Balancing the interests in the context of data retention (INVODAS)

Poland

Krzysztof Wojciechowski

Part 1: General overview of the legal transposition, the national (societal) context and the constitutional/fundamental rights legal framework

A. State of play of the transposition of the Directive 2006/24/EC

I. Legal provisions

- *Introductory remark:* If national legal provisions mandating the retention of electronic communications data without any *specific* reason (i.e. stockpiling, without an actual, concrete cause) have existed already before the Directive 2006/24/EC (in the following: "the Directive") was enacted, please also make reference to these when answering to questions 5 to 35.

- *Introductory remark:* Most of the questions concerning retention obligations refer to the national provisions transposing the Directive. Some questions, however, make explicit reference to the "national law" or the "national legal system" as a whole. In these cases, we request you to provide more comprehensive information. In any case, only retention *without a specific reason* (i.e. stockpiling, without an actual, concrete cause) of data generated or processed in *electronic communications* is concerned by this questionnaire. Other retention obligations, for instance those requiring that there be a suspicion of a crime having been committed, are not covered by this questionnaire.

1. Have the provisions of the Directive already been transposed into national law?

The Directive 2006/24/EC has been transposed into Polish law in 2009. Before that different sets of rules existed. Elements of data retention were introduced in the Regulation by Minister of Infrastructure of 24 January 2003[1] enacted on the basis of

[1] *Regulation on fulfillment by operators of tasks serving the defense and security of the state, as well as public security and order*, Journal of Law (*Dziennik Ustaw* – Dz.U.) 2003, No 19, item 166.

Art.40 of the Telecommunications Law of 2000[2] dealing with operators' tasks related to state/public defense, security and order. The Law provided for an obligation to secure, on operator's cost, *technical and operational possibilities of fulfillment in a telecommunications network tasks for the public prosecution, courts, authorized entities subordinated to the Minister of Defense, Minister of Interior, Minister of Finance, Chief of the Agency of National Security*. The Regulation of January 2003 *i.a.* obliged operators to make available to *authorized entities* data in their possession for last 12 months (§ 5 p.7). However this obligation concerned the data "in possession", thus it did not include a duty to store the data, but rather applied to data stored for other purposes.

With the adoption of the new Telecommunications Law of 2004[3] (TL) data retention became a statutory obligation. Art.165 para.1 of the Law obliged operators of public telecommunications networks and providers of publicly available telecommunications services who processed data concerning subscribers and end users, given the fulfillment by *authorized entities* of tasks and duties for defense, security and public order, to store these data for 12 months. As of 2006[4] the term was extended to 2 years[5]; also the obligation for operators and providers storing transmission data of *special diligence in order to protect the security and confidentiality of these data and interests of persons concerned* was added. Separate provisions regulated the control of the content of communications and access to certain data *on request of authorized entities*, including public prosecution and courts.[6]

The first draft act transposing the Directive 2006/24/EC was adopted by the government in July 2007; the draft provided for 4 years of data retention. After parliamentary elections that year the new government decided to change the draft, *i.a.* to limit the data retention term to 2 years. However that first draft was submitted to the Parliament as a draft of the group of parliamentarians[7] in January 2008 and finally rejected a year later. In October 2008 the Government adopted a new draft act implementing the Directive and submitted it to the Parliament[8]. In consequence, the act amending the TL so as to transpose the Directive was adopted in July 2009. Art.165 para.1 of the TL was repealed and new set of provisions on data retention

---

2 The act of 21 July 2000, Dz.U. 2000, No 73, item 852, with amendments.

3 The act of 16 July 2004, Dz.U. 2004, No 171, item 1800, with amendments.

4 The act of 29 December 2005 amending the Telecommunications Law and the Code of Civil Procedure, Dz.U. 2006, No 12, item 66; entry into force: 9 February 2006.

5 During the legislative works there was even the proposal, finally rejected, to extend the term of data retention to 15 years, with the argument that it would correspond to the term of prescription of criminal offences under the Penal Code. In 2007 another draft act amending the TL, that was not adopted, was supposed to extend the data retention term to 5 years.

6 Art.179 and f. of the TL

7 The draft is available (in Polish) at the website of Polish Sejm (lower house of the Parliament):
http://orka.sejm.gov.pl/Druki6ka.nsf/0/54DA88C06633A502C1257516003C9E7D/$file/1452.pdf

8 The draft is available (in Polish) at:
http://orka.sejm.gov.pl/Druki6ka.nsf/0/01759E51562DDFD3C1257516003C9E95/$file/1448.pdf

based on the Directive was introduced (Articles 180a-180g of the TL). These new statutory rules were as of 1 January 2010 complemented by the Regulation of the Minister of Infrastructure.

- ***If transposition has <u>not at all</u>, or only in <u>parts</u>, been accomplished:***

2. **What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?**

   N.a.

3. **Is transposition still intended? If so: What is the current state of play of the transposition process? Until when is it likely to be finalised?**

   N.a.

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   N.a.

- ***If transposition has been <u>accomplished</u>:***

General questions

5. **Is there an English version of the texts available? If so: Please indicate the respective URL.**

   The English version of unofficial consolidated version of the Telecommunications Law is available on the website of the Office of Electronic Communication: http://www.en.uke.gov.pl/_gAllery/10/58/1058/telecommunications_law.pdf

   (For provisions transposing the Directive - see Articles 180a-180g).

   The text of the so-called Retention Regulation (see below) is available only in Polish:

   http://www.mi.gov.pl/files/0/1792145/Rozpzart180cust21412finalrev1popr2312bezrej.pdf

6. **Since when have the relevant regulations been in force? Are there any transition periods in place regarding the application of these regulations?**

   See below.

7. **What type of legal act do the existing rules meant to transpose the Directive's provisions pertain to (e.g. Act of Parliament, decree-law, regulation/decree, administrative provisions etc)? Please give an overview of all legal provisions enacted for this purpose (stating the type of legal act and the matter regulated therein) and describe**

   a) **whether "more important matters have been dealt with by (parliamentary-enacted) legislation whereas provisions of a more technical/technology-oriented character are tackled by decrees/administrative provisions, and**

   b) **whether the types of legal acts chosen for the different matters regulated correspond to those usually chosen in your legal system for such kind of matters.**

   The transposition have been done in two steps.

   First, provisions implementing the Directive were included in the broader revision of the Telecommunication Law of 2004[9] (TL) by the act of 24 April 2009[10] amending this Law. This revision in particular added Articles 180a – 180g of the TL on duties of data retention, as well as provisions on access to retained data to the acts on certain institutions that obtained competence of such an access (ex. the Police, Border Guard, Fiscal Control, certain special services etc.). The said act amending the TL entered into force on 6 July 2009, except one provision (dealing with a case of insolvency of an operator or provider) that entered into force on 1 January 2010.

   Secondly, more detailed provisions were introduced by the Regulation of Minister of Infrastructure of 28 December 2009 on *detailed categories of data and operators of publicly available telecommunications networks and/or providers of publicly available telecommunications services obliged to retain and store such data*[11], called *Retention Regulation* (RR). The Regulation entered into force on 1 January 2010, however the transition period of 6 months was envisaged for operators of public telecommunications networks and providers of publicly available telecommunications services that operated before the RR entered into force, if they were unable to meet the requirements of the Regulation; in the transition period data subject to retention obligations, should be retained and stored under former rules.[12]

---

9 Act of 16 April 2004 Telecommunications Law, Dz.U. (Dziennik Ustaw) of 2004, No 171, item 1800, with amendments.

10 Dz.U. 2009, No 85, item 716.

11 Dz.U. 2009, No 226, item 1828.

12 Polish Chamber of Informatics and Telecommunications in the letter of 08.03.2010 asked Minister of Infrastructure to extend this period until 31.12.2010, raising the arguments of high costs for operators and difficulties with technical solutions necessary to fulfill the Regulation. The term has not been extended.

Further details of a technical nature relating to data retention are included in two other regulations.[13]

Transposition of the Directive partly by a parliamentary act and partly by regulations (dealing with more detailed, technical issues), adopted by competent ministers on the basis of statutory delegation, corresponds to usual method of regulating such kind of matters..

8. Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions given therein differ from those in art. 2 para. 2? Are there any other terms mentioned in the Directive or in the directives referred to by the Directive (see the reference made in art. 2 para. 1 of the Directive to Directives 95/46/EC, 2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?

Certain terms defined in Art.2 para.2 of the Directive are also defined in Polish provisions transposing the Directive.

A. Relevant *data* are defined in Art.180c para.1 of the Telecommunications Law and §§ 3-7 of the Retention Regulation. These provisions include more detailed description of data covered than the definition in the Directive, however the description relates to the purpose laid down in Art.2 para.2 a) of the Directive (see below for more details).

B. The term *user* as defined in Art.2 para.2 b) of the Directive has not been specifically defined in the Polish provisions introduced to transpose the Directive. These provisions apply the term *end user* (*użytkownik końcowy*) which is defined in Art.2 p.50 of the TL (i.e. within general provisions of the Law), as *an entity using or requesting a publicly available telecommunications service to satisfy its own needs*.

C. *Telephone service* has not been specifically defined for data retention purposes. The general provisions of the TL contain definitions of the following related terms: *publicly available telephone service* (Art.2 p.30), *telecommunications service* (Art.2 p.48), *call* (Art.2 p.24a), *telecommunications message* (Art.2 p.27a), *telephone call* (Art.2 p.26).

D. *User ID* is defined (as *user identifier*) in § 2 p.7 of the Retention Regulation, as follows: *unique identifier allocated to an end user by an operator of public telecommunications network or a provider of publicly available*

[13] Regulation of Minister of Infrastructure of 30 December 2009 on a form for transfering by telecommunications enterprise to Chairman of the Office of Electronic Communication of information concerning making available of data, Dz.U. 2010, No 3, item 15; Regulation of Prime Minister of 22 March 2010 on a method of transfer and making available data in case of insolvency of a operator of public telecommunications network and/or provider of publicly available telecommunications services, Dz.U. 2010, No 48, item 281.

telecommunications services, related to provided service of access to Internet or service of Internet communication.

E. *Cell ID* a such has not been defined. The Retention Regulation uses and defines the term *BTS station* as *an equipment which permits connection of telecommunications terminal equipment, used in mobile public telephone network with a fixed part of this network* (§ 2 p.13 of the RR; see also § 4 pp. 4-5 of the RR as quoted below).

F. *Unsuccessful call attempt* is defined in the context of telecommunications confidentiality in Art.159 para.1 p.5 of the TL as *calls between telecommunications terminal equipment or network termination points which have been set up and not answered by an end user or aborted.*

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

Under Art.180c para.1 of the TL the obligation of data retention and storage cover the data necessary to:
1) trace the network termination point, telecommunications terminal equipment, an end user:
a) originating the call,
b) called;
2) identify:
a) the date and time of a call and its duration,
b) the type of a call,
c) location of telecommunications terminal equipment.
Detailed categories of data to be retained are defined in the *Retention Regulation,* depending on the type of networks and services, and thus separately for fixed public telecommunications networks (§3), mobile public telecommunications networks (§ 4), services of redirection and reconnection of a call (§ 5), Internet access services, e-mail services and Internet telephone services (§ 6 and 7).

For fixed and mobile telecommunications networks these are numbers of terminal equipment (telephones), from which the call was initiated and to which the call was directed, names and addresses of users of these telephones, the date and time of a start, end and duration of a call, as well as data on localization of telephones. As regards localization of a telephone in mobile network detailed data necessary to trace an approximate localization is defined in § 4 p.5-6; it covers besides the mere identification of the BTS station's antenna in the reach

of which terminal equipment was located and geographic location of this BTS station, also *azimuth, bundle and working reach of the BTS station's antenna.*
In case of an Internet access service, e-mail service, and Internet telephony service (§ 6) the data covered allows to individualize an end user using such a service, in particular through his identifier and identifier of network equipment, IP address and data related to the time of connection and disconnection with Internet. One of the possible identifiers of an end user initiating the call is a number of a network port (besides of DSL identifier and MAC address).
In case of an e-mail service and Internet telephony service (§ 7) in addition data concerning a recipient of a call are to be retained.

For the sake of completeness the provisions in question, in unofficial – author's own translation, are presented in the annex.

Polish legislator chose different systematic methodology in listing data to be retained, than the one used in the Directive. Also wording used in Retention Regulation is slightly different, given the need to make it coherent with the terminology of Polish Telecommunications Law and practice.
Apart from aspects of the legislative technique, Polish rules defining data to be retained go beyond the Directive. In particular e-mail services has not been explicitly limited to the Internet e-mail services, although the context and content of the relevant provisions show that this is the field that was mainly intended to be covered (§ 6 and 7 of the RR). It is clear that data on unsuccessful call attempts have to be retained (Art.180a para.5 of the TL) both in relation to fixed and mobile public telecommunications networks (§ 3 p.3 a/ and § 4 p.3 a/ of the RR).

10. Does national law otherwise provide for, or allow for, the retention of electronic communications data (customer records, traffic data and/or the content of communications) beyond the data to be retained in accordance with the Directive? Please specify the substance of these provisions.

Under Art.180a para.6 of TL the data retention obligation should be performed in a way that does not lead to a disclosure of the content of communications.

In general, content and data subject to telecommunications confidentiality (user's data, content of individual communications, transmission data, location data, unsuccessful call attempts data), may be processed (*i.e.*: collected, recorded, stored, elaborated, modified, deleted or made available) only where it refers to the service provided to an user or is necessary to perform it, and for other purposes only when it is permitted under statutory provisions of law (Art.161 para.1 of the TL). As regards user's data a provider of publicly available telecommunications services is entitled under the TL (Art.161 para.2) to process certain data on a user being a natural person, concerning his/her identification (name, birth), address, personal number, ability to perform an agreement for the provision of telecommunications services. With the consent of a user (a natural person), the processing of certain other user's data is allowed, as personal tax number, bank account, credit card number etc. (Art.161 para.3 of the TL).

A provider of publicly available telecommunications services is obliged to record data with regard to performed telecommunications services to the extent that allows to determine the amount due for performing these services as well as to consider a complaint. The data shall be stored for at least 12 months, and in the event of a complaint being filed, for the time necessary to resolve the dispute (Art.168 of the TL).The processing of transmission data necessary for charging subscriber fees and interoperator settlements is permissible if a subscriber or an end user has been informed on the type of transmission data that is to be processed by a provider of publicly available telecommunications services, and on the period of such a processing (Art.165 para.2 of the TL). The processing of the transmission data for marketing purposes requires a consent of the subscriber or the end user (Art.165 para.2 of the TL).

