that intelligence services fall outside the cognition of the Polish Data Protection Authority (General Inspector for Personal Data Protection, *Generalny Inspektor Ochrony Danych Osobowych*). Its inspection powers under the Data Protection Act[38] are explicitly excluded with regard to personal data processed by these institutions.[39] Therefore, the regular administrative law redress mechanisms in case of data protection breaches are not available to data subjects in the case of the use of data retention by intelligence services.

[36] Poland, Criminal Code (Kodeks Karny), 6 June 1997, Article 231.
[37] Poland, Data Protection Act (Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych),29 August 1997,Articles 49-54a.
[38] Poland, Data Protection Act (*Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych*), 29 August 1997.
[39] Poland, Data Protection Act *(Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych*), 29 August 1997, Article 43 (2).

Version of 1 October 2014

Annex 1 – Legal Framework relating to mass surveillance

A. Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Telecommunications Law (*Prawo telekomunikacyjne*) 16 July 2004 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	Articles 180a, 180c and 180d constitute general legal basis obliging telecom providers to collect and retain telecommunications data (such as traffic and location data, but without the content of communication) and make them accessible at the request of intelligence agencies for their statutory purposes. Specific regulations with regard to the access of particular institutions to these data are included in different legal acts concerning their activity (described below).			Collecting data, storing data, destroying data	Based on Article 180a. 1 of Telecommunications Law, telecom providers operating in Poland are obliged to collect data generated in a communications network on the Polish territory for a period of 12 months.	There is no specific law allowing for mass surveillance in another country.

Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym*) (CBA) 9 June 2006 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	The circumstances that may give rise to surveillance are listed in Article 2 of the Act on Anti-Corruption Bureau which contains a number of specific crimes that fall within the CBA's competences and are associated with identification, prevention and detection of corruption.	Combating corruption and protecting the economic interests of the State	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a written request from the Head of the CBA or from a person authorized by the Head of the CBA; 2) at an oral request from a CBA agent having written authorization of the Head of the CBA or of a person authorized by the Head ofthe CBA; 3) remotely, via a telecommunications network, at the request of a CBA agent possessing written authorization referred to in point 1.	Acquiring data from telecom providers, analyzing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				To ensure the safety of transmitted data, telecommunications network must comply with the statutory requirements. Transfer of data takes place without the involvement of employees of telecom providers.			
Act on Internal Security Agency and Foreign Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*) 24 May 2002 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	Article 28 in connection with Article 5 of the Act states that the legitimate grounds for surveillance conducted only by the Internal Security Agency include: 1) recognition, prevention and control of threats affecting the internal security of the state and its constitutional order, in particular sovereignty and	Combating internal threats to national defence	There is no need to receive a judicial warrant. Telecom providers provide data at a official request submitted in one of three procedures: 1) at a request of an Internal Security Agency's officer designated in a written request of the Head of the Internal Security Agency, or a person authorized by the competent authority;	Acquiring data from telecom providers, analyzing data, storing data, destroying data,	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

		international standing, independence and integrity of its territory, and national defence 2) identification, prevention and detection of selected crimes: espionage, terrorism, unauthorized disclosure or use of classified information and other crimes affecting the security of the state, crimes affecting the state's economics, corruption crimes or illegal arms trafficking; 3) protection of classified information; 4) obtaining, analyzing, processing and		2) at an oral request of an agent of the Internal Security Agency having written authorization of the Head of the Internal Security Agency; 3) remotely, via a telecommunication s network, at the request of an Internal Security Agency's agent who holds an authorization referred to in point 2. To ensure the safety of transmitted data, telecommunication s network must comply with the statutory requirements. Transfer of data takes place without the involvement of the employees of telecom providers.			

		disseminating to competent authorities the information that may be relevant to the internal security of the state and its constitutional order; 5) taking other actions specified in separate laws and international agreements.					
Act on Military Counter-intelligence Service and Military Intelligence Service (*Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego)* 9 June 2006 – Act of Parliament	These intelligence services are concentrated on soldiers serving on active duty, military officers of the Military Counter-intelligence Service and Military Intelligence Service and employees of the Polish Armed Forces	Article 32 in connection with Article 5 of the Act states that the legitimate grounds for surveillance conducted by the Military Counter-intelligence Service include: identification, prevention and detection of offenses committed by soldiers serving on active duty,	Public order, public safety (crime investigation)	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a written request of the Head of the Military Counter-intelligence Service or a person authorized by the Head of the	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

	and other organizational units of the Ministry of National Defence. These categories of soldiers and any users of telecommunications services who are associated with cases investigated by those institutions could be subject to such surveillance.	military officers, officers of the Military Counter-intelligence Service and officers of the Military Intelligence Service, and employees of the Polish Armed Forces and other organizational units of the Ministry of National Defence. These offences are described in: 1) Chapter XVI of the Polish Criminal Code; 2) Chapter XVII of the Polish Criminal Code; 3) Chapter XXXIII of the Polish Criminal Code;		Military Counter-intelligence Service; 2) at an oral request from the Military Counter-intelligence Service agent having written authorization of the Head of the Military Counter-intelligence Service; 3) remotely, via a telecommunications network, at the request of the Military Counter-intelligence Service agent possessing written authorization referred to in point 1. To ensure the safety of transmitted data, telecommunications network must comply with the statutory			

		4) Article 140 and 228-230 of the Polish Criminal Code; 5) crimes associated with terrorist activity and other than those listed above which affect the security of the country's defence potential, the armed forces and defence organizational units, as well as countries which provide mutuality; 6) offences which are referred to in Article 33 paragraphs 1, 2 and 3 of the Act of 29 November 2000 on foreign trade in goods, technologies and services of strategic importance for national security		requirements. Transfer of data takes place without the involvement of the employees of telecom providers.			