The use of location data (beyond the data necessary for message transmission and billing purposes), is permissible only if a provider of publicly available telecommunications service obtained the consent of a subscriber or an end user, or performed the anonymisation of this data. Location data may be processed only where this is necessary to provide value added services (Art.166 of the TL).

A provider of publicly available telecommunications services shall inform a subscriber with whom an agreement for the provision of telecommunications services is concluded, as well as the remaining end users, of the scope and purpose of processing transmission data and other data concerning the subscriber or end users, as well as of the possibility of influencing the scope of this processing (Art.163 of the TL). End user data may be processed during the period within which an agreement remains in force, and after its termination during the period of vindication of claims or the performance of other tasks provided for in the law (Art.164 of the TL).

The processing of data provided in the TL is subject to personal data protection rules.

Control and fixation of the content of communications is regulated by separate provisions concerning *authorized entities* (ex. the Police) and criminal procedure; it requires court order.

11. According to the national rules transposing the Directive, for which purposes is data retention mandated in each case?

The broad purpose of data retention is *state defense and security, as well as public security and order*, as says the title of Part VIII of the TL. More specific purposes are determined by *separate provisions* which mandate *authorized entities*, public prosecutors and courts to obtain an access to data retained. The purpose of making available of data to the Police, the Border Guard, the Military Police is *prevention and detection of criminal offences*; in case of fiscal intelligence - it is *prevention and detection of fiscal criminal offences* and certain other offences related to corruption and international transfers. In case of the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego* – ABW), the Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne* – CBA), the Military Counter-intelligence Service

(*Służba Kontrwywiadu Wojskowego* – SKW) – no specific purpose of obtaining the access to data is defined, besides respective statutory definitions of their tasks. In case of public prosecutors and courts the telecommunications data should be made available *if they are relevant for pending proceedings*. Such a broad basis for access to data retained has been criticized. In particular in Ombudsman's letters to the Prime Minister[14] the argument was raised that (as opposed to the case of the control of a content of telephone calls) the catalogue of criminal offences in relation to which the access to data may be obtained has not been limited, which allows to use data also in minor offences, like traffic accidents. Moreover "the prevention of crimes" and tasks of the relevant secret services (ABW, CBA, SKW) are so broad that in connection with the lack of external control (court orders – see below) they allow authorized entities to obtain the access to data whenever it is deemed useful for these entities in performance of their tasks. This leads the Ombudsman to the conclusion that the measures do not meet proportionality requirements, and thus need to be amended. The same argumentation has been raised in the motion to the Constitutional Court filled by the group of Parliamentarians on 28 January 2011.[15]

12. Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?

The provisions transposing the Directive into Polish law do no differentiate between ordinary and sensitive data, and do not provide for any special rules on sensitive data. Nor do they exist on data related to legally protected confidentiality.
Sensitive data are defined in Poland in Art.27 para.1 of Personal Data Protection Act[16] as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court.

---

14 The letter of 05 February 2010 to the Prime Minister *on legislative initiatives of members of the Government concerning certain aspects of citizens' activities in the Internet*. The Polish text is available at: http://www.sprawy-generalne.brpo.gov.pl/pdf/2009/12/637079/1459206.pdf

The letter of 17 January 2011 to the Prime Minister on obtaining by the special services of information subject to the telecommunications confidentiality. The Polish text is available at:

http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf

15 Morion of 28.01.2011, to the Constitutional Court, by the group of Parliamentarians (from SLD – *Democratic Left Alliance* – socialdemocratic party); the text (in Polish) is available on:

http://www.sld.org.pl/aktualnosci/p-r-m-a-6710/aktualnosci.htm

16 The act of 29 August 1997, consolidated text: Dz.U. 2002, No 101, item 926, with amendments. The English translation is available:

http://www.giodo.gov.pl/144/id_art/171/j/en/

Processing of such data is forbidden, except in listed circumstances[17], including a specific provision in a statutory act.
Provisions transposing the Directive do not exclude any category of users, although the data that concern some of them may be subject to the legally protected confidentiality, namely notary, lawyers', medical or journalistic confidentiality. Under Art.180 para.2 of the Code of Criminal Procedure such confidentiality may be repealed, by the court, only when necessary for the good conduct of justice and if certain facts may not be established with other evidence. However in case of journalistic confidentiality this may not lead to the disclosure of sources. The data retention rules do not take special legal protection of those confidentialities into account, which was criticized by the Polish Ombudsman.[18] This aspect was also covered by the motion to the Constitutional Court by the group of Parliamenatrians of 28.01.2011.

13. **For how long do the data retained in accordance with the national rules transposing the Directive have to be kept available? In case a distinction is made according to data categories: Please describe the criteria the distinction is based upon and the reasons therefore.**

The data retained according to Polish provisions transposing the Directive have to be kept for 24 months counted from the day of a call or an unsuccessful call attempt. After the expiry of this period the data shall be erased, except data secured under *separate provisions*.

14. **Which authorities or other bodies are entitled to access the data retained (e.g. law enforcement agencies, security authorities and/or intelligence, other public bodies, (private) claimants/litigants)?**

Bodies entitled to access the data retained are: the Police, the Border Guard, the Military Police, the fiscal intelligence, the Internal Security Agency (ABW), the Central Anti-Corruption Bureau (CBA), the Military Counter-intelligence Service (SKW) – called *authorized entities*, as well as public prosecutors and courts.

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative offences), security, civil action (e.g. to enforce copyright claims))? Does the**

---

17 Art.27 para.2 of the Personal Data Protection Act allows processing of sensitive data in case of: 1) written consent,of the person concerned, 2) the specific statutury provisions, 3) in the vital interest of the person where he/she is incapable of giving his/her consent; 4) when necessary for the purposes of churches and other religious unions, associations, foundations, and certain other non-profit organisations, in relation to the members of those organisations or to the persons in regular contact with them, 5) when data is necessary to pursue a legal claim; 6) with regard to employment when provided by the law, 7) for the purposes of health protection under certain conditions, 8) in relation to the data made publicly available by the person concerned, 9) when necessary for scientific researches when publication results thereof does not allow to identify data subjects, 10) in exercise of the court or administrative decisions.

18 The letter of 17 January 2011 to the Prime Minister (quoted above).

national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?

The data retained may be used for purposes of prevention and detection of criminal offences, and in relation to criminal proceedings, as well as security tasks performed by certain state agencies (ABW, CBA, SKW). The mechanism may serve the protection of intellectual property and other private law rights or interests only in case of criminalized offences.

16. Which specific requirements have to be fulfilled in order to access the data for one of the purposes mentioned in question 15 (e.g. a suspected serious crime, specific risks to public safety)?

As explained above (p.11) Polish law does not limit the access to data retained only to certain (e.g. most serious) crimes and risks to public security. The right of access of certain specialized *authorized entities* is limited to the purposes related to their scope of competences.

17. Is it required to obtain a court order before accessing the data retained? Is it required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed?

In case of prosecutors and courts the request of data access shall take a form of an order of the court or prosecutor (Art.218 § 1 of the Code of Criminal Procedure).

In case of the access by *authorized entities* the entitlement to such an access is derived from the law itself. The procedure of access to data subject to retention obligations is distinct from the so called *operational control activities*, in particular such as fixation of the content of communications. In the later case the law does provide for a court order. No such requirement is provided for in case of retained data access. In certain acts on *authorized entities* (the ABW, CBA, SKW) the requirement of a court order was explicitly excluded.[19] Instead the persons entitled to exercise the right of access within *authorized entities* are indicated by the law, and certain formal requirements are provided for. For example, in case of the Police - data should be made available: to policeman indicated in written application of Chief Commandant of the Police or district commandant of the Police, or persons authorized by them, but also on oral request or via telecommunications network to policeman who has written authorization of these persons. The parallel solution has been adopted in case of the Border Guard, the Military Police, the ABW, CBA, SKW.[20] The oral request of an adequately authorized person has not been envisaged in case of the fiscal intelligence.[21]

---

19 See respectively: Art. 28 para.1 of the act of 24 May 2002 on the Internal Security Agency and Agency of Intelligence; Art.18 para.1 of the act of 9 June 2006 on the Central Anti-corruption Bureau; Art. 32 para.1 of the act of 9 June 2006 on the Military Counter-intelligence Service and the Military Inteligence Service – all as amended by the act of 24 April 2009.

20 Respectively: Art.20c para.2 of the act of 6 April 1990 on the Police; Art. 10b para.1 of the act of 12 October 1990 on the Border Guard; Art.30 para.2 of the act of 24 August 2001 on the Military Police and military entities of order; Art.28 para.2 of the act of 24 May 2002 on the Internal Security

The law does not provide for a hearing with aggrieved party or his/her involvement in the proceedings before the data is accessed.

18. Is it provided for by law that the aggrieved party shall be notified of a data access? As a rule, does this notification have to be effected prior to or after the data access? Under which conditions is it allowed to deviate from this rule?

In case of the access by the court or prosecutor, the respective order in principle shall be delivered to addressees of the communications, subscriber of the telephone or sender whose list of calls or other communications was made available. However delivery may be postponed for a prescribed period, necessary for the proper conduct of the case, however not longer than until the final end of the case (Art.218 § 2 of the Code of Criminal Procedure).

As far data access by the Police and other *authorized entities* is concerned there are no specific provisions on notification of the aggrieved party. This is, as a disproportional limitation of the right of privacy, one of elements covered by the motion to the Constitutional Court by the group of Parliamentarians.

[The Personal Data Protection Act provide for a general obligation of the controller of data to inform a person concerned about collection of data directly after their fixation, however this duty does not apply in case of data processed under the provisions of law by state bodies and non-public entities performing public tasks (Art. 25 para.2 p.5). Also special acts provide for collection of personal data without the knowledge of a person concerned (*i.a.* the Police Act, Border Guard Act, Military Police Act, CBA Act, ABW Act, SKW and SWW Act).]

19. Does the aggrieved party have a right to be informed about the data accessed as far as they are related to him/her?

The provision transposing the Directive do not regulate this aspect. Whereas certain general standards of a right to be informed about the accessed data are provided for in the Data Protection Act[22], it is not clear how these rules work together with the

---

Agency and Agency of Intelligence (ABW Act); Art.18 para.2 of the act of 9 June 2006 on the Central Anti-corruption Bureau (CBA Act); Art. 32 para.2 of the act of 9 June 2006 on the Military Counter-intelligence Service and the Military Inteligence Service (SKW and SWW Act) – all as amended by the act of 24 April 2009.

21 Art.36b para.2 of act of 28 September 1991 on the Fiscal Control, as amended by the act of 24 April 2009.

22 General rules on personal data protection (Data Protection Act) grants to every person a right to control processing of data, which concern him/her, and are included in collection of data, including the right to information on making available of data (Art.32 para.1 p.5). This information, including on the recipients of the data and the scope of access they have been granted, should be provided by the controller, at the request of the data subject, within the period of 30 days, in an intelligible form, if so requested – in writing (Art.33 p.4). The controller shall refuse the information in particular if it would result in the disclosure of of the information constituting a state secrecy, pose a threat to national defence or security, human life and health, or public order, or to economic or financial interests of the state (Art.30 in connection with Art. 34 of the Data Protection Act).

provisions of transposing the Directive.[23] The motion of the group of Parliamentarians to the Constitutional Court raises the lack of provisions on duty to inform the aggrieved party on the accessed data, even after a closure of the proceedings, in the provisions transposing the Directive. This leads to a situation that an individual may never be informed of an access to data on him/her. The motion treats it as a deficit of the protection of privacy. The Ombudsman makes a link between the lack of duty to inform the person concerned and restriction of his/her right to court resulting from access to data retained without a court order, with conclusion that provisions in question do not respect the right to court (Art.45 para.1 and Art.77 para.2 of the Constitution).

20. May the aggrieved party have recourse to the courts for the (intended and/or already effected) data access? Which remedies do the aggrieved party dispose of? What rights does the aggrieved party have in the case of an unlawful data access or processing operation?

In case of data access by a court or prosecutor, on the basis of a court's or prosecutor's order, such an order is, in principle, subject to an interlocutory appeal to the court (Art.236 of the Code of Criminal Procedure), within 7 days of the delivery of the order. However, as explained, a delivery of an order may be postponed if it is necessary for the proper conduct of the case (see – p.18).

As regards access to retained data by the Police and other *authorized entities* no specific recourse of the aggrieved party to the court is provided for, as opposed to the case of *operational control* (ex. fixation of the content of calls).

Unlawful data access or processing would be subject to remedies and sanctions provided for in the civil, criminal and administrative law (see – p.30).

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

Operators of a public telecommunications network and providers of publicly available telecommunications services are obliged to make available the data subject to retention obligation only to *authorized entities* (the Police and other state security services) as well as to the court and prosecutor under the terms and procedure specified in separate provisions (Art.180a para.1 p.2 of the TL).

---

[23] In doctrine the view has been presented that those general rules do apply to telecommunication data covered by the TL (A.Krasucki*, Prawo telekomunikacyjne. Komentarz*, Warszawa 2010, p.592-594) Author refers to Art.5 of the Data Protection Act that declares that in case when separate laws provide for more effective protection, the provision of those laws shall apply. According to one view this provision constitute the exception from the basic principles of interpretation of law, like *lex specialis derogat legi generali* and *lex posterior derogat legi priori* (D.Adamski, *O ochronie danych w telekomunikacji*, Monitor Prawniczy 2007, No 4), while other view does not exclude application of these rules to data protection despite the Art.5 of the act (A.Drozd, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2008),

Under Art.180a para.1 p.3 of the TL the operators and providers are also obliged to protect data retained against accidental or unlawful destruction, loss or alternation, unauthorized or unlawful storage, processing, access or disclosure, in accordance with the provisions of Article 159-175 on telecommunications confidentiality and end user data protection, and Article 180e of the TL. The later provision requires application of appropriate technical and organizational measures, as well as limitation of access to retained data only to authorized employees.

22. When do the accessing bodies have to destroy the data transmitted to them?

In case of the Police, the Border Guard, the Military Police the data obtained that contain information relevant for criminal proceedings shall be transferred to the competent prosecutor. Other data shall be immediately destroyed in the presence of the committee and by the official record.[24] There are no similar solution in case of access to the data retained by the ABW, CBA and SKW, as opposed to the case of *operational control* (ex. fixation of content of calls)[25] The lack of provisions in acts on ABW, CBA and CKW concerning the duty to destroy accessed retained data that are irrelevant for their tasks has been criticized by the Ombudsman and covered by the motion of the group of Parliamentarians to the Constitutional Court.