		and the maintenance of international peace and security					
Act on the Border Guard (*Ustawa o Straży Granicznej*) 12 October 1990 – Act of Parliament	All users of telecommunications services provided by telecommunications operators in Poland	The Act states in Article 10b that the legitimate ground for surveillance is to prevent or detect crimes which are within the cognition of the Border Guard (especially concerning crossing the border).	Border protection, prevention of illegal immigration	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a written request of the Commander Chief of the Border Guard, or the division commander of the Border Guard, or the person authorized by them; 2) at an oral request of an agent holding a written authorization of the persons referred to in point 1; 3) remotely, via a telecommunication	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				s network, at a request of an agent possessing written authorization of the persons referred to in point 1. To ensure the safety of transmitted data, telecommunication s network must comply with the statutory requirements. Transfer of data takes place without the involvement of the employees of telecom providers.			
Act on Customs Service (*Ustawa o Służbie Celnej*) 27 August 2009 – Act of Parliament	All users of telecommunica tions services provided by telecom providers in Poland	The Act states in Article 75d that the legitimate ground for surveillance is to prevent or detect tax offences which are described in Section 9 of the Tax Criminal Code.	Public order, public safety.	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a request of an agent designated in a written request of the Head of the Customs Service or	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				the Director of the Customs Chamber or a person authorized by them; 2) at an oral request of an agent holding a written authorization of the persons referred to in point 1; 3) remotely, via a telecommunications network, at a request of an agent possessing written authorization of persons referred to in point 1. To ensure the safety of transmitted data, telecommunications network must comply with the statutory requirements. Transfer of data takes place without the involvement of the employees of telecom providers.			

Act on Military Police and Military Law Enforcement Agencies (*Ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych*) 24 August 2001 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	The Act states in Article 30 that the legitimate ground for surveillance is to prevent or detect crime, including tax offences.	Public order, public safety (crime investigation)	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a request of Military Police soldier designated in a written request of the Commander in Chief of the Military Police or the division commander of the Military Police or a person authorized by them; 2) at an oral request of the Military Police soldier holding a written authorization of the persons referred to in point 1; 3) remotely, via the telecommunications network, at a request of the Military Police	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				soldier who holds a written authorization of the persons referred to in point 1. To ensure the safety of transmitted data, telecommunications network must comply with the statutory requirements. Transfer of data takes place without the involvement of the employees of telecom providers.			
Act on the Police (*Ustawa o policji*) 6 September 1990 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	The Act states in Article 20c that the legitimate ground for a non-procedural surveillance is to prevent or detect crimes that fall within the competences of the police.	Public order, public safety (crime investigation)	There is no need to receive a judicial warrant. Telecom provider provides data at an official request submitted in one of three procedures: 1) at a request of a police officer designated in a written request of the Chief of Police or voivodeship	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				commander of Police or a person authorized by them; 2) at an oral request from a police officer holding a written authorization of the persons referred to in point 1; 3) remotely, via a telecommunications network, at a request of a police officer possessing a written authorization referred to in paragraph 1. To ensure the safety of transmitted data, telecommunications network must comply with the statutory requirements. Transfer of data takes place without the involvement of			

				the employees of telecom providers.			
Act on Treasury Control (*Ustawa o kontroli skarbowej*) 28 September 1991 – Act of Parliament	All users of telecommunications services provided by telecom providers in Poland	The Act states in Article 36b that the legitimate ground for surveillance is to prevent or detect tax offences.	Economic well-being, tax collection	There is no need to receive a judicial warrant. Telecom providers provide data at an official request submitted in one of three procedures: 1) at a written request of the General Inspector of Treasury Control; 2) at a written request of an employee of the tax intelligence service having a written authorization from the General Inspector of Treasury Control to act on his behalf and access data referred to in paragraph 1;	Acquiring data from telecom providers, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the amount of data flow caught.	There is no specific law allowing for mass surveillance in another country.

				3) remotely, via a telecommunications network, at a request of an employee of the tax intelligence service possessing a written authorization referred to in paragraph 2. To ensure the safety of transmitted data, telecommunications network must comply with the statutory requirements. Transfer of data takes place without the involvement of employees of telecom providers.			
Act on Providing Electronic Services (*Ustawa o świadczeniu usług drogą elektroniczną*) 18 July 2002	All users of telecommunications services provided by Internet Service Providers in Poland	Article 18 paragraph 6 of the Act imposes an obligation for Internet Services Providers (ISPs) (such as hosting operators or search engine operators) to "disclose information on the processed data to government authorities for the purposes of proceedings conducted by them." Based on this Act intelligence services have access to these data for their statutory purposes without any judicial warrant. The Act on			Collecting data, analysing data, storing data, destroying data	There are no limitations in terms of nationality, national borders, time limits, or the	There is no specific law allowing for mass surveillance in another country.

– Act of Parliament		Providing Electronic Services does not, however, impose a data retention obligation on ISPs for any specific period.		amount of data flow caught. The intelligence services can acquire data only from ISPs which are in the Polish jurisdiction. There are no specific regulations on acquiring data from an ISP which operates in Poland but does not have a legal entity or a representation in Poland.	

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*
Constitution of the Republic of Poland (*Konstytucja Rzeczpospolitej Polskiej*) 2 April 1997 These provisions provide a general framework for all laws concerning the fundamental right to privacy of communication, and the limitation of powers with regard to collection of individuals' data by public authorities. Article 47 states that: "Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life."	Right to privacy, secrecy of communications, informational autonomy	These rights apply to everyone who is under Polish jurisdiction. In other words, they also apply to, other than Polish, EUcitizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.