As regards the fiscal intelligence - the information on the request of access to data retained is passed to Minister of Finance, who shall order immediate destruction of data in the presence of the committee and by the official record, in case of unjustified request.[26]

Dimension 2 (State – economy)

23. Which private bodies/enterprises (e.g. internet service providers) are obligated to retain the data? Please distinguish the group of obligated parties from providers of neighbouring services.

According to the Retention Regulation following categories of operators and providers are obliged to retain and store data: 1) operators of a fixed public telecommunications network and providers of publicly available telecommunications services provided in such networks (§ 8); 2) operator of a mobile public telecommunications network and providers of publicly available telecommunications services provided in such networks (§ 9); 3) providers of publicly available telecommunications services providing an Internet access service (§ 11); 4) providers of publicly available telecommunications services providing an e-mail service (§ 12); 5) providers of publicly available telecommunications services providing an Internet telephony service (§ 12).

---

24 See respectively: Art.20c para. 6 and 7 of the Police Act; Art.10b para. 5 and 6 of the Border Guard Act; Art.30 para. 5 and 6 of the Military Police Act.

25 See respectively: Art.27 para.15 and 16 of the ABW Act; Art.17 para. 15 and 16 of the CBA Act; Art. 31 para.14 and 15 of the SKW and SKK Act. The difference is that the data relevant for criminal proceedings are passed to the General Prosecutor. Destruction of materials that does not confirm comitment of a criminal offence is ordered by the Chief of the relevant service.

26 Art.36b para.4 and 5 of the act on the Fiscal Control.

Operators of public telecommunications networks and providers of publicly available telecommunications services whose economic activity consist exclusively of: 1) providing associated services, or 2) broadcasting or retransmission of radio or television programmes – were exempted from the Retention Regulation (§ 13).

24. Within the group of parties obligated in principle to retain data, are there some who are (by law) or may be (upon request) exempt from these obligations, e.g. non-commercial service providers or service providers with a minor turnover/market share?

No further exemptions are provided for.

25. Which of the data categories that have to be retained according to the Directive have already been retained by the obligated parties before the Directive entered into force, e.g. for billing or other business purposes or in order to comply with (other) legal obligations?

Before the entry into force of Polish provisions implementing the Directive operators of public telecommunications networks and providers of publicly available telecommunications services were obliged under Art.165 para.1 of TL to retain for 2 years processed transmission data on subscribers and end users. Transmission data are broadly defined in Art.159 para.1 p.3 as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network indicating geographic location of terminal equipment of a user of publicly available telecommunications services.

26. Are there any legal obligations on data security in place other than those mentioned in your answer to question 21 (e.g. rules on data quality, on system stability and reliability, against unauthorised destruction, loss or alteration of the data)?

No further specific obligations are provided for.

27. Which additional costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?

No such holistic and precise data are available. However the Polish Chamber of Informatics and Telecommunications, in its letter of 08.04.2010 to Minister of Infrastructure[27], estimated that costs of implementation of the Retention Regulation

[27] The letter called for additional transition period for application of the Retention Regulation until 31.12.2010. The letter is available (in Polish):

http://www.piit.org.pl/_gAllery/93/59/9359/List_retencja_2010.04.08.pdf

amount to between 2,5 and 15 Million PLN (c. 625 000 – 3,75 Million EUR) - per operator.

28. Do the obligated parties receive reimbursement for their costs by government? If so: Which costs are reimbursed (only costs for disclosure of retained data or also costs for investment into the required storage technology and/or costs to ensure data security and separate data storage)? What legal requirements have to be met for an obligated party to be eligible for cost reimbursement?

The operators and providers subject to data retention obligations shall fulfill them at their costs. Thus they are oblige to cover costs of: 1) retention and storage of the data, and their destruction after the prescribed term; 2) making available of the data to *authorized entities*, prosecutors and courts; 3) protection of the data.

No reimbursement is envisaged. In the decision of 25 March 2010 the Supreme Court made clear that costs of *making available of data (in the meaning of Art.180a para.1 p.2 of TL) cover costs of searching of data, creation of appropriate lists and sending data via telecommunications networks; such costs shall be covered by the operators or providers, and can not be included in procedural costs* (subject to reimbursement).[28]

29. What (statutory) rules are in place governing co-operation between the party retaining the data and the party (public authority) accessing them?

The law indicates the persons entitled within authorized entities (the Police, the Border Guard, the Fiscal Control, the Military Police, the ABW, CBA, SKW), to whom telecommunications entities shall make the data available, and stipulates that this process shall be performed in the absence of employees of the telecom entity or their minimal necessary presence, if such a possibility is envisaged in agreements between a chief of the authorized entity and the telecom entity. Also conditions required for making available of data via telecommunications networks are provided for by the law, namely: 1) the use of the network shall guarantee: a) possibility to identify the person obtaining the data, their category, and the time when they were obtained, b) technical and organizational safeguards preventing unauthorized persons from access to data; 2) data access via telecom networks is justified by the specificity or the scope of tasks performed by the *authorized entity* or of its activities.[29]

---

28 I KZP 37/09, OSNKW 2010/5/43.

29 Respectively: Art.20c paras.1, 2a and 5 of the Police Act; Art. 10b paras.1-4 of the Border Guard Act; Art.36b para.2, 3 and 6 of the Fiscal Control Act; Art.30 paras.2, 2a and 4 of the Military Police Act; Art.28 paras. 2-4 of the ABW Act; Art.18 paras. 2-4 of the CBA Act; Art. 32 paras.2-6 of the SKW Act – all as amended by the act of 24 April 2009.

30. Does the national law provide for any sanctions (e.g. administrative or criminal penalties) and/or obligations to pay compensation for damages suffered in case of an infringement of data retention provisions by the obligated parties? Please describe the content of these rules.

Under Art.209 para.1 p.1 of the TL any person who fails to fulfil an obligation to provide information or to submit documents provided for in the TL could be liable to administrative financial penalty. This provision could apply when an operator or provider fails to fulfil its obligations to transfer data subject to retention obligation to authorized entities.

Also a conduct of an operator infringing his duty of telecommunications confidentiality or rules on processing of data subject to this confidentiality, as well as subscriber's and end user's data – is subject to administrative financial penalty according to Art.209 para.1 points 24 and 26 of the TL. Administrative remedies and penal sanctions in case of non- compliance with provisions on data processing are also provided for in the Personal Data Protection Act.

In addition to the administrative financial penalty referred to above, the TL (Art.209 para.2) empowers the President of UKE to impose a financial penalty on a physical person in charge of a telecommunications undertaking (up to 300% of his/her monthly remuneration).

It seems also possible to apply general remedies provided for in the Civil Code, including a claim for compensation of damages (Art. 415 and f. of the Civil Code), if conditions thereof are fulfilled and proved (damage, casual link, illegality and fault). Also compensation for the moral loss (non-pecuniary damage) may be claimed, since a disclosure of personal data is treated as an infringement of personal goods (rights of personality) under civil law (Articles 23-24 and 448 of the Civil Code).

Unlawful disclosure or use of information, against the statutory duty or accepted obligation, is a criminal offence under art.266 of the Criminal Code.

As regards, unlawful operations of *authorized entities*, prosecutors and courts, as acts of public authorities, would result under the civil law in responsibility of the Treasury of the State for damages (art.417/1/ and ff. of the Civil Code).

Under the penal law such operations could constitute a criminal offence of breach of the powers (art. 231 of the Criminal Code).

Dimension 3 (State – State)

31. Which public body is responsible for establishing the contact with the party retaining the data in order to actually access that data when an entitled body (see question 14) so wishes?

The law enumerates public bodies entitled to data access (see - p.14) and indicates persons within these bodies entitled to obtain data (see - p. 17). The provisions on access to data by *authorized entities* mentions also agreements between a chief of a respective entity and a telecom entity, that may regulate the necessary presence of telecom's employees when data are transferred. Thus the overall responsibility for co-operation with telecom entities lays on the chief of the authorized public institution. The contact in a given case is established by the entitled person dealing with the case within authorized entity that requests data access.

32. Are there any regional entities (e.g. constituent states/federal states, autonomous regions or the like) vested with own authority that have been granted their own rights of access (in addition to those of the central state/federal state) to the retained data?

Poland has no federal structure. The public administration is divided into state administration and local self-government (communities). All *authorized entities* under data retention rules, as well as prosecutors and courts are state institutions.

33. What (legal) rules are in place governing co-operation among the different bodies accessing the data and between these and other public authorities (in general as well as in particular as regards the exchange of the retained data)? Have general rules of co-operation been adapted in the course of the Directive's transposition?

Under the law *authorized entities* shall transfer data relevant for criminal proceeding to the competent prosecutor. No specific provisions on cooperation between *authorized entities* or exchange of data were adopted in the course of the Directive's transposition.[30]

[30] Explicit provisions on making available to other *authorized entities* of information obtained through access to data subject to retention are included in the Fiscal Control Act, which entitles the fiscal intelligence to make this data available to duty and fiscal bodies, a court or prosecutor in relation to pending proceedings, certain state bodies, services and institutions (Art.36e).

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

Legal acts transposing the Directive do not deal with aspects of international co-operation, in particular an exchange of data with other countries. Poland has not ratify the CoE Cybercrime Convention. Under Polish provisions on data retention the list of *authorized entities* include only national state institutions, therefore any request of access by foreign state bodies could not be exercised directly, but would require the involvement of relevant national entitled bodies.

35. Which are the bodies in charge of monitoring compliance with the national rules (including, but not limited to, those on data security pursuant to Articles 7 and 9 of the Directive) by all parties involved? Do these authorities act with complete independence or do they exercise their functions under the supervision of a superior authority or ministry? Which kind of supervision is applied (comprehensive supervisory control in terms of both legality and technical advisability or supervision limited to the control of legality)?

The President of the Office of Electronic Communications (*Urząd Komunikacji Elektronicznej* - UKE) exercises controls of operators of a public telecommunications network and providers of publicly available telecommunications services within the scope of obligations referred to in Article 180a (1) of the TL (data retention, storage, making available to entitled bodies, protection), excluding obligations related to personal data protected under the provisions on personal data protection (Art. 192 p.5b of the TL). The operators and providers subject to data retention obligation shall submit to the President of UKE yearly reports on fulfillment of their duties of making retained data available to *authorized entities*, courts and prosecutors.
As far as processing of personal data is concerned the control is exercised by the General Inspector of Personal Data Protection (*Generalny Inspektor Ochrony Danych Osobowych* - GIODO), under the act on protection of personal data.
The President of UKE is a central body of state administration, appointed and dismissed by the Sejm (lower house of the Parliament) upon the request of the Prime Minister. The President of UKE reports to the Minister of Infrastructure, who passes the yearly report with his/her opinion to the Prime Minister. The administrative decisions by the President of UKE in certain cases are subject to appeal to the District Court in Warsaw – the court for the protection of competition and consumers.
The GIODO is appointed and dismissed by the Sejm, with the consent of the Senate. He/she reports to the Sejm. Administrative decisions of the GIODO are subject to appeal to the administrative court.

With the exception of reporting to the government (the President of UKE) or the Sejm (the GIODO), the possibility of dismissal and court control of decisions, both the President of UKE and the GIODO once appointed are independent bodies in performance of their statutory competences.
The controls exercised by the GIODO and the President of UKE are limited to legality. As the legal provisions on data retention contain certain obligations on data security, this may however also concern technical aspects necessary to fulfill the obligations.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

Yes. On 28 January 2011 the group of Parliamentarians submitted the motion to the Constitutional Court requesting the Court to declare that Polish provisions implementing the Directive do not conform with the Constitution. The Ombudsman sent a letter to Prime Minister questioning constitutionality of those provisions and requesting relevant changes.

If so, please answer to the following questions:

a) Who are the plaintiffs/claimants and the defendants/respondents?

The motion to the Constitutional Court was submitted by the group of Parliamentarians from the social-democtractic party (*Sojusz Lewicy Demokratycznej* – Democtratic Left Alliance – SLD). As challenged provisions were enacted by the Parliament the role of defendant-respondent is played in such cases by the Sejm.

b) Which legal norms claimed to be in conflict with the challenged law do the plaintiffs/claimants base their motion upon?

The motion covers two aspects: 1) provisions on so-called operational control in concrete cases (which goes beyond the subject matter of this study); 2) provisions on data retention – namely Articles 180a para.1 and 180c of the TL in relation with Article 20c of the Police Act, Art.10b of the Border Guard Act, Art.36b of the Fiscal Control Act, Art.30 of the Military Police Act, Art.28 of the ABW Act, Art.18 of the CBA Act, Art.32 of the SKW Act. According to the motion these provisions are contrary to the following constitutional provisions: Art.2 (the rule of law), Art.47 (right of privacy), Art.49 (communications secrecy), Art.51 para.2 and 4 (information autonomy) in relation with the Art.31 para.3 (proportionality).

c) Please describe briefly the outcome of concluded proceedings and the essential grounds of the rulings issued. Do these rulings seek to reach a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having

constitutional status? Do the rulings make reference to previous case-law that deals the legitimacy of other collections of personal data?

N.a. The case is pending.

37. Are there any lawsuits – pending or concluded by a final adjudication – with European courts (e.g. ECtHR, ECJ) concerning the legality of data retention obligations in which your Member State is/was involved (the indication of the case number is sufficient)?

N.a.

III. State of play of the application of the national law enacted to transpose the Directive

38. Where are the data stored (e.g. at the service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

The second part of legal provisions transposing the Directive into the Polish law (the Retention Regulation), became fully applicable on 1 July 2010. It is thus too early to collect experiences on the practical application.

Under the TL the data shall be stored in principle by the operators and providers obliged. However the obligation of data retention may be fulfilled by two or more operators or providers jointly. An operator or provider may also entrust another telecommunications undertaking with the performance of this obligation, by means of an agreement. This entrustment shall not release the entrusting party from responsibility for the performance of this obligation (Art. 180b of the TL). In case the obliged operator or provider ceases its telecommunications activities, its obligation of data retention shall be considered as completed if the data is submitted to another operator of a public telecommunications network or the provider of publicly available telecommunications services for further storage, making available and protection.
If obliged operator or provider was declared bankrupt, the data shall be submitted by the bankrupted party to the President of UKE for further storage, making available and protection. The method of submitting the data to the President of UKE and making this data available by him/her to entitled bodies are defined in the regulation by the Prime Minister (Art.180a paras.2 and 3).