Article 49 states that: "The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute." Article 51 paragraph 2 states that: "Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law."			
Criminal Code (*Kodeks Karny*) 6 June 1997 Article 231 of the Criminal Code provides a general right to challenge the situation where the public official exceeds his authority or neglects his duties which should be treated as an offence	Right to challenge situation where the public official exceeds his authority or neglects his duties.	This right applies to everyone who is under Polish jurisdiction. In other words, it also applies to, other than Polish, EU citizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.

(in this case – an agent of intelligence services who might be accused of exceeding his competences in the case of unlawful acquisition of telecommunication data). There are no specific provisions in Polish criminal law concerning the right to challenge the legality of mass surveliance conducted by intelligence services. Article 231of the Criminal Code states that: “A public official who, exceeding his authority or not performing his duty, acts to the detriment of a public or individual interest shall be subject to the penalty of deprivation of liberty for up to 3 years.”			

Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym*) This act states that the Central Anti-Corruption Bureau can process personal data for the period in which they are required to perform its statutory duties. The Central Anti-Corruption Bureau is obliged to verify all stored personal data, and the necessity of their further processing at least every five years. After this process, the Central Anti-Corruption Bureau shall remove all the unnecessary personal data (Article 22a paragraph 8). After such verification, a commission appointed by the Head of the Central Anti-Corruption Bureau immediately removes the unnecessary personal data. The whole operation shall be minuted, including in particular a list of deleted data and the method of their deletion (Article 22a paragraph 9). These provisions apply only to processing of personal data. There are no secific provisions concerning telecommunication data obtained from telecom providers on the basis of Article 180c and 180 d of the Telecommunications Law. However, since some of the telecommunication data can be considered personal data – the above provisions may be, to a certain extent, relevant in terms of safeguards against mass-surveillance.	Obligation to delete personal data	These rights apply to everyone who is under Polish jurisdiction. In other words, they also apply to, other than Polish, EU citizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.
Act on Military Police and Military Law Enforcement Agencies (*Ustawa o Żandarmerii Wojskowej i wojskowych organach porządkowych*) 24 August 2001	Obligation to delete telecommunication data Obligation to delete personal data	These rights apply to everyone who is under Polish jurisdiction. In other words, they also apply to, other than Polish, EU citizens and third country	These rights apply only within Polish jurisdiction.

Data obtained on the basis of Articles 180c and 180d of the Telecommunications Law (telecommunication data) which do not contain information relevant to the proceedings related to criminal offences shall be immediately destroyed under commission supervision. The whole procedure shall be minuted (Article 30 paragraph 6). More generally, personal data collected by the Military Police can be stored for the period necessary to comply with its statutory duties. The Military Police and Military Law Enforcement Agencies shall review these data at least every 10 years from the date of obtaining the data (Article 29).		nationals whenever they are within Polish jurisdiction.	
Act on Border Guard (*Ustawa o Straży Granicznej*) 12 October 1990 The data obtained from telecom providers on the basis of Article 180c and 180d of the Telecommunications Law (telecommunication data) which do not contain information relevant to the proceedings related to criminal offences shall be immediately destroyed under a supervision of a competent commission. The whole procedure shall be minuted (Article 10b paragraph 6). More generally, personal data collected by the Border Guard can be stored for the period necessary to comply with its statutory duties. The Border Guard shall review these data at least every 10 years from the date of obtaining the data (Article10a paragraph 3).	Obligation to delete telecommunication data Obligation to delete personal data	These rights apply to everyone who is under Polish jurisdiction. In other words they also apply to, other than Polish, EU citizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.

Act on Customs Service (*Ustawa o Służbie Celnej*) 27 August 2009. "Data obtained as a result of actions based on Article 180c and 180d of the Telecommunication Law which do not contain information relevant to the proceedings related to tax offenses shall be immediately destroyed under commission supervision. The whole procedure shall be minuted." (Article 75d paragraph 5) More generally, personal data collected by the Customs Service can be stored for the period necessary to comply with its statutory duties. The Customs Service shall review these data at least every 10 years from the date of obtaining the data (Article 7 paragraph 12).	Obligation to delete telecommunication data	These rights apply to everyone who is under Polish jurisdiction. In other words they also apply to, other than Polish, EU citizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.
Act on the Police (*Ustawa o policji*) 6 September 1990 "Data obtained as a result of actions based on Article 180c and 180d of the Telecommunication Law which do not contain information relevant to criminal proceedings shall be immediately destroyed under commission supervision. The whole procedure will be minuted." (Article 20c paragraph 7). More generally, personal data collected by the Police can be stored for the period necessary to comply with its statutory duties. The Police shall review these data after closing each case and at least every 10 years from the date of obtaining the data (Article20 paragraph 17).	Obligation to delete telecommunication data	These rights apply to everyone who is under Polish jurisdiction. In other words they also apply to, other than Polish, EU citizens and third country nationals whenever they are within Polish jurisdiction.	These rights apply only within Polish jurisdiction.

Annex 2 – Oversight bodies and mechanisms

There are no oversight bodies which specifically exert control over mass surveillance of communication. There are only oversight bodies which control the general activity of intelligence services, not focused on surveillance of communication[40]. The main body with binding oversight competences with regard to intelligence services is the Prime Minister (its competences are described below).The Prime-Minister has the most far-reaching competences with regard to oversight of the intelligence services out of all oversight institutions, but – as shown by the latest report of the Supreme Audit Office issued on 26 August 2014 – in practice this oversight lacks efficacy (see report "Prime Minister supervision on special services"[41]). The current regulations limit the ability to exercise effective oversight of special services by the Prime Minister. The Prime Minister is also devoid of important supervisory tools e.g. full knowledge of the internal procedures used by intelligence services.

Other bodies have mostly non-binding competences with regard to the oversight of intelligence services (i.e. they have only advisory competences with regard to their current actions, future policies or draft law proposals concerning their competences and cannot question particular activities or impose any sanctions).

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Parliamentary Commission for Intelligence Services (*Sejmowa Komisja ds. Służb Specjalnych*) (KSS)	Parliamentary	Chapter 12 of the Resolution of the Polish Sejm on Polish Sejm Rules of Procedure (*Uchwała Sejmu Rzeczypospolitej Polskiej Regulamin*	*Ex ante* and *ex post*, also during the surveillance	9 members of the Polish Lower Chamber of Parliament (Sejm), elected in a special procedure described in Sejm Rules of Procedure. Chairperson of parliamentary clubs or groups of at least 35 MEPs can nominate each	The Commission does not have a direct power to monitor the process of mass surveillance, but it has a general competence with regard to the supervision of intelligence services. *Inter alia*, the Commission has the power to give opinions on draft laws,

[40] See also European Parliament's report; *Parliamentary Oversight of Security and Intelligence Agencies in The European Union*, available at: http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

[41] This is the main conclusion from the Supreme Audit Office's report which was revealed to the public opinion. The full content of the report is secret. Naczelna Izba Kontroli, (2014), Nadzór nad służbami specjalnymi, Press release, 26 August 2014, available at: www.nik.gov.pl/aktualnosci/nadzor-nad-sluzbami-specjalnymi.html.

		Sejmu Rzeczypospolitej Polskiej) 30 July 1992		candidate. Sejm, on a proposal from the Presidium of the Sejm submitted after consultations with the Convention of Elders, chooses the composition of the Commission in total voting. The Commission elects its bureau composed of the chairperson and two deputies. The President of the Commission and deputies perform their duties for six months, and then there is a recomposition of the bureau.	regulations, decrees and other normative acts concerning intelligence services. The Commission also examines the annual reports of the heads of intelligence services, evaluates the draft budgets in relation to intelligence services, considers the annual reports on their implementation and other financial information of the intelligence services, evaluates proposals for the appointment and dismissal of individual persons as heads of intelligence services and their deputies, familiarizes itself with information about intelligence services' particularly important activities, including suspicions of irregularities in the activities of the intelligence services and suspicions of breaches of law by those services.

Prime Minister (*Prezes Rady Ministrów*)	Executive	Article 33a paragraph 1, point 7 and 7a of the Act on Divisions of Government Administration (*Ustawa o działach administracji rządowej*) 4 September 1997	*Ex ante* and *ex post*, also during the surveillance	Elected by the majority of Sejm in a procedure decribed in the Polish Constitution.	As a head of executive power, the Prime Minister has a general competence of supervision of intelligence services. In particular, the Prime Minister appoints and dismisses heads of intelligence services. The Prime Minister does not have specific competences with regard to mass surveillance tools.
Collegium for Intelligence Services (*Kolegium do Spraw Służb Specjalnych*)	Executive	Chapter 2 of the Act on Internal Security Agency and Foreign Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*) 24 May 2002 Council of Ministers Regulation on detailed	*Ex ante* and*ex post*, also during the surveillance.	The Collegium is composed of 7 people: Six of them are members *ex officio*: -Prime Minister – Chairman - minister responsible for internal affairs, - minister responsible for foreign affairs, - minister responsible for national defence, - minister responsible for public finances, - Head of the National Security Bureau. One member of the Collegium – Secretary of the	Consultative and advisory body of the Council of Ministers in matters of programming, monitoring and coordination of intelligence services. Collegium does not have specific competences with regard to mass surveillance tools.

		procedures and rules of the Collegium for Intelligence Services and the range of activities of the Secretary of the Collegium (*Rozporządzenie Rady Ministrów w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakresu czynności sekretarza tego Kolegium*) 2 July 2002		Collegium – is appointed and dismissed by the Prime Minister.	
Agent for the control of personal data processing by the Central Anti-Corruption Bureau (CBA) (*Pełnomocnik do spraw kontroli przetwarzania przez*	Executive	Article 22b of the Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym*)	*Ex post*	Head of the CBA appoints the Agent for the control of personal data processing from among CBA officers.	Supervising the compliance of the processing of personal data collected by the CBA with the provisions of the CBA Act and the provisions of the Data Protection Act.

Centralne Biuro Antykorupcyjne danych osobowych)		9 June 2006			According to the Act, the Agent is entitled, in particular, to: 1) inspect any documents connected with performed control; 2) free admission to the premises and facilities controlled by CBA; 3) demand written explanations. In case of finding a violation of provisions by officers of CBA, the Agent may issue a written order to remove them. In case of finding a violation of the provisions of the Act on the Central Anti-Corruption Bureau and the provisions of the Act on Data Protection, the Agent takes action to clarify the circumstances of the breach, and immediately informs the Prime Minister and the Head of the CBA.

President of the Office of Electronic Communications (*Prezes Urzędu Komunikacji Elektronicznej*) (UKE)	Executive (internal regulatory authority)	Article 192 of the Act on Telecommunications Law (*Ustawa prawo telekomunikacyjne*) 16 July 2004	*Ex post*	President of UKE is appointed and dismissed by the Parliament with the consent of the Senate at the proposal of the Prime Minister. The term of office of the President of UKE is 5 years.	According to Article 180g, telecom providers are obliged to provide information to the President of UKE every year about: 1) the total number of requests from intelligence services based on Article 180c of Telecommunications Law; 2) the time elapsed between the date of retention of data and the date of submission by the intelligence services of the request for access to these data; 3) the total number of cases in which a request from intelligence services could not be realized.
Supreme Audit Office (*Najwyższa Izba Kontroli*)	*Supreme audit institution*	Articles 202-207 of the Constitution of the Republic of Poland (*Konstystucja Rzeczpospolitej Polskiej*) 2 April 1997	*Ex post*	The President of the Supreme Audit Office is appointed by the Sejm with the consent of the Senate for a period of 6 years, which may be extended for one more period only. Other staff of the Supreme Audit Office are civil servants.	The Supreme Audit Office has the power to audit the activity of government administration, e.g. intelligence services. The results of audits, conclusions and submissions taken by