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

Art.180a para.1 p.1 of the TL requires the retention and storage of data in the territory of the Republic of Poland.

Companies involved in the storage are obliged to conform with personal data rules provided for in the TL (Part VII) and Personal Data Protection Act.

40. Which technical and/or organisational measures ensure in practice that

As explained above, as the second part of provisions implementing the Directive became applicable recently, it is too early to collect practical experiences on application thereof, including on technical and/or organizational measures taken in practice. The responses below therefore has to be limited to measures provided for in the law**.**

a) no data are retained beyond what is permitted?

The categories of data to be retained by each category of the operators or providers are specifically defined in the Retention Regulation. The control by the President of UKE and the GIODO is envisaged.

b) where so required, the necessity to obtain a court order before accessing the data is duly observed and that State bodies otherwise cannot get access to the data (e.g. technical measures inherent to the system)? Are there any technical interfaces enabling State bodies to access the data directly (even if this may be illegal)?

As explained, a court or prosecutor's order is envisaged only in case of access by courts or prosecutors. This is not required in case of access by the Police and other authorized entities, and the lack of court control of their access to retained data is being challenged in the motion to the Constitutional Court and criticized by the Ombudsman.

c) data are not used for purposes other than those they are permitted to be used?

d) data are protected against unauthorised or unlawful (deliberate or accidental) storage, processing, access or disclosure, destruction, loss or alteration (cf. questions 21 and 26; e.g. through encryption, physical protection, application of the four-eyes principle along with secure authentication, local/decentralised storage etc)? Please describe the measures taken both by the party retaining the data and by the party accessing them.

Under Art.180e of the TL for the purposes of data protection a telecommunications undertaking shall apply appropriate technical and organizational measures and shall provide access to this data only to authorized employees.
Special conditions have to be met for making the data available via telecom networks. Such an access shall be exercised in the absence of employees of telecommunications entity and/or in their necessary presence if such a possibility is envisaged in the agreement between a chief of entitled accessing public body and the telecom entity.

e) data are destroyed safely (i.e. irrevocably) and immediately upon expiry of the retention period provided for by law?

On the part of operators and providers obliged to retain data the law provides for general obligation to destroy them after the expiry of the 2 years term, except data that were secured under separate provisions. As regards destruction of data accessed by the authorized entities the law does not provide for coherent and satisfactory solution. When data accessed by the Police, the Military Police and/or the Border Guard does not contain information relevant for criminal proceedings, the data shall be immediately destroyed by the accessing party in the presence of the committee and by the official record. However there is no external control of such a destruction. In case of other authorized entities (CBA, ABW, SKW) the relevant statutory acts do not contain provisions on an obligation to destroy data that are irrelevant for statutory tasks of those services. These elements are questioned in the mentioned motion to the Constitutional Court .

f) the aggrieved parties are notified accordingly, if this is provided for by national law (e.g. technical measures inherent to the system, specific assignment of the task to staff, cf. question 18)?

g) sensitive data (cf. question 12) are not retained or transmitted, respectively, as far as this is provided for by national law?

41. Is there an effective control that the measures referred to in question 40 are effectively applied (e.g. data protection audit, (in-house or public) data protection officer, external auditors)?

The control in relation to the personal data protection is exercised by the GIODO. The control over fulfillment by the operators and providers of their data retention obligations is exercised by the President of UKE. The responsibility for operations of *authorized entities* related to retained data access lays on the chief of the respective entity (ex. Chief Commandant of the Police).

The motion to the Constitutional Court and Ombudsman's position claim that the overall system of data retention do not contain sufficiently effective internal and external control over appropriateness of access, processing and destruction of data.

42. What technical (de facto and/or de iure) standards are applied with respect to data retention and transmission? Have the operational systems used been designed in such a way that interoperability is ensured? How is it ensured that security standards are adjusted to the current technological state of the art?

The law requires the technical measures for protection of data to be *appropriate*. The access to data by *authorized entities* through transmission via electronic network is allowed only if this network guarantees technical and organizational safeguards preventing access of unauthorized persons to the data.

43. How is co-operation between the party retaining the data and the party accessing them effected in practice? Please describe the procedure of data transmission from the retaining to the accessing party.

The procedure of data transmission from the retaining operators or provider to authorized entity is initiated by the request of entitled person within this entity. In most cases of *authorized entities* the data shall be made available: 1) to an official indicated in a written request of the general chief of the entity or the district/regional chief or the person authorized by them; 2) on oral request of the official who has written authorization of these persons; 3) via telecommunications network to the official who has written authorization of the persons. The data may be made available via telecom networks if certain conditions related to identification of the accessing person and of the data, as well as to technical and organizational safeguards against unauthorized access are met. Transmission via telecom network shall be exercised in the absence of employees of telecommunications entity or in their necessary presence if such a possibility is envisaged in the agreement between a chief of entitled accessing public body and the telecom entity. Data that are relevant for criminal proceedings shall be transmitted to the competent prosecutor; other data accessed by the Police, the Border Guard and the Military Guard, shall be immediately destroyed by the accessing party in the presence of the committee and by the official record; there is however no provisions on such obligations in statutory acts on ABW, CBA and SKW.

44. According to which procedure are cross-border requests issued or responded to, respectively? Is/are there (a) common working language(s) used in this context?

There is no special procedure for cross-border requests. It is a matter of co-operation of *authorized entities* with their foreign counterparts.

B. National (societal) context

45. In general, is society aware of the public surveillance measures adopted in your country? How are these measures assessed by citizens, economy, the government and other public bodies? Please describe the public debate on the introduction (and, if corresponding rules have existed before the Directive entered into force, also on the amendment) of data retention in your country. Please illustrate the situation as comprehensively as possible, i.e. differentiating by political and social groups (political parties, civil rights groups, labour unions as well as other professional organisations of the professions concerned (police officers, judges, lawyers/attorneys), consumer and business associations, the media, etc), and by the parties involved (businesses, data protection officers, law enforcement agencies, government representatives).

Polish legal provisions transposing the Directive were officially promulgated. Moreover there were numerous media announcements (articles, items in news programmes etc), which allowed the society to be informed about the measures introduced. The public debate related to data retention in Poland has not been as fierce as in other countries. The government raised the argument of a need to transpose the Directive. The adoption of the maximum allowed normal term (2 years) was explained in the official justification of the governmental draft by the danger of using Polish territory, due to its geographic location on the east-west and

north-south trails, as the logistic base or transit point for terrorist groups, as well as a transit route in drugs smuggling; also the fact that EU FRONTEX agency has its headquarters in Poland was raised. Interestingly, earlier the main opposition party proposed its own draft of the act transposing the directive (based on the working draft prepared within the former government formed by this party), including the term of 4 years of data retention. Moreover, at different stages even the term of 15 years was proposed with the argument that it would correspond to the basic term of prescription of criminal offences under the Penal Code.

The act amending the TL including provisions implementing the directive was adopted by the Sejm (lower house of the Parliament) with the support of all political parties, with overwhelming majority of 423 votes for 429 validly cast, with only 1 vote against and 5 abstentions.

The concern or criticism was expressed mainly by certain civil society organizations, and Internet activists. Professional organizations of telecommunications sector, also raised the human rights aspects, but mainly put the emphasis on the practical aspects, in particular financial consequences of new rules and difficulties with technical measures necessary to implement them; with this arguments they unsuccessfully proposed the postponement of the entry into force of obligations imposed on operators and providers by the Retention Regulation until the end of 2010.

Ombudsman declared his concerns with the data retention rules, send letters to the Prime Minister raising constitutional doubts and requesting amendments to provisions transposing the directive. Recently (28.01.2011) the group of Parliamentarians submitted the motion to the Constitutional Court challenging conformity with the Constitution of data retention rules and provisions on so-called operational control. The media coverage of the motion concentrated mainly on the later aspect, in particular in the context of possible invigilation of journalists.

In the public debate it is often observed that the most fundamental problems relating to data retention go beyond national law and originate from the Directive. However also certain specific problems concerning strictly the national transposition are raised, and they are addressed in the motion to the Constitutional Court and in the Ombudsman position.

46. Are there any obligations in your country to retain other personal data without a specific reason (e.g. passenger name records (PNRs), employment data, etc)?

No similar data retention statutory obligations exist. The provisions concerning retention of certain data relate to specific purpose (ex. security of mass events).

47. Are there any statistics on cases where the specific objective of a data access (e.g. the detection of serious crimes or the prevention of specific security threats) could be achieved? Are there any evaluations on the effectiveness of data retention in your country as a whole? If so: please provide the main results of the research.

No such information is available

48. Is there any information available about whether and, where applicable, how communication patterns have changed since data retention has been introduced in your country?

No such information is available. There are no apparent signs of the change of communication patterns due to introduction of data retention obligations.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

The objections have been raised about the purpose of use of the data retained, as too broad and thus doubtful as far as proportionality is concerned, and lack of sufficient internal and external control of access, processing and destruction of data. The Ombudsman in his letter to the Prime Minister requested changes in data retention provisions so as to make them in conformity with the Constitution. Amendments would include in particular: - limitation of purposes of data use to detection of the serious criminal offences specified in the law, - addition of a requirement, that information sought may not be gathered in another way; - addition of provisions protecting professional secrecy; - introduction of external control (by courts or specialized independent body) of data access, through the requirement of court order, or in a similar way; - coherent obligation of all authorized entities to destroy data irrelevant for the detection of serious criminal offences, under adequate internal and external control. In the response the Government agreed partly with Ombudsman's suggestions, namely to: - limit the purpose of access to telecommunications data only to fulfillment of tasks precisely specified in the law; - introduce the rule of destruction of data irrelevant for conducted proceedings, as regards services that are not subject to such a duty under current provisions, - consider the concept of external independent control over activities of services authorized to data access, however non-judiciary one. The Government did not share a proposal of excluding certain persons from data retention due to protection of their professional secrecy. The response announces that special working group appointed by the Prime Minister will prepare proposals of amendments in statutory acts on services authorized to data access and possibly also in the TL concerning access to data subject to telecommunications confidentiality, which will allow the appropriate legislative initiative.[31]

[31] The letter of the Secretary of State in the Chancellery of the Prime Minister – the Secretary of the Committee for Special Services, of 09.03.2011, summary (in Polish) available at: http://www.sprawy-generalne.brpo.gov.pl/szczegoly.php?pismo=1540465

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[32] **– considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?**

Privacy, personal data and secrecy of communications are explicitly protected by the Polish Constitution of 1997[33], in the following provisions:

Art. 47. 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.

Art. 49. The freedom and secrecy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute.

Art.51. 1.No one may be obliged, except on the basis of statute, to disclose information concerning his person.

2. 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.

3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.

4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.

5. Principles and procedures for collection of and access to information shall be specified by statute.

---

[32] In the following, national "(constitutional) law" means any national legal norm that (within the national legal system) is at a level superior than that of any other law (in countries with a written constitution: legal norms at constitutional level).

[33] English, German and other translations of the Polish Constitution are available at:

http://www.sejm.gov.pl/prawo/konst/konst.htm

The proportionality principle, essential in assessing the constitutionality of the statutory limitations of these rights, is declared in Art.31 para. 3 of the Constitution:

"Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights.

The protection of privacy and communication secrecy are often treated as related to the *information autonomy* of human being, linked to human dignity, which under the Constitution constitutes a source of human and citizen freedoms and rights (Art.30 para.1).[34]

The protection of the secrecy of communications under Art.49 of the Constitution covers different forms of communications (correspondence, telephone calls and other forms of communications), in respect of the content of communications[35], but also, according to doctrine, the mere fact that the communication between others took place.[36] The secrecy of communications protects all participants of communication process.[37]

Limitations of this protection are possible, in the cases and manner provided for in statutory acts, and according to the proportionality requirement.

The Constitutional Court differentiates between collection of data on individuals that are on the one hand useful or helpful for authorities and on the other necessary (essential) for protection of public interest. Only the later may pass the proportionality test.[38]

In a democratic state of law it is not necessary to store information on citizens, that has been obtained in operational activities, due to potential usefulness of such information. This may be applied only in relation to the concrete proceedings, conducted on the basis of the law allowing for limitation of freedom due to state security and public order - explained the Constitutional Court. However in the same decision it declared as compatible with the Constitution the provision of the Police Act allowing the storage of data obtained for the purpose of detecting a crime as long as they are *indispensable to the fulfillment of the statutory tasks of the*

---

34 Decision of the Constitutional Court of 17 June 2008, K 8/04. English summary available at:

http://www.trybunal.gov.pl/eng/summaries/documents/K_8_04_GB.pdf

35 W.Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Zakamycze 2002; W.Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej*, Warszawa 2000.

36 A.Bojańczyk, *Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania się*, Palestra 2003/1-2/45; S.Hoc, *glosa do uchwały SN z 22.01.2003, I KZP 45/02*, Przegląd Sądowy 2003/11-12/201; A.Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prokuratura i Prawo, 2003/10/16.

37 The Consitutional Court in the decision of 12.12.2005, K 32/04, declared as unconstitutional the provision of the Police Act that allowed for *operational control* under written consent of sender or recipient of the content of communications, without court's order. The Court explained that such a consent of only one side of communication process, does not guarantee impartial control of the Police acitivities.

38 Decisions of: 17.06.2008, K 8/04; 20.11.2002, K 41/02; 12.12.2005, K 32/04

Police, and thus even after acquittal of a person who was subject of surveillance or the discontinuation of proceedings against such a person. The court take into account that this provision refers to information collected legally (with the consent of the court), which may be instrumental to the fulfillment of the Police tasks against another person, unnecessary data should be erased and that retention of sensitive data is excluded. Given these safeguards and the circumstances of modern times (danger of organized crime and terrorism) the Court found the said norm as not exceeding the legislator's regulatory discretion determined *i.a.* by the proportionality principle.[39]

The Constitutional Court declared as contrary to the Constitution (Art.51.2 in connection with Art.31.3) different statutory provisions granting state entities such as the fiscal intelligence or the Police the competence to gather information about persons, if legislator failed to specify precisely circumstances in which that would be allowed and/or it failed to specify an exhaustive list of these types of information.[40]

Although the purpose of data retention is specified in Polish law and corresponds to the one of the purposes listed in Art.31 para.3 of the Constitution (the protection of security and public order), at least certain elements of the existing system may give rise to constitutional objections, as shown by the above letters of the Ombudsman to the Prime Minister, and the motion to the Constitutional Court by the group of Parliamentarians.