					Supreme Audit Office are presented to the Sejm.
Human Rights Defender (*Rzecznik Praw Obywatelskich*)	*Ombudsman*	Article 191 paragraph 1.1. of the Constitution of the Republic of Poland *(Konstystucja Rzeczpospolitej Polskiej*) 2 April 1997 Article 16 paragraph 2.2 of the Act on the Human Rights Defender	*Ex post* and *ex ante*	Human Rights Defender is appointed by the Sejm with the consent of the Senate.	The Human Rights Defender does not have a direct power to monitor the process of mass surveillance, but it has a general competence to challenge the constitutionality of a normative act which poses a threat to fundamental right, also regarding mass surveillance. The Human Rights Defender is an A-status institution according to the Paris Principles. It is a constitutional body held in high regard.
Prosecution Office (*Prokuratura*)		Article 191 paragraph 1.1. of the Constitution of the Republic of Poland *Konstystucja Rzeczpospolitej Polskiej*) 2 April 1997	*Ex post* and *ex ante*	The Prosecutor General is appointed by the President of the Republic of Poland from among the candidates nominated by the National Judicial Council and the National Council of Public Prosecution.	The Prosecutor General does not have a direct power to monitor the process of mass surveillance, but it has a general competence to challenge the constitutionality of a normative act .

		Article 17 of the Act on the Prosecution Office (*Ustawa o prokuraturze*) 20 June 1985 r.			

Annex 3 – Remedies

There is no specific procedure, concerning remedial actions that can be taken in response to mass surveillance at each stage of the surveillance process. There are, however, three possible ways to challenge the legality of mass surveillance, if a person finds out that his/her data were unlawfully acquired. Intelligence services are not obliged to inform individuals about the fact that they were subject to surveillance. Individuals do not have access to data acquired by intelligence services either.

Civil Code – protection of personal rights				
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**
Collection **Analysis*** **Storing*** **Destruction*** **After the whole surveillance process has ended**	*n/a*	*n/a*	Individuals may file a lawsuit with a regional civil court (*sąd okręgowy*) claiming that intelligence services breached personal rights of the plaintiff. The concept of personal rights in Poland encompasses privacy. Under article 24 of the Civil Code, the legislator allowed for several kinds of remedies in the event of personal rights violation. The claimant may seek the removal of the results of the infringement through – for example – a publication of apologies. They may also seek compensation in the case when a moral and pecuniary damage occurred (they may also	Poland, Article 23 and 24 of the Civile Code (*Ustawa kodeks cywilny*) 23 Aprill 1964

			ask the defendant to make a donation for a charity or a community purpose).	

Criminal Code – misuse of competences of a public official				
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**
Collection **Analysis*** **Storing*** **Destruction*** **After the whole surveillance process has ended**	*n/a*	*n/a*	One can report the offence described in Article 231 of the Criminal Code to the prosecution or the police. Article 231 states that a public official who exceeds his authority or does not perform his duty, acts to the detriment of a public or individual interest shall be subject to the penalty of deprivation of liberty for up to 3 years. Excessive acquisition of telecommunication data may constitute a misuse of competences by intelligence service officials.	Article 231 of the Polish Criminal Code (*Kodeks karny*) 6 June 1997

Data Protecion Act – criminal sanctions for data protection breaches				
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**
Collection*	*n/a*	*n/a*	One can report an offence to the prosecution or the police on the grounds of the Data Protection Act. Chapter 8 of the Data Protection Act contains provisions on the criminal liability for offences defined in Articles 49-52 of the Act. They include, *inter alia*, offences such as: disclosure or providing access to data to unauthorized persons, processing personal data in a data filing system where such processing is forbidden or is a violation of the obligation to protect data against unauthorized takeover, damage or destruction. The offences are prosecuted by law enforcement bodies in accordance with the general procedural rules laid down in the Code of Criminal Procedure. Under the applicable criminal provisions laid down in the Data Protection Act, the possible criminal sanctions, depending on particular offences are: fine and restriction or deprivation of liberty.	Data Protection Act *(Ustawa o ochronie danych osobowych)* 29 August1997
Analysis*				
Storing*				
Destruction *				
After the whole surveillance process has ended				

* 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 term of imprisonment ranges from less than a year, if the infringing party acted inadvertently, up to 3 years, if the offence concerns sensitive data.	

Annex 4 – Surveillance-related case law at national level

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

Case title	K 23/11
Decisiondate	30 July 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Constitutional Court (*Trybunał Konstytucyjny*)
Key facts of the case (max. 500 chars)	In 2011, the Human Rights Defender and Prosecutor General made several applications to the Constitutional Court to conduct, *inter alia*, a review of the laws governing the use of telecommunication data stored by telecom providers (data retention) by intelligence agencies. Both organs used their entitlement to initiate an abstract constitutional review of the respective regulations (i.e. not connected with a specific case).
Main reasoning/argumentation (max. 500 chars)	The applicants argued that the current regulations violate the right to privacy (freedom of communication) and the principle of specificity of law. In particular, they complained that the laws do not provide any external control over the use of data retention by intelligence services. They also argued that existing laws pose threats to the journalistic sources of information and advocates' professional secrecy. The full reasoning of the Court has not yet been published. The reasoning may be important for the perception of these issues in Poland.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court agreed with the applicants' argumentation with regard to regulations allowing different intelligence services to use data retention and found these provisions unconstitutional. Currently, the intelligence services have too broad access to telecommunication data, which enables them to acquire data secretly without any possibility for the data subject to question such conduct. Therefore, it is crucial that law should provide for judicial or any other independent control over the use of information obtained by the intelligence agencies from telecom providers.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The data retention regulations that were found unconstitutional by the Court will lose their binding force in 18 months from the date of publication of the judgment in the Journal of Laws. In a long term, a legislative procedure will have to be launched in order to amend the current data retention laws and adjust them to the ruling. The Minister of Interior announced that the ministry will analyse the judgment and prepare a draft law within the next 12 months[42].