51. Under which conditions is it permitted to limit the exercise of the fundamental rights mentioned in your answer to question 50, according to national (constitutional) law?

As explained, the limitations of privacy, protection of personal data and secrecy of communications, are allowed under the Constitution, if provided for under the statutory acts, necessary in a democratic society for protection of certain values and if the essence of these rights is not violated.

52. If national (constitutional) jurisprudence has already ruled on the constitutionality/legality of the legal act(s) transposing the Directive: To which conclusion has it come? Is it possible, according to the court's opinion, to transpose the Directive in conformity with national (constitutional) law?

N.a.

---

39 Decison of the Consitutional Court of 12.12.2005, K 32/04. The English summary available at: http://www.trybunal.gov.pl/eng/summaries/documents/K_32_04_GB.pdf

40 Decisions of the Consitutional Court of: 20.06.2005, K 4/04 (fiscal intelligence); 12.12.2005, K 32/04 (Police surveillance); 17.06.2008, K 8/04 (Fiscal Control).

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

As the Constitutional Court is bound by the limits of the motion, its decisions on different surveillance measures so far has been based on an assessment of the specific provisions challenged. However the Court differentiated surveillance measures that are only potentially useful for authorities, and those necessary for specific public purposes (like state security and public order); only the later ones may pass the proportionality test. The motion to the Constitutional Court against provisions on data retention, that has been submitted by the group of Parliamentarians on 28.01.2011, questions constitutionality of specific provisions and does not relate to the whole system of surveillance measures. In its assessment of the proportionality of a given measure the Court may check to what extend the intended purpose has been already achieved with other measures, which may be of importance for the test of necessity in a democratic society of the assessed measure. The motion puts an emphasis on a different aspect, underlying that legislator has not limited access to retained data only to cases when it is absolutely necessary, but – due to broad purposes of such an access and broad discretion of the authorized entities – when it is only useful for those services. The motion also touches upon the aspect of possible infringement of the essence of constitutional rights and freedoms (Art.31 para.3 *in fine* of the Constitution), such as right of privacy, communication secrecy and information autonomy, by the existing data retention rules, due to lack of appropriate restrictions as regards the scope and procedures of interference in those rights. It remains to be seen whether and to what extent the Constitutional Court will establish in the future decision in this case more general guidelines on limits of public surveillance measures .

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

Art.51 para.2 of the Constitution makes clear that public authorities shall not acquire, collect nor make available information on citizens other than necessary in a democratic state ruled by law. There is no explicit provision on data relating to communications of mutual trust and/or covered by the professional secrecy of lawyers, doctors and journalists. The motion to the Constitutional Court and Ombudsman's position both raise this aspect, claiming that the law should provide for exemptions in such cases, due to constitutional protection respectively of the right of defense, the right of privacy and the right to information. On the other hand the Government does not share these concerns and is not willing to introduce an exemption of persons of certain professions from data retention rules. Again, it remains to be seen how the Constitutional Court will deal with this issue.

II. Dimension 2 (State – economy)

55. Does the retention obligation restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties (telecommunications and internet service providers etc)? In your opinion (based on/supported by the current state of the discussion in academia and jurisdiction, where available), are these restrictions in line with national (constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

No doubt, the data retention obligation constitutes the limitation of freedom of economic activity of operators and providers subject to this obligation. Two provisions of the Constitution are most relevant for this freedom. Under Art.20 "*a social market economy, based on the freedom of economic activity, private ownership, and solidarity, dialogue and cooperation between social partners, shall be the basis of the economic system of the Republic of Poland."* Art. 22 says that *"limitations upon the freedom of economic activity may be imposed only by means of statute and only for important public reasons".* The aspect of interference with operators' and providers' economic freedom, although raised by telecom undertakings, was less present in the public debate than the citizens' rights of privacy, protection of personal data and secrecy of communications. This may be explained by the fact that obligations imposed on operators and providers originate in the EU law.

Statutory nature of rules on data retention in the TL as well as their rationale (state security and public order as important public reasons) correspond to requirements of Art.22 of the Constitutions. The doubtful element is however that the concrete purposes of data retention has been defined in a broad and imprecise way. As data may be used in relation to any criminal offence or activity in performance of statutory duties of authorized state special services, and not only in cases of most serious criminal offences, the question arises whether public reasons justifying retention obligations which limit operators' and providers' freedom of economic activity are sufficiently important.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

Law enforcement is a task of the state. It is however not excluded that certain obligations necessary for the law enforcement or for the prevention of crimes are imposed on private actors by statutory acts, if constitutional requirements, in particular the proportionality principle, are respected (ex. obligations of the witnesses during legal proceedings).

57. According to national (constitutional) law, is it imperative to provide for reimbursement of the obligated parties for the costs incurred?

The Constitution requires a compensation in case of expropriation. There is no general requirement of reimbursement of any costs resulting from obligations imposed on private undertakings, which constitute a limitation of their economic activity freedom.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

Ratified international treaties, including ECHR, after promulgation in the Official Journal, constitutes a part of national legal order and applies directly, unless its application depends on the enactment of a statute. An international agreement ratified upon prior consent granted by a statute has precedence over statutes if such an agreement cannot be reconciled with the provisions of such statutes (Art. 91 paras.1 and 2 of the Constitution). As the ECHR was ratified upon statutory consent in 1993 and as under Art.241 of the Constitution treaties ratified and promulgated before its entry into force shall be considered as covered by Art.91, this rule apply also to the ECHR. The Constitutional Court has a power to assess conformity of statutory acts to the international treaties ratified upon statutory consent, including the ECHR; if the Court decides that the act or the provision(s) challenged do not conform to such a treaty, the act looses its binging force. The ECHR and case-law of the ECourtHR are also taken into account by the Constitutional Court in its application (and interpretation) of the Constitution.

The motion to the Constitutional Court and the position of the Ombudsman on data retention rules sent to the Prime Minister include references to the ECHR and the case-law of ECourtHR. While the Ombudsman claims that Polish provisions on data retention do not conform to the Art.8 of the ECHR, the motion to the Court was legally based, in part relating to data retention, only on provisions of the Polish Constitution, however it refers also to the case-law of the ECourtHR[41].

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

Under Art.91 para.3 of the Constitution: *If an agreement, ratified by the Republic of Poland, establishing an international organization so provides, the laws established*

[41] Judgement of 06.09.1978, *Klass and Others v, Germany*, Application No 5029/71.

by it shall be applied directly and have precedence in the event of a conflict of laws."

As under Art.288 of the TFEU Directives are binding *as to the result to be achieved (...) but shall leave to the national authorities the choice of form and method*, a Directive shall be transposed to the national law. Transposition of a Directive normally requires statutory act, enacted by the Parliament and signed by the President. Parliamentary works on an act implementing a Directive are normally initiated with a governmental draft, although also Deputies, the Senate, President and a group of 100 000 citizens have the competence of legislative initiative. In case of non-transposition or inappropriate transposition of a Directive, Polish doctrine, following the case law of the ECJ, sees the possibility of a (vertical) direct effect of a Directive granting rights to individuals vis-à-vis the state. This concept however was not specifically considered in relation to the data retention Directive.

Polish doctrine jurisprudence (both of the Constitutional Court and the Supreme Court) and doctrine developed yet before the accession to the EU the concept of so called pro-Community- (or pro-European) interpretation, which requires that in application of national legal provisions also the EU law is taken into account. In particular in case national provisions transposing a EU directive, the closest possible interpretation to the European law should be adopted.

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

Polish Constitution explicitly allows, by virtue of international agreements, to *delegate to an international organization or international institution the competence of organs of State authority in relation to certain matters.* Such an agreement require a consent for ratification in a statute adopted two-thirds majority in the Sejm and Senate; granting of consent for ratification of such agreement may also be passed by a nationwide referendum.

61. In which way have the powers regarding data retention been divided among ministries and authorities in your country? In case there are regional territorial entities (covering only parts of the country) that are vested with own powers and authorities (cf. question 32): how is competence split among the authorities of these entities and between these authorities and the authorities of the central state/federal state?

Poland has no federal structure. Powers regarding data retention belong to state authorities.The data retention, as a part of the Telecommunications Law, belongs to competences of the Minister of Infrastructure (MI). While legislative competences as regards statutory acts (like the TL) belong to the Parliament, the drafts are most often prepared by the government, and in case of the TL this task is performed by the MI. The regulation on detailed categories of data subject to retention and categories of obliged operators and providers under Art.180c para.2 of the TL shall also be enacted by the MI, in agreement with the Minister of Internal Affairs.

Supervision of application of data retention rules is performed by the President of UKE, to whom telecommunications undertakings shall submit yearly reports on making available of retained data to authorized entities (Art.180g of the TL). The President of UKE submits information based of these reports to the European Commission. The power of access to retained data has been granted to courts and prosecutors, the Police, the Military Police, the Border Guard, the Fiscal Control, the ABW, the CBA and the SKW, in relation to their statutory competencies. In case of the Fiscal Control the law provides for the supervision of data access by the Minister of Finance. In case of other authorized entities the supervision is performed by the chief of the service in question.

62. Does national (constitutional) law set any limits regarding the transmission of retained data to other countries? If so: Please describe these limits.

Polish Constitution does not directly refer to this aspect of data processing.

IV. Assessment of the overall situation

63. In your view, what options for improvement are there in your country in terms of balancing the interests of freedom and security in the context of data retention?

At the present stage there are no official, known concrete proposals for improvement of data retention rules. However taking into account the motion by the group of Parliamentarians to the Constitutional Court and the position of the Ombudsman partly shared by the Government it is likely that certain solutions will be proposed. Possible improvements, aimed at removing objections raised so far, could include: 1) limiting the purposes of access to data to serious listed criminal offences, so as to make the rules coherent with their official justification, the directive and the proportionality principle; 2) the requirement that the access to data is authorized only if information sought may not be obtained in another, less intrusive, way; 3) providing for an external control (in the form of an order by the court or other independent authority) in case of access by *authorized entities* (as in case of access by courts themselves under present rules); 4) providing for a coherent rules on destruction of data that are irrelevant for the statutory purpose of access; 5) the obligation to inform a citizen concerned on data access (possibly subject to certain restrictions related to good conduct of proceedings); 6) possible exemptions of communications covered by legally protected confidentiality (lawyers, doctors, journalists). This would not however remove the most fundamental concerns raised by certain civil society organizations and Internet activist, relating to threats to privacy and secrecy of communications resulting from the data retention mechanism as such, that could be only resolved on the EU level.

Balancing the interests in the context of data retention (INVODAS)

Poland

Krzysztof Wojciechowski

Part 2: Overarching issues and country-specific questions

A. General part (Questions to the experts in all Member States)

1. Does national (constitutional) law provide for a right to communicate *anonymously*?

The freedom and secrecy of communications is protected under Art.49 of the Polish Constitution and related to the right of privacy (Art.47) and the information autonomy (Art.51). This protection covers not only the content of the communications, but also the integrity of communications (in the sense that it is not altered by the third party), as well as according to doctrine, the mere fact that a communication between certain persons took place. Consequently, if an individual chooses to communicate with another person anonymously, disclosure of his identity may be treated as a violation of his/her secrecy of communications.

Under the constitution the secrecy of communications may be limited in cases and in a manner specified in the statutory act. Thus disclosure of identity in case of anonymous communications is not impossible if provided for by the law in line with the proportionality principle.

2. **Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country.[1] How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?**

In the Report on retention of telecommunication data published on 05.07.2011 the Government proposed a number of changes to existing rules on data retention and on access to such data.[2] It is a governmental response to numerous initiatives questioning existing data retention rules, including steps taken by the Ombudsman, the motion to the Constitutional Court by the group of Parliamentarians, activity of civil society and human rights organisations.

The Ombudsman in the letter of 17.01.2011 to Prime Minister questioned constitutionality of these provisions and requested changes thereof, without however proposing concrete amendments, but identifying shortcomings of current provisions and in that way suggesting general directions of necessary changes. In order to eliminate objections raised by the Ombudsman in particular the following amendments would be needed:

- the purpose of data access and use should be limited to detection of serious criminal offences listed in the law;

- data access should be possible only if the information sought may not be obtained in another, less intrusive way;

- provisions on protection of professional secrecy (lawyers', doctors', journalists') should be added;

- data access by all authorised entities should be made subject to external control, through the obligation to obtain a court order or similar independent judgment;

- all authorised entities should be obliged to destroy data irrelevant for the statutory purpose of data access (detection of serious listed criminal offences) and internal and external control mechanisms should be provided for such a destruction.

First, the government in its response (of 11.03.2011) agreed only with small part of Ombudsman's arguments. In general, the government saw data retention as a less intrusive mean among restrictions of the right of privacy than the operational control

[1] This question aims at getting an update to your answers to the first questionnaire (in particular, to questions 49 and 63).

[2] http://bip.kprm.gov.pl/kprm/komunikaty/281_4067.html

(ex. fixation of telephone calls). Consequently the government did not believe that the same level of protection (and thus the same procedural guarantees) should apply to both cases, and in relation to data retention more flexible rules are possible, i.a. the requirement of court order is not necessary. The response said that Ombudsman's suggestion on the external control of access to data retained by other (non-judiciary) independent body is interesting and should be considered. The government found that it is impossible to exclude persons whose activity is protected by the professional secrecy from data retention rules. Such a solution is not necessary as data retention does not lead to disclosure of content of communications that is a real subject matter of the secrecy. The government agreed to limit the purpose of access to data only to fulfilment of tasks specified in the law and to provide for an obligation of all authorised services to destruct data that are irrelevant for pending proceedings.

The special governmental working group was appointed to prepare legislative solutions for more rigid control over services accessing the telecommunications data.

The Governmental Report of 05.07.2011 is the first result of these works. In general, it upholds the position, that statutory data retention regime is indispensible for investigation and prosecution of serious crimes. However, in the same time the report confirms the need for a major reform of Polish data retention rules in order to limit interference of state organs with privacy of citizens and strengthen the control over state special services. Consequently it proposes a number of concrete measures:

1) shortening of the term of data retention to one year;

2) limitation of retained data usage only to serious criminal offences: punishable by custodial sentence of a maximum period of at least three years or committed with the use of electronic communications means; with regard to courts access would be allowed also in case of other criminal offences if proving of a given fact by other evidence is impossible or specially difficult; access by special services would be limited to their specific, listed tasks instead of general statutory remit;

3) creation of further control instruments;

4) strengthening of supervision by the public prosecutors;

5) introduction of a duty to destroy unnecessary data;

6) making publicly available of the statistics on the use by each state organ of the data subject to telecommunications confidentiality.

It is also proposed to limit the definition of the telecommunications confidentiality, so as to exclude personal data of subscribers, which should be protected rather by personal data protection rules.

In order to strengthen the control, the report proposes an appointment of plenipotentiaries for the protection of personal and telecommunications data in each entity authorized for access the retained data. A plenipotentiary would be appointed by the head of a given entity, but - as a guarantee of independence – could not be dismissed without a consent of a supervisory authority. Public prosecutors would be broader informed on access to telecommunications data by the authorised entities.

It is proposed to provide for an absolute obligation for authorized entities to destroy data that are useless or are not anymore useful for the intended purpose, as well as an obligation of telecom operators to destroy data after the end of the retention term. Also additional rules on the protection of retained data against unauthorised access by the third parties are planned.

Moreover authorized entities should be obliged to make statistics on accessed data publicly available. Such statistics would include overall number of requests to operators, number of billings, number of localisation assessments, number of persons who were subject of activities connected with access to telecommunications data.

The report proposes also creation of a new independent supervisory body for the control of activities of special services competent also in the field of their access to retained data. The body would consist of 6 members, appointed by the Sejm (lower house of the Parliament) for 6 years term of office, possibly with 3 members rotating after 3 years. The Chairman and Vice-chairman would be judges with at least 10 years of practice in criminal cases. Members of the body would have to fulfil special conditions guaranteeing their independence and professionalism. The tasks and competences of the body would include also handling the complaints from citizens concerning special services activities. The body would report to Sejm, but could also present its findings to the Prime Minister, ministers and heads of special services, requesting explanations. The governmental report however does not specify in detail the role of the body in access by authorised entities to retained data.

As the competences of the new body would be limited to control over special services the report proposes to consider a creation of a similar body for supervision of police services.The governmental report, together with the debate on the European Commission report on data retention directive, accelerated the public discussion on possible revision of data retention rules. The motion to the Constitutional Court, the Ombudsman's letter, the governmental response and information on large scale of data access have been noted by the media, with the main emphasis on possible invigilation of journalists. The governmental proposals try to respond to the growing criticism towards data retention regime and its application.

The report of 05.07.2011 was received as a step in the right direction, in particular in terms of limiting the scope of discretion of authorized entities in access to and use of retained data and making available of statistics. However a number of issues met with criticism. The proposal to limit the purpose of data retention was commented as insufficient, as still the category of criminal offences punishable by

custodial sentence of a maximum period of at least three years is very broad. Commentators also noticed that there is no proposal for a duty to inform a person concerned about access to his/her telecommunications data.

Data retention is one of issues discussed by the government with non-governmental organisations within the context of regulation of the Internet. Certain civil society organisations and Internet activist raise fundamental doubts about data retention rules questioning their legitimacy on both European and national level, highlighting that there is no evidence of necessity of those rules, as opposed to the their usefulness for security service which however is not sufficient to restrict the right of privacy. Under this view data retention is unnecessary as it would be sufficient to use data stored for commercial reasons (billing purposes). German, Romanian and – recently – Czech decisions by respective constitutional courts are quoted, with the argument that Polish data retention provisions are even more far reaching. On the other hand the motion to the Constitutional Court against data retention provisions and Ombudsman's position concentrate rather on specific shortcomings of existing rules, and do not question the whole data retention system as such. Recent governmental proposals from the point of view of supervision over special services may be seen as a major reform, however in relation to data retention the proposals are rather cautious and do not reveal the will for fundamental revision, but clearly show that data retention regime will be defended, subject to adjustments aimed at resolving most manifest constitutional objections.

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

General obligations of co-operation with public authorities in the detection, investigation and prosecution of criminal offences, include in particular duty to inform about commitment of a criminal offence, a duty to testify as a witness, a duty to deliver objects that may serve as a evidence or are subject to sequestration as a security for financial penalties, a duty of assistance to organs conducting a criminal proceedings. Each of these means requires further explanation.

As far as duty to inform about the commitment of a criminal offence (duty of denunciation) is concerned, the universal and special (only of listed subjects) duty should be distinguished. As regards the universal duty there is a legal duty and citizens'- societal (non-legal) one.

The universal legal duty, provided for in Art.240 para.1 of the Criminal Code (*Kodeks Karny - KK*), concerns only those who have a reliable piece of information about punishable preparation, attempt and/or commitment of certain listed most serious criminal offences (genocide; crimes against humanity; war crimes; *coup d'etat*; violent attempt against constitutional state organs; espionage; attempt against the life of the President of Poland; terrorist attempt; homicide; causing the incident threatening the life or health of many persons or enormous damage; piracy in water

or air transportation; imprisonment; human trafficking; hostage taking; crimes of terrorist nature). Persons who have such information shall immediately inform a body competent for investigating criminal offences. Criminal responsibility of a person who fails to fulfil this duty is exempted in case he/she has sufficient grounds to believe that the state body knows about a given offence and also in case of an apprehension of criminal responsibility of the person concerned or a person proximate to him/her. The legal duty of denunciation (Art.240 KK) does not apply to an attorney-at-law who obtained a given piece of information when providing a legal assistance and a priest who heard about the criminal offence during confession; however it applies to journalists and doctors, as the duty provided for in Art.240 KK has a priority over journalistic and medical secrecies.[3]

Art. 304 para.1 of the Code of Criminal Procedure (*Kodeks Postępowania Karnego – KPK*) provides for a societal (citizens'), but non-legal, duty to inform a prosecutor or the Police about commitment of a criminal offence prosecuted *ex officio*. There is no criminal sanction in case of non-compliance with this duty. The legal duty of denunciation of other criminal offences than referred to in Art.240 KK applies only to state and local self-government institutions, which in relation to their activities got known about a commitment of an offence prosecuted *ex officio* (Art.304 para.2 KPK).

Special duty of denunciation concerns specific persons or entities, in a specific context. The duty of this type is provided for in the Act of 16 November 2000 on counteracting money laundering and financing of terrorism (consolidated text: Dz.U. of 2010, No 46, item 276), which implements the Directive 2005/60/EC on the prevention of use of the financial system for the purpose of money laundering and terrorist financing (that replaced the Directive 91/30/EEC amended by the Directive 2001/97/EC) – the Money Laundering Directive. The Anti-Money Laundering Act obliges listed subjects (ex. banks, financial institutions, notaries and lawyers)[4] to register transactions in principle of value exceeding 15 000 Euro, analyse transactions, apply means of financial security on the basis of the risk evaluation[5], and to inform the General Inspector of Financial Information (*Generalny Inspektor Informacji Finansowej – GIIF)* about registered transactions, as well as to inform GIIF about planned transaction, which raises a justified suspicion that it may serve money laundering or terrorist financing.

---

3 L.Gardocki, *Prawo karne*, Warszawa 2008, p.294.

4 The list of obliged subjects includes in particular credit institutions, banks, institutions of electronic money, investment firms, entities performing broker's activity, certain hazard games entities, life insurance companies, investment funds and their societies, public post operators, notaries, attorneys-at-law, legal advisers, licensed auditors, tax advisors, providers of accounting services, *bureau de change* providers, auction houses, antiquarians, factoring enterprises, noble metals and stones enterprises, real-estate agents, foundations, associations and entrepreneurs receiving payment in cash exceeding 15 000 Euro. Not all the duties provided for by the Anti-Money Laundering Act apply equally to all obliged subjects, ex. lawyers are exempted from some duties.

5 Means of financial security include in particular: an identification and verification of an identity of a client; due diligence duties in identification of the beneficiary and verification of his/her identity; obtaining information on intended purpose and nature of client's business relations; monitoring of these relations.

Another special duty of denunciation is provided for in Art.12 of the Act of 29 July 2005 on counteracting of violence in a family[6], that obliges every person, who within performance of his/her professional duties (ex. teachers, nurses, doctors) got a suspicion of commitment of a prosecuted *ex officio* criminal offence with the use of violence in a family to inform the Police or a prosecutor. All persons being witnesses of violence in a family are obliged to inform the Police, a prosecutor or others entities counteracting the violence in a family.

There are also special duties of denunciation of different institutions (public or private) performing public tasks, for example: organs of Environment Protection Inspection when they assess that criminal offence against the environment has been committed are obliged to notify organs of investigation[7], a rector of an academy is obliged to notify such organs about commitment of criminal offence of plagiarism by a student[8], etc.

As regards the duty to testify as a witness, codes respectively of criminal, civil and administrative procedure oblige in principle each person called as a witness to be present and to testify. Further remarks refer to criminal procedure, as it applies in relation to criminal offences. Persons that are proximate[9] to the accused person and persons that are accused in another proceeding on participation in the same criminal offence may refuse to testify. A witness may refuse to answer the question if response could expose him/her or a proximate person to criminal responsibility. It is forbidden to interrogate as witnesses attorneys-at-law representing accused persons in criminal cases - concerning the facts known by them due to provision of a legal advice or handling with a case, and priests - concerning facts revealed to them during confessions. Persons obliged to keep the professional secrecy, may refuse to testify on circumstances covered by this secrecy, unless a court or a prosecutor releases them from a duty to keep it.

A duty to deliver certain objects is provided for in Art. 217 and f. of the KPK. There is an obligation to deliver objects that may constitute an evidence in proceedings or that may be retained as a security of financial penalties, pecuniary penal means and/or reparation of damages, upon the request of a court or a prosecutor, and in urgent situations also of the Police or other authorised entity. In the later case a person concerned may request an order of a court or prosecutor approving the retention; such an order shall be delivered in 14 days. In the case of refusal of voluntary delivery of those objects, they may be compulsory taken away.

The special duty of delivery (Art.218 of the KPK) refers to authorities, institutions and entities conducting an activity in field of post and/or telecommunications,

---

6 Dz.U. of 2005, No 180, item 1493 with amendments. The act has been significantly revised in 2010, including Art.12.

7 Art.15 of the Act of 20.07.1991 on Environment Protection Inspection, consolidated text: Dz.U. of 2007, No 44, item 287, with amendments.

8 Art.214 para.6 of the Act of 27.07.2005 Law on Academic Education, Dz.U. No 164, item 1365.

9 Husband or spouse, ascendant, descendant, brother or sister, relative in the same line and degree, person in adoption relation and her husband or his spouse, life partner (Art.120 para.11 of the KK).

customs offices, as well as transport enterprises. They are obliged to deliver to a court or a prosecutor, at the request in the form of an order, correspondence, dispatches, data subject to retention obligation under the Telecommunications Law (TL), if these are relevant for the pending proceedings. Only a court or a prosecutor are authorised to open them or command to do so. A court's or prosecutor's order shall be delivered to addressees of correspondence and to subscriber or sender, whose list of calls or other communications has been accessed. Delivery of the order may be postponed for a limited time, necessary for a good conduct of the case, and not later than until final closure of the case. Correspondence and dispatches irrelevant for the criminal proceedings shall be immediately return to appropriate institutions or enterprises.

In addition, the law provide for a "quick freeze" duty of authorities, institutions and entities conducting a telecommunications activity (Art.218a), that was introduced in 2004 as an implementation of Articles 16 and 17 of the Council of Europe Cybercrime Convention, although Poland has not ratified it yet. Those entities are obliged to immediately secure, at the request of a court or a prosecutor in the form of an order, for the limited time, not exceeding 90 days, computer data in pieces of equipment that contain these data on the carrier or in computer systems. Data irrelevant for proceedings shall be released from security preservation. Technical methods of preparation of systems and networks to collect those data (other than telephone calls or other communications), as well as methods of securing computer data are determined by the regulation of the Minister of Justice in agreement with Minister of Infrastructure, Minister of Defence and Minister of Interior.

Last but not least, the law provides for a general obligation to provide an assistance at the request of organs conducting criminal proceedings, if otherwise a given act of proceedings is impossible or significantly more difficult (Art. 15 para.3 of the KPK[10]). Such a duty lays on the legal persons, entities without legal personality and physical persons. The entity which conducts preparatory proceedings are: the Police (in case of an inquiry – *dochodzenie*) and a prosecutor (in case of an investigation – *śledztwo*), who may however delegate the whole or parts of proceedings, or specific acts thereof to the Police. Also the Border Guard, the Military Police, the Agency of Internal Security (ABW) and the Central Anticorruption Burreau (CBA) have the rights of the Police, however only within their respective competencies. Although a duty of an assistance is not limited as regards its extend and there are no explicit exclusions of certain entities and persons, the doctrine assumes that other rules of the criminal procedure apply also to that duty. In effect, as the universal duty of denunciation covers only listed most serious criminal offences (see above), the view is presented that an active role of private actors in investigations within an assistance duty should be limited accordingly. Also persons who may refuse to

[10] The provision in question has been amended and extended in 2007. Before it covered state, self-government and social institutions. Currently these institutions are still covered by the duty, without the requirement of an impossibility or an obstruction of proceedings without the assistance requested.

testify or may not be interrogated as witnesses are deemed to be excluded from the assistance duty.[11]

The duty of assistance may take a form of provision of information. In case of information specifically protected (ex. bank confidentiality), the special provisions regulate duties related to making it available to public authorities. For example banks are obliged to provide information subject to bank confidentiality in particular to: a court or a prosecutor in relation to proceedings concerning a criminal offence or fiscal criminal offence, or in relation to request of legal assistance from another state on the basis of a ratified international treaty; the General Inspector of Fiscal Control in relation to criminal or fiscal criminal cases; the Police, the Chief of the CBA – when necessary for effective prevention and investigation of listed criminal offences and subject to a court's order; customs service - in relation to proceedings concerning fiscal criminal offence.[12] A similar solution exists with regard to insurance companies, as far as information subject to confidentiality of insurance agreements is concerned.[13]

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

The KPK grants the accused person the right to refuse to answer some questions or to submit any explanations (Art.175 para.1). Persons proximate to the accused person may refuse to testify as witnesses (Art.182 para.1 KPK). The same right is granted to a witness, who is accused in another case on co-commitment of the criminal offence covered by given proceedings (Art.182 para.3 KPK). A witness may refuse to answer a question, if this could expose him/her or a person proximate to him/her to a liability for a criminal or fiscal criminal offence (Art.183 para.1 KPK). It is forbidden to interrogate as a witness an attorney-at-law acting as a counsel for the defence with regard to the facts that he/she got to know providing a legal advice or dealing with the case, and a priest with regard to the facts that he got to know during a confession (Art.178 KPK). Persons who are obliged to keep a secrecy may refuse to testify as regards facts covered by a secrecy in question, unless a court or a prosecutor releases them from a duty to keep a secrecy (Art.180 para.1 KPK). An additional rule is provided for persons obliged to keep a notary's, attorney-at-law's, legal adviser's, tax adviser's, medical or journalistic secrecy.