42 Poland, Polish Press Agency, Minister of Interior Bartłomiej Sienkieiwcz: two expert teams analyse the Constitutional Court's rulling (Szef MSW Bartłomiej Sienkiewicz: dwa zespoły analizują wyrok TK ws. zasad inwigilacji), http://wiadomosci.wp.pl/kat,1342,title,Szef-MSW-Bartlomiej-Sienkiewicz-dwa-zespoly-analizuja-wyrok-TK-ws-zasad-inwigilacji,wid,16791240,wiadomosc.html?ticaid=113388&_ticrsn=3, 31 July 2014, available at: (accessed on 7 August 2014).

Case title	Wróblewski v. CBA, I ACa 1002/12
Decision date	26 April 2013
Reference details (type and title of court/body; in original language and English [official translation, if available])	Court of Appeals in Warsaw (*Sąd Apelacyjny w Warszawie*)
Key facts of the case (max. 500 chars)	B. Wróblewski, a journalist of one of the Polish dailies, filed a suit with the court against the Central Anti-Corruption Bureau (CBA) claiming that CBA had infringed his personal interests. The infringement allegedly consisted of an unlawful acquisition, for an unknown reason, of his telecommunications data, including phone records and location data for 6 months between 2005 -2007. The journalist was known for writing about high-profile and scandalous operations of the CBA.
Main reasoning/argumentation (max. 500 chars)	The journalist claimed that CBA infringed his constitutional rights including the right to privacy, freedom of communication and, above all, the right to freedom of expression because it posed a threat to the confidentiality of his journalistic source. He claimed that the practice of using data retention, by collecting and reviewing billing information concerning a journalist, is unlawful despite broad competences of the CBA in this respect.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court stated that by accessing journalist's phone records the intelligence services had clearly interfered with his constitutional freedoms. Such interference should be possible solely when it is clearly permissible under the law, appropriately justified and proportionate in comparison to the benefits expected to be obtained (e.g. in case of a serious crime). The court also confirmed that the journalists' phone billings should be protected under the regulations concerning the journalistic shield laws.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The CBA was obliged to publish an apology to the journalist in the press for violating his privacy and was ordered to destroy the illegally acquired telecommunication data concerning the claimant. The ruling is final (the Court of Appeal upheld the previous judgment of the District Court in Warsaw[43]). The judgment was executed by the CBA.

43 Poland, Regional Court in Warsaw (*Sąd Okręgowy* w *Warszawie*), II C 626/11, 26 April 2012.

Case title	Helsinki Foundation for Human Rights v. ABW, II SA/Wa 710/14
Decisiondate	24 June 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Voivodeship Administrative Court in Warsaw (*Wojewódzki Sąd Administracyjny w Warszawie*)
Key facts of the case (max. 500 chars)	In October 2013, three Polish NGOs (HFHR, Panoptykon Foundation, Amnesty International) prepared a set of requests for disclosure of public information by different state agencies and institutions after the so-called "Snowden disclosures". In particular, NGOs formed 100 specific PRISM-related questions addressed to various institutions. One of the requests was addressed to the Internal Security Agency. It concerned the existence of an agreement between the Internal Security Agency and the US authorities on the telecommunication data exchange, and asked whether the Agency is in possession of certain tools and means used for telecommunication mass surveillance. The Agency refused to provide such information.
Main reasoning/argumentation (max. 500 chars)	The Internal Security Agency argued that it could legitimately refuse access to such information because disclosing it would harm the state's interests (public security).
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court stated that the refusal was unjustified. The public has the right to obtain information about the fact that Polish intelligence services' cooperate with foreign bodies and about the general scope of this cooperation. As regards the means and tools employed by the services for mass surveillance, although sometimes the public security may provide a legitimate reason not to reveal them, there have to be always specific grounds demonstrated to refuse access to such information. The Agency did not prove sufficiently that refusal was necessary and proportionate in this case.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Agency's refusal was quashed by the court. The ruling is not final. The Agency submitted a cassation appeal to the Supreme Administrative Court. The date of the court hearing has not been determined yet. If the ruling becomes final, the Agency will have to re-examine the HFHR's request, taking into account the court's guidelines.

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). Pleaseprovidename, website and contactdetails

Name of stakeholder (in English as well as your national language)	**Type of stakeholder**, *civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Ministry of Administration and Digitization of Poland (*Ministerstwo Administracji i Cyfryzacji*)	Government	ul. Królewska 27 00-060 Warsaw tel. (0048)22 245 59 20 mac@mac.gov.pl	https://mac.gov.pl
Ministry of the Interior (*Ministerstwo Spraw Wewnętrzych*)	Government	ul. StefanaBatorego 5, 02-591 Warsaw tel. (0048) 22 621 20 20 kancelaria.glowna@msw.gov.pl	https://www.msw.gov.pl
Office of Electronic Communications (*Urząd Komunikacji Elektronicznej*)	Public authority/ national regulatory authority	ul. Kasprzaka 18/20 01-211 Warsaw tel. (0048) 22 534 91 90 uke@uke.gov.pl	http://www.uke.gov.pl
The Constitutional Court (*Trybunał Konstytucyjny*)	Judicial body	al. Jana Christiana Szucha12a, 00-918 Warsaw tel. (0048) 22 621-65-03	http://trybunal.gov.pl