---

11 J.Grajewski, L.K.Paprzycki, S.Steinborn, *Kodeks postępowania karnego. Komentarz*, Vol. I (Articles 1-424), LEX 2010, Art.15, Nb 12.

12 Art.105 of the Act of 29.08.1997 the Bank Law, consolidated text: Dz.U. of 2002, No 72, item 665.

13 Art.19 of the Act of 22.05.2003 on the insurance acitivity, consolidated text: Dz.U. of 2010, No 11, item 66.

These persons may be interrogated with regard to a fact covered by the secrecy only if this is essential for the good conduct of justice, and the fact may not be discovered on the basis on another evidence (Art.180 para.2 KPK). Journalists may not be released from a duty to keep a secrecy as regards data that allows identification of an author of an editorial material, a letter to an editor or other material of similar nature, as well as identification of persons providing information for publication, if these person reserved non-disclosure of such data. This rule however does not apply to information concerning a criminal offence that is subject to the universal duty of denunciation (see above – p.3), i.e. the most serious offences against the state, security, life, as well as terrorist criminal offences (Art.180 paras 3 and 4).

Exceptions concerning a duty to testify are deemed to apply also to a duty to deliver an object (Art.217 KPK; see above – p.3) and a duty to assist organs conducting criminal proceedings (Art.16 para.3 KPK; see above – p.3).

The rules on refusal to testify or deliver an evidence against the person concerned, may also apply to facts, which are covered by the data subject to retention under the TL. There is however no provision that would exclude application of provisions on data retention and access, with regard to data concerning persons who have the right to refuse to testify or deliver an evidence against themselves or against those in special relationship of confidence. It seems also difficult, in the lack of explicit specific provisions, to draw from the mere general rules of criminal procedure the conclusion that this right to refuse prevails over data retention and access rules. Apparently, the motion to the Constitutional Court against the data retention provisions and the position of the Ombudsman are based on a similar assumption, as they both question the lack of special treatment under Polish data retention rules of data concerning persons that are obliged to keep professional secrecy (lawyers, journalists, doctors).

5. Where/how are data, that have been requested by entitled bodies, stored by these bodies once obtained? What measures have to be taken by these bodies in order to safeguard data protection and data security?

Provisions added in the course of implementation of the data retention directive to the statutory acts on respective *authorised entities* entitled by law to access data subject to retention (the Police, Border Guard, Military Police, Fiscal Control, ABW, CBA, SKK) do not determine where and how retained data once obtained by this entities should be stored. With regard to the Police, Border Guard and Military Police relevant acts provide for that documents (obtained within an access to retained data), which include an information relevant for a criminal proceeding, are transferred to a competent prosecutor, while other documents shall be destroyed in the presence of the committee and by the official record. In case of the Fiscal Control the Minister of Finance orders immediate destruction of the data obtained, if the request for access has been deemed unjustified. The provisions on access to retained data in acts on the ABW, CBA and SKK do not explicitly regulate the further use of the data and destruction of data irrelevant for statutory purposes of those services – which is challenged in the motion to the Constitutional Court and in

the Ombudsman's position. The governmental report of 05.07.2011 proposes to provide for an absolute duty to destroy useless data that have been accessed.

General duties of data controllers to safeguard personal data are provided for in the Personal Data Protection Act (Articles 36-39). The controller is obliged to implement technical and organizational measures to protect the personal data being processed, appropriate to the risks and category of data, and in particular to protect data against their unauthorized disclosure, takeover by an unauthorized person, unlawful processing, any change, loss, damage or destruction. The documentation describing the way of data processing and measures to protect personal data shall be kept. The controller is obliged to appoint an administrator of information security who supervises the compliance with security principles, unless the controller performs these activities by himself. The processing of data may be carry out exclusively by authorized persons. The controller is obliged to ensure supervision over access and transfer of data. Technical and organizational means of protection of processed data are determined in the regulation by the Minister of Interior and Administration[14]. Under the regulation the documentation on data processing and protection consists of a policy of security and guidelines of administration of computer systems in which data is processed. A policy of security includes in particular a list of buildings, rooms or parts thereof where the data is processed, a list of personal data collections, a way of transfer of data between systems, technical and organization means to safeguard confidentiality, integrity and accountability of processed data. Guidelines of administration include i.a. a way, place and term of storage of electronic carriers of information that includes personal data. There are three levels of security of personal data processing, depending on a category of data and a danger level: 1) basic (no sensitive data, no connection to a public network), 2) enhanced (sensitive data included, but no connection to a public network), 3) high (if at least one piece of equipment, that serves to process personal data, is connected to a public network). The appendix to the regulation determines the means of security for each level.

The acts on respective *authorised entities* (to access retained data) include more specific provisions on collection and processing of information, including personal data, for the purposes of their respective statutory tasks. Detailed rules are determined in regulations. For example the Police is authorised to gather, obtain, collect, process and use for the purposes of fulfilment of statutory tasks information, including personal data, on persons suspected of commitment of a criminal offence publicly prosecuted, about persons of unknown identity or seeking to hide their identity, and about persons wanted – also without their knowledge and consent. This information may include *i.a.* information on the methods of activities of a perpetrator, his/her social circle and contacts.

[14] The regulation of the Minister of Interior and Administration of 29 April 2004 on documentation of personal data processing as well as on technical and organizational conditions with which equipment and computer systems, which serve personal data processing, should comply, Dz.U. of 2004, No 100, item 1024.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

There are no complete official statistics on the transmission of retained data to the authorised entities.

On the basis of reports delivered to the President of UKE by telecom operators it was estimated that in 2009 those operators transmitted responses to 1 060 000 requests from authorised state institutions[15].

Further enquiry conducted on behalf of the government by the Minister – Coordinator of Special Services, the results of which were made public in the beginning of 2011[16], led to the general conclusion that in practice requests concern most often subscribers data, lists of calls (billings) and localisation of mobile phones. The enquiry concerned the amount of requests in 2009 and in part of 2010 (only January-October was covered) by each authorized entity. However statistic data on requests to access retained data were not collected by all authorized entities. In case of courts, prosecutors and the Police it proved impossible to obtain such statistics, as information is included only in the files of proceedings in specific cases. The data delivered by remaining six authorised entities allowed to estimate the amount of requests by each of them.

In 2009 (in thousands): the Border Guard – 163; the Military Police – 1,3; Fiscal Intelligence – 4; ABW – 138; CBA – 45; SKK – 113. Together all six services: c. 464. On this basis it was estimated that within 1 060 000 requests in 2009 noted by the UKE (following the reports of telecom operators) c. 56% were deemed to be made by courts, prosecutors and the Police, 15% by the Border Guard, 13% by the ABW, 11% by the SKW, 4% by the CBA, 1% by the Fiscal Intelligence.

In the whole period covered by the enquiry (22 months: from 01.01.2009 to 31.10.2010): the Border Guard – 298 (thousand of requests); ABW – 266; SKW -

---

15 This information was presented by the press; see: *Gazeta Wyborcza* of 09.11.2010, E.Siedlecka, *Nasze bilingi i internet pod lupą służb*, available:

http://wyborcza.pl/1,75478,8634123,Nasze_billingi_i_internet_pod_lupa_sluzb.html

It was also presented on the website of the civil society organisation *Panoptykon*, active i.a. in data retention debate:

http://www.panoptykon.org/content/milion-zapyta-o-dane-retencyjne

16 The results of governmental enquiry are made available at the *Panoptykon's* website:

http://www.panoptykon.org/sites/default/files/Material_Cichocki_sprawdzenia_luty2011.pdf

It was also covered by media; for example see:

http://wyborcza.pl/1,75478,9081579,Sluzby_zdradzaja__jak_czesto_siegaly_po_billingi.html

http://tech.wp.pl/kat,1009781,title,O-co-sluzby-specjalne-pytaja-operatorow,wid,13119164,wiadomosc.html#czytajdalej

207; CBA – 84; Fiscal Intelligence – 8; Military Police – 4; in total: 867 (without courts, prosecutors and the Police).

As regards the category of data requested, the enquiry shown that requests of the six (among 9) authorised entities in the period covered concerned: in 54% - data identifying subscribers, 34% - lists of calls (billings), 9% - localisation of a mobile phone, 3 % - other data (ex. redirection of calls, IMEI numbers, etc.).

The enquiry shown the need to collect statistics on requests concerning data subject to retention under coherent methodology by all authorised entities, which is announced in conclusions of the governmental analysis, and also proposed in the governmental report of 05.07.2011.

The estimates presented above should be treated with caution. They are neither complete, nor do they contain fully comparable data. They cover period that does not correspond to the entry into force of data retention provisions transposing the Directive. They cover all requests on telecommunications data, including those concerning categories of data which would be in large part accessible independently of data retention rules (subscriber identification). Requests concerning ex. mobile telephone subscriber identification, are normally directed to all operators of such services while only one may lead to data access. Thus the numbers emanating from the estimates above may not exactly illustrate the effects of implementation of the Directive on data retention. More time is needed to collect complete and reliable statistics.

However, even taking into account all necessary reservations to available estimates, they show the large extend in which access of state services to telecommunications data has been used in Poland. In the public discussion the link has been made between numbers emanating from these estimates and the low threshold of legal requirements to obtain access to retained data (broad purpose of access; lack of sufficient internal and external control, ex. no court order). It remains to be seen whether more complete and reliable statistics will confirm this tentative conclusion.

B. Questions to the experts from only some of the Member States

7. Please give your own opinion on the constitutionality of the data retention regime in your country as a whole.

Data retention regime in Poland as a whole raises serious constitutional concerns. The mechanism of keeping and making available to state services detailed records of facts of individuals' communications (even without records of content thereof), constitute an invasion in the right of privacy, secrecy of communication and information autonomy of an individual. Data retention constitutes a heavy burden for telecom enterprises limiting their freedom of economic activity. The mechanism, to the extent it leads to possible access to information covered by legally protected professional secrecy, also interferes with the right of defence (lawyers' secrecy), the right of privacy in the field of personal health (medical secrecy) and the freedom of expression (journalistic secrecy). Constitutional rights and freedoms that are

touched by data retention mechanism are not absolute ones. They may be subject to limitations, if provided for by a statutory act, for public purposes, if the principle of proportionality is fulfilled and if the essence of the right or freedom is not neglected. Not all of these requirements are met by Polish provisions on data retention. The regulation has a statutory nature and serves the public security and order, which are the purposes justifying the limitation of constitutional rights and freedom. However, Polish data retention rules fail to comply with the proportionality principle. The mere necessity of these rules, highly burdensome for obliged operators and providers, and highly intrusive in citizens' rights and freedom, is questionable. While certainly there are many indicators, including (incomplete) statistics on extensive use of this mechanism by authorized entities, illustrating that data retention is useful for their activities, it is not equally certain whether the mechanism is essential and irreplaceable for the declared purpose i.e. detection, investigation and prosecution of serious crimes, and – moreover – whether the results of this regime outweigh the burden it places on the citizens and economic actors. Retention of data for billing purposes and quick freeze preservation constitute to certain extend an alternative to data retention, although these instruments do not guarantee availability of historic data, that might be necessary in certain situations. It remains to be proven with empirical evidence to what extend this added value of data retention justifies existence of this burdensome mechanism. The current statistics, partly due to late implementation of the Directive in Poland, do not allow the assessment in this regard. In these circumstances it seems premature either to exclude the necessity of any regime of data retention or confirm a need for it. However, under the established Polish constitutional case-law there are several concepts that could be important in assessment of constitutionality of mere existence of data retention mechanism as such: 1) the presumption of constitutionality of existing law, 2) concept of favourable attitude towards EU law in interpretation of national law (in particular implementing EU law); 3) approved necessity for additional instruments of public security and order in modern times, as technical means allowing the faster communication and movement are often used for criminal activities and new dangers for democratic society (ex. organised crime, terrorism) exist. Given that data retention originates in EU law, exists in most EU Member States, is deemed necessary by their authorities, and even in those countries where the implementing laws have been declared unconstitutional Courts have not excluded possibility of such a transposition of the Directive that would meet constitutional standards, it would seem too far reaching at this stage to assume that any data retention regime *per se* is unconstitutional.

However, as such a regime is very intrusive in constitutional rights and freedoms, and burdensome, it should remain strictly limited and include special guarantees, that exclude discretion of state authorities and secure protection of citizens, in terms of substantial and procedural legal provisions.

The purpose of data retention and access in Poland is too broad. It is not limited to detection, investigation and prosecution of serious crime, but includes prevention and detection of any criminal offences or in case of special services goals related to tasks of those services. Therefore the whole regime is not strictly limited to its declared purpose.

Moreover the access to retained data is not limited to situations where there are no other less intrusive means of obtaining sought information. Thus such access may be obtained wherever deemed useful for authorized entities within their broadly defined tasks, and not only when really necessary in fight against serious crime. The argument that data retention relates to the mere facts of communications and not their contents, and is less intrusive than fixation of calls and other control of content of communications, and thus do not require equally strict guarantees, do not justify such an omission. In each assessment of (non)availability of less intrusive means this element (level of intrusiveness of access to retained data in comparison with other means) could be well taken into account.

One of the most manifest problems with regard to Polish data retention rules is lack of sufficient internal and external control of access to retained data by authorized entities (except access by courts and prosecutors). In particular there is no requirement of the court order to access data, as opposed to the case of control of content of communications and access to information from banks or insurance companies. Again the argument about the lesser intrusiveness (than in case of control of communications content) is not convincing, because information on financial situation (subject to a court order) could be less intrusive from the point of view of the right of privacy than the data relating to facts of communications with certain persons or presence in certain places. Moreover, it is difficult to understand why in case of courts and prosecutors, i.e. authorities of high level of independence and professional (including ethical) standards there is a guarantee of formal order, while in case of state security services subordinated to the government this is not the case. Independent external control of access to retained data is absolutely indispensable to fulfil proportionality requirement. The most natural solution in Polish legal system would be the court order. The lack of such an external control combined with excessively broad purpose of data access, results in constitutionally unacceptable discretion of authorized entities in access to the retained data.

Also guarantees of destruction of data accessed without the valid grounds or data that proved to be unnecessary are not sufficient and coherent (for all authorized entities), which is in details described in another point.

The lack of sufficient guarantees of respect for legally protected professional secrecies related to relationships of trust and necessary for protection of such constitutional values as the right of privacy (medical secrecy), right to defence (lawyers secrecy) and right to information (journalistic secrecy) is also highly problematic. The argument that these secrecies are not violated as contents of communications are not revealed, does not resolve the problem. First, in some cases frequency of contacts with certain professionals, presence in certain places does reveal strictly private information (ex. related to health). Secondly, confidentiality of sources lay at the heart of the journalistic secrecy and access to retained data (sometimes together with publicly available information) could allow identification of the journalist's source. Therefore the lack of provisions that would make data retention and access rules compatible with general rules on evidence gathering as far as legally protected secrecies are concerned, may be seen as a legislative forbearance.

In conclusion, Polish rules on data retention constitute disproportionate limitation of constitutional rights and freedoms and require deep revision so as to be able to meet constitutional standards. The motion to the Constitutional Court by the group of parliamentarians and position of the Ombudsman in this regard are fully justified.

Moreover, the collection of complete, reliable and sufficiently precise statistics on access to retained data is essential for thorough assessment of overall necessity in a democratic society of the data retention regime.

8. Is there a constitutionally fixed limit to a conferral of national sovereignties to the EU in terms of *substance*, i.e. are certain matters/powers exempt from the general possibility of being delegated to the EU? If so: is this limitation in any way binding for Polish representatives in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?

Under Art.90 para.1 of the Constitution *the Republic of Poland may, by virtue of international agreements, delegate to an international organization or international institution the competence of organs of State authority in relation to certain matters*. This provision constituted the basis for accession to the EU. The Constitution allows only transfer of competences in *certain matters*.

Consequently, as explained by the Constitutional Court in its decision of 2005 on the Accession Treaty, this implies a prohibition on the delegation of all competences of a State authority organ or competences determining its substantial scope of activity, or competences concerning the entirety of matters within a certain field.[17] The Court added that neither Article 90 para.1 nor Article 91 para.3[18] of the Constitution authorize delegation to an international organization of the competence to issue legal acts or take decisions contrary to the Constitution, being the *supreme law of the Republic of Poland* (Article 8 para.1). These provisions do not authorize the delegation of competences to such an extent that it would signify the inability of Poland to continue functioning as a sovereign and democratic State.[19] In particular the norms of the Constitution within the field of individual rights and freedoms indicate a minimum and unsurpassable threshold which may not be lowered or questioned as a result of the introduction of Community provisions.[20] A possible collision between the EU law and the Constitution may not be resolved by assuming the supremacy of the EU law over a constitutional norm; such a conflict could be

---

17 Decision of the Constitutional Court of 11.05.2005, K 18/04, on the Accession Treaty. Summaries in English and German are available at:

http://www.trybunal.gov.pl/eng/summaries/documents/K_18_04_GB.pdf

http://www.trybunal.gov.pl/eng/summaries/documents/K_18_04_DE.pdf

18 Art.91(3) of the Constitution: *If an agreement, ratified by the Republic of Poland, establishing an international organization so provides, the laws established by it shall be applied directly and have precedence in the event of a conflict of laws.*

19 Decision of the Constitutional Court of 11.05.2005, K 18/04.

20 *Ibidem.*

resolved either by amending the Constitution or causing modification of the EU law provision or, ultimately, by Poland's withdrawal from the EU.[21]

In a more recent decision on the constitutionality of the Treaty of Lisbon, the Constitutional Court held the view that Article 90 of the Constitution together with the Preamble and other provisions referring to state's sovereignty and democracy, determine the limits of conferring competences on the Union. This limit is constituted by the following factors determining constitutional identity of Poland: the respect for the principles of Polish sovereign statehood, democracy, the principle of a state ruled by law, the principle of social justice, the principles determining the bases of the economic system, protection of human dignity and the constitutional rights and freedoms.[22] Therefore, it is admissible to confer the competences, only to the extent this does not infringe on the constitutional basis of the state. The Court noted that this rule is, in principle, recognized in the primary law of the EU. There are several guarantees of observance of this rule. First, the conferral of competences requires a consent in a statute adopted by the qualified majority or in a nationwide referendum. Secondly, there is the constitutional review of the delegation of competences by the Constitutional Court, which is competent to assess the constitutionality of normative acts granting the consent for the delegation of competences and of the relevant international treaty (and each treaty amending that treaty). In addition, there is a mechanism ensuring the participation of the Polish democratic representation and the authorities of the Polish state as regards having an impact on the content of the EU law, its enactment and effective implementation in Poland. The Court observed that the model of the European Union, adopted in the Treaty of Lisbon, is to ensure respect for the principle of protection of the state's sovereignty in the process of integration, as well as respect for the principle of favorable predisposition towards the process of European integration and the cooperation between States. This finds confirmation in the compatibility of values and goals of the Union determined in the Treaty of Lisbon as well as the values and goals of the Republic determined in the Polish Constitution, and in specifying the principles of distribution of competences between the Union and its Member States. The Court concluded that Poland is a Member State of the EU, which respects the sovereignty and national identity of Member States and guarantees freedoms and rights of the individual.[23]

Representatives of the Polish state, also when acting in EU organs and institution, are naturally bound by the Polish Constitution, which is the *supreme law of the Republic of Poland* (Art.8 para.1 of the Constitution).

---

21 *Ibidem.*

22 Decision of the Constitutional Court of 24.10.2010, K 32/09. The full text of the decision in English is available at:

http://www.trybunal.gov.pl/eng/summaries/documents/K_32_09_EN.pdf

On conferral of competences - see: pp.20-38.

23 *Ibidem.*

After the accession to the EU and a long debate on the suitability of the current constitutional provisions to the Polish membership in the EU, the amendment to the Constitution was prepared in order to regulate more specifically Polish participation in the EU. The draft act amending the Constitution was submitted by the President to the Parliament and is currently debated in the Sejm (lower house)[24]. Under the draft a new chapter Xa on the Polish membership in the EU would be added (Articles 227a-227k). The opening provision reads: *Art.227a. The Republic of Poland is a Member State of the EU, which respects sovereignty and national identity of Member States, respects principles of subsidiarity, democracy, state rules by the law, respect for the inherent and inalienable dignity of the person, freedom and equality, and guarantees the protection of human rights and freedoms comparable to the protection of those rights and freedoms in the Constitution*.

This provision, which is rather of a confirmatory nature, is intended as an axiological basis of participation of Poland in European integration processes and as a limit of constitutional legitimacy of Poland's membership in the EU. It also should serve, according to official justification of the draft, *i.a.* as a indicator of fundamental directions of Poland's European policy, obliging Polish organs of public authority to act at the EU level for the protection of fundamental values referred to in this provision.

The draft revision also contains provisions on the procedure of conferral of competences in *certain matters* to the EU, on the rights of EU citizens in Poland, on competences of Polish state organs *vis-a-vis* the EU, on actions of Polish state to ensure an effect of the EU law in the national legal order, and last but not least on the procedure of Poland's withdrawal from the EU.

9. What considerations during the legislative procedure have led to the deviations between the Directive and the national law in terms of the *data categories* to be retained?

The reasons for statutory provisions transposing the Directive, were presented in a general way. The official justification of the governmental draft of transposition referred to the Directive and the general need to secure evidence in criminal matters. Particular emphasis was put on the danger of terrorism and drug smuggling in the context of Poland's location. These reasons were presented as a justification for the adoption of the maximum allowed term of data retention. Although no explicit link was made between these reasons and data categories to be retained, one may assume that they could have influence on overall regime of data retention.

Detailed data categories subject to retention obligation were determined in the Regulation by the Minister of Infrastructure (Retention Regulation - RR). The official justification of the Regulation refers to the Directive and provisions transposing it in the Telecommunications Law, including Art.180a para.5 of the TL

---

[24] The draft of 12.11.2010 of the Act amending the Constitution of the Republic of Poland, Sejm's document No: 3598, available in Polish at:

http://orka.sejm.gov.pl/Druki6ka.nsf/0/0FA39CE6B812715AC12577E400489FEF/$file/3598.pdf

which says that data retention obligation applies also to data on unsuccessful call attempts. As regards the localization data, the justification of the RR mentions that in majority data listed in the RR are already in possession of operators and there is no need to generate these data only for retention purposes; thus para. 4 pp. 5 and 6 of the RR were intended to harmonize the extent and categories of data transferred by all operators. Additional information on approximate localization of an end piece of equipment (and not only on the territory where it is located) are – according to the justification of the RR - *extremely useful in investigation of criminal offences, often they constitute a key aspect of the evidence process*. Provisions of the RR were intended to present new parameters that may appear in the future, and which will show more precise location of the end piece of equipment without generating additional costs, except those that will be covered anyway due to improvements of operators' systems – explains ministerial justification of the RR. I was underlined in the document (also in the context of the data of unsuccessful call attempts and redirection of calls), that under the Directive and the TL the retention and storage obligation cover data generated in telecom network and/or processed by the operators and providers, which implies that they shall retain and store only these data that are available to them.

10. As regards the parties obligated to retain the data:

- **Are there any rules preventing the same data from being retained more than once (e.g. when the network operator and the service provider are different legal personalities who, in principle, would both be covered by the retention obligation)? If so: please describe the content of these rules.**

  There are certain rules that serve the purpose to avoid the same data being retained more than once. In particular, Art.180b para.2 of the TL allows to outsource contractually the fulfilment of an obligation of data retention, storage, making available and protection. An obliged network operator or service provider may entrust another telecommunications undertaking with performance of these obligations. This entrustment does not release the entrusting party from the responsibility. Moreover, under Art.180b para.1 of the TL the said obligations may be performed jointly by two or more network operators or service providers.

  The statutory provision empowering the Minister of Infrastructure to enact the RR, refers to the need to avoid multiple retention and storage of the same data. This requirement was taken into account – according to the ministerial justification of the RR – by separate determination of the data categories to be retained for each category of network operators and service providers in the RR.

- **According to §13 TL, "(o)perators of public telecommunications networks and providers of publicly available telecommunications services whose economic activity consist exclusively of: 1) providing associated services" are exempt from the retention obligation. Can you provide a definition of the term "associated service" in this context? Is this definition comparable**

to the definition of "associated facilities" laid down in Art. 2 lit. e Directive 2002/21/EC?

§ 13 p.1 of the Retention Regulation exempts from the retention obligation operators or providers of associated services/facilities (Polish: *udogodnienia towarzyszące*).[25] This term is defined in the Art.2 p.44 of the TL. This definition (in "unofficial consolidated translation" available at the UKE website) reads:

44) associated facilities – additional functional or service facilities associated with a telecommunications network which enable or support the provision of telecommunications services via that network, or associated with a telecommunications service which enable or support the provision of that service, in particular conditional access systems and electronic programme guides.

This definition corresponds to the definition in Art.2 (e) of the Directive 2002/21/EC.

- **Additional information on the subjects exempted from the retention obligation.**

The Ministry of Infrastructure and the President of UKE took a position on the application of data retention rules to providers of free access to the Internet (hotspots).[26] Both organs are of the opinion that such providers do not run economic activity and thus are not telecommunications undertakings which provide telecommunications services in the meaning of the TL (Art.2 p.27). Consequently such providers are not covered by the data retention obligations.

11. Please give more details about where and how the data is stored (see your answers to questions 38 and 39 of the first questionnaire): is it possible today to provide further information about how storage of the data to be retained is effected in practice? Does Polish law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC?

No further information on details where and how the data is stored is available.

The rules on the transfer of personal data to third countries are laid down in the Chapter 7 (Articles 47 and 48) of the Personal Data Protection Act of 1997 (with

---

25 In the response to the part 1 of the INVODAS questionnaire and the annex (unofficial, author's own translation of excerpts from the RR) – the term the term *associated services* was used, while indeed *associated facilities* would be more precise.

26 The position of the President of UKE of 01.04.2011 – available at:

http://www.uke.gov.pl/uke/index.jsp?place=Lead01&news_cat_id=168&news_id=6581&layout=3&page=text

The position of the Ministry of Infastructure of 28.02.2011 – available at:

http://www.uke.gov.pl/_gAllery/40/09/40095/Opinia_MI_JST_HOTSPOT.pdf

subsequent amendments), which transposed the Directive 95/46/EC. The relevant provisions read (in translation available at the GIODO website):

Article 47
1. The transfer of personal data to a third country may take place only, if the country of destination ensures at least the same level of personal data protection in its territory as that in force in the territory of the Republic of Poland.
2. The provision of paragraph 1 above shall not apply to the transfer of personal data required by legal provisions or by the provisions of any ratified international agreement.
3. Nevertheless the controller may transfer the personal data to a third country provided that:
1) the data subject has given his/her written consent,
2) the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request,
3) the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject,
4) the transfer is necessary or required by reasons of public interests or for the establishment of legal claims,
5) the transfer is necessary in order to protect the vital interests of the data subject,
6) the transfer relates to data which are publicly available.

Article 48
In cases other than those referred to in Article 47 paragraph 2 and 3 the transfer of personal data to a third country which does not ensure at least the same level of personal data protection as that in force in the territory of the Republic of Poland, may take place subject to a prior consent of the Inspector General, provided that the controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject.

12. Are there any specifications regarding data security with respect to storage and transmission (objectives to be achieved – e.g. "adequate confidentiality" – and/or quality requirements to be fulfilled – e.g. an obligation to encrypt the data before transmitting them to the authorised bodies)? If so: Are the technical and organisational measures necessary to implement these legal requirements standardised or specified in any other way, e.g. through guidelines issued by the supervisory authority? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.

In particular: do they provide for measures in one or more of the following areas:
- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**
- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**

- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
- **access logging**
- **secure (irreversible) deletion after expiry**
- **error correction mechanisms (e.g. hash functions, checksums)**
- **secure data transmission (cryptographic security, postal delivery)**
- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**
- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**
- **staff training/internal control mechanisms to ensure compliance with the law and other rules**
- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or generally to any data processing (in electronic communications)?

Legal requirements regarding data security with respect to storage and transmission are formulated in the specific context of data retention in a rather general manner. Network operators and service providers covered by data retention duties are obliged to protect data subject to retention against accidental or unlawful destruction, loss or alternation, unauthorized or unlawful storage, processing, access or disclosure, in accordance with the provisions on telecommunications secrecy and protection of end users data. The TL