		prezydialny@trybunal.gov.pl	
Human Rights Defender (*Rzecznik Praw Obywatelskich*)	Ombudsman	Aleja Solidarności 77 00 - 090 Warsaw tel. (0048) 22 55 17 700 biurorzecznika@brpo.gov.pl	http://www.brpo.gov.pl
Supreme Audit Office (*Najwyższa Izba Kontroli*)	Public authority/ top independent state audit body	ul. Filtrowa 57 02-056 Warsaw tel. (0048) 22 444 50 00 nik@nik.gov.pl	http://www.nik.gov.pl
Inspector General for the Protection of Personal Data (*Generalny Inspektor Ochrony Danych Osobowych*)	Data protection authority	ul. Stawki 2 00-193 Warsaw tel. (0048) 22 860 70 86 kancelaria@giodo.gov.pl	http://www.giodo.gov.pl
Helsinki Foundation for Human Rights (*Helsińska Fundacja Praw Człowieka*)	Civil society	ul. Zgoda 11, 00-018 Warsaw tel. (0048) 22 556 44 40 hfhr@hfhrpol.waw.pl	http://www.hfhr.pl
Panoptykon Foundation (*Fundacja Panoptykon)*	Civil society	ul. Orzechowska 4/4, 02-068 Warsaw tel. (0048) 660 074 026 fundacja@panoptykon.org	http://panoptykon.org
Digital Center (*Centrum Cyfrowe*)	Civil society	ul. Andersa 29 00-159 Warsaw kontakt@centrumcyfrowe.pl	http://centrumcyfrowe.pl
Amnesty International Poland (*Amnesty International Polska*)	Civil society	ul. Piękna 66A/2 00-672 Warsaw	http://amnesty.org.pl

		tel. (0048) 22 827 60 00 amnesty@amnesty.org.pl	
Press Freedom Monitoring Centre (*Centrum Monitoringu Wolności Prasy*)	Journalistic association	ul. Foksal 3/5, 00-366 Warsaw tel. (0048) 22 827-58-96 cmwp@ikp.pl	http://www.freepress.org.pl
Modern Poland Foundation (*Fundacja Nowoczesna Polska*)	Civil society	ul. Marszałkowska 84/92 00-514 Warsaw tel. (0048) 22 621 30 17 fundacja@nowoczesnapolska.org.pl	http://nowoczesnapolska.org.pl
Free and Open Source Software Foundation (*Fundacja Wolnego i Otwartego Oprogramowania*)	Civil society	ul. Staszica 25/8 60-524 Poznań tel. (0048) 61 6243474 info@fwioo.pl	https://fwioo.pl
The Supreme Bar Council (*Naczelna Rada Adwokacka*)	Professional	ul. Świętojerska 16, 00-202 Warsaw tel. (0048) 22 505 25 01 nra@nra.pl	http://www.nra.pl
Lex InformaticaAssociation (*Naukowe Centrum Prawno-Informatyczne*)	Think tank/academia	ul. KazimierzaWóycickiego 1/3 Lok.17 01-938 Warsaw info@ncpi.org.pl	http://ncpi.org.pl
Prof. dr hab. Andrzej Adamski	Academia	ul. WładysławaBojarskiego 3,	http://www.law.umk.pl

Professor at University of MikolajKopernik in Torun (*Uniwersytet im. Mikołaja Kopernika w Toruniu*)		87-100 Toruń tel. (0048) 56611 40 91 aadamski@law.uni.torun.pl	
Central Anti–Corruption Bureau (*Centralne Biuro Antykorupcyjne*)	Intelligence service	Al. Ujazdowskie 9, 00-583 Warszawa tel. (0048) 22437 22 22 kontakt@cba.gov.pl	www.cba.gov.pl/
Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*)	Intelligence service	Rakowiecka 2A, 00-993 Warszawa tel. (0048) 22 565 91 10 poczta@abw.gov.pl	http://www.abw.gov.pl
Foreign Intelligence Agency *(Agencja Wywiadu)*	Intelligence service	02-634 Warszawa ul. Miłobędzka 55 tel. (0048) 22 640-50-19 poczta@aw.gov.pl	http://www.aw.gov.pl/
Military Counter-intelligence Service (*Służba Kontrwywiadu Wojskowego*)	Intelligence service	ul. Oczki 1 00-909 Warszawa 60 tel. (0048) 2268 46 119 email: skw@skw.gov.pl	www.skw.gov.pl/
Military Intelligence Service (*Służba Wywiadu Wojskowego*)	Intelligence service	Aleja Niepodległości 243 02-009 Warszawa tel. (0048) 2268-32-666 sww.kontakt@mon.gov.pl	http://www.sww.gov.pl/
Border Guard (*Straż Graniczna)*	Intelligence service	al. Niepodległości 100 02-514 Warszawa tel. (0048)22 5004000	http://www.strazgraniczna.pl/

		gabinet.kg@strazgraniczna.pl	
Customs Service (*Służba Celna)*	Law enforcement agency	Ul. Świętokrzyska 12, 00-916 Warszawa tel. (0048) 22 694-38-50, sekretariat.cp@mofnet.gov.pl	http://www.mf.gov.pl/sluzba-celna
Military Police (*Żandarmeria Wojskowa)*	Intelligence service	ul. Jana Ostroroga 35 01-163 Warszawa tel.: (0048) 22 6 857 105 kgzw_sekretariat@wp.mil.pl	http://www.zw.wp.mil.pl/pl/index.html
Police (*Policja*)	Law enforcement agency	ul. Puławska 148/150, 02-624 Warszawa tel. (0048) 22 62 102 51	http://www.policja.pl/
Treasury Control (*Kontrola Skarbowa)*	Intelligence service	ulŚwiętokrzyska 12, 00-916 Warszawa +48 (22) 694 55 55 kancelaria@mofnet.gov.pl.	http://www.mf.gov.pl/kontrola-skarbowa

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

Cichocki, J. (2011), Raport dotyczący retencji danych telekomunikacyjnych, Sekretarz Stanu ds. Bezpieczeństwa w Kancelarii Premiera, Warszawa

Urząd Komunikacji Elektronicznej (2013), Udostępnianie danych telekomunikacyjnych w 2012 r., Press release, 2 April 2013, www.uke.gov.pl/udostepnianie-danych-telekomunikacyjnych-w-2012-roku-12248

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

Naczelna Izba Kontroli (2014), Nadzór nad służbami specjalnymi, Press release, 26 August 2014

http://www.nik.gov.pl/aktualnosci/nadzor-nad-sluzbami-specjalnymi.html

Rzecznik Praw Obywatelskich (2011), wnioski do Trybunału Konstytucyjnego w sprawie zgodności z Konstytucją ustaw stanowiących podstawę dla pobierania przez służby danych telekomunikacyjnych, Warszawa

Naczelna Izba Kontroli (2013), Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne, Warszawa

Naczelna Rada Adwokacka (2011), Retencja danych: troska o bezpieczeństwo czy inwigilacja obywateli? Polak najbardziej inwigilowanym obywatelem Europy?, Warszawa

Rzecznik Praw Obywatelskich (2013), Wystąpienie do Prokuratora Generalnego w sprawie zapobiegania sytuacjom nieautoryzowanego przetwarzania danych osobowych polskich internautów, Warszawa

3. Non-governmental organisations (NGOs)

Klicki, W. and Obem, A. and Szymielewicz K. (2013), *Telefoniczna kopalnia informacji. Przewodnik*, Warszawa, Fundacja Panoptykon
http://telefoniczna-kopalnia.panoptykon.org/

Szumańska, M. and Szymielewicz, K. (2013), *Access of public authorities to the data of Internet service users*, Warszawa, Fundacja Panoptykon
http://panoptykon.org/sites/panoptykon.org/files/transparency_report_pl.pdf

Mednis, A. and Szymielewicz, K. Lach, K. (2011), *Privacy Report - Poland*, Privacy international
https://www.privacyinternational.org/reports/poland

Helsińska Fundacja Praw Człowieka (2011), Stanowisko HFPC ws. Pozyskiwania billingów oraz treści informacji tekstowych dziennikarzy, Warszawa
http://www.obserwatorium.org/images/inwigilacja_dziennikarzy_29_12_2011.pdf

Helsińska Fundacja Praw Człowieka (2012), Uwagi Helsińskiej Fundacji Praw Człowieka do projektu założeń ustawy o zmianie niektórych ustaw w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych, Warszawa
http://www.obserwatorium.org/images/retencja_MSW.pdf

Helsińska Fundacja Praw Człowieka (2012), Stanowisko Helsińskiej Fundacji Praw Człowieka w sprawie z powództwa Bogdana Wróblewskiego, Warszawa
http://www.obserwatorium.org/images/Stanowisko%20HFPC_Wroblewski.pdf

Helsińska Fundacja Praw Człowieka, (2013), '100 pytań o inwigilację do polskich władz', Press release,
www.hfhr.pl/100-pytan-o-inwigilacje-do-polskich-wladz

Bodnar, A. (2013), presentation given at the European Parliament LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 18 November 2013, published at:
www.europarl.europa.eu/document/activities/cont/201311/20131115ATT74519/20131115ATT74519EN.pdf.

4. Academic and research institutes, think thanks, investigate media report:

Adamski, A. (2005), Retencja danych o ruchu telekomunikacyjnym – polskie rozwiązania i europejskie dylematy, *Acta Uniwersytetu Wrocławskiego Przegląd Prawa i Administracji*, No. 70, pp. 173-188.

Adamski, A. (2012), Kontrola dostępu do danych telekomunikacyjnych podlegających obowiązkowi retencji na tle ustawodawstwa wybranych państw Unii Europejskiej, Warszawa

Adamski, D. (2007), Retencja danych telekomunikacyjnych - *uwagi de lege ferenda* wynikające z przepisów wspólnotowych, *Monitor Prawniczy*, No. 4, pp. 8-11.

Czuchnowski, W. (2010), Dziennikarze na celowniku służb specjalnych, Gazeta Wyborcza, Warszawa

Głowacka, D. (2011), Kontrola billingów w świetle gwarancji chroniących osobowe źródła informacji dziennikarskiej, Biuletyn Informacyjny Obserwatorium Wolności Mediów w Polsce, No. 24, pp. 1-4
http://www.obserwatorium.org/images/biuletyn%20nr%2024%20www.pdf

Konecki, J. Misztal-Konecka, J. (2010), Billing jako dowód w postępowaniu w sprawach o wykroczenia, *Państwo i Prawo,* No. 7, pp. 78-87.

Ostrouch, S. (2013), Retencja danych telekomunikacyjnych wykorzystywanych przez organy ścigania w świetle systemu ochrony praw człowieka, In: Jaskiernia, J. *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka. Materiały konferencyjne,* pp.284-291.

Rogalski, M. (2010), Prawo telekomunikacyjne. Komentarz. (Warszawa)

Siwicki, M. (2011), Retencja danych transmisyjnych na podstawie art. 180a Prawa telekomunikacyjnego, *Prokuratura i Prawo* 2011, No.9, pp. 111-124.

Wach, M. (2009), Retencja danych a prawo do ochrony prywatności, *Radca Prawny*, No.2 pp. 89-92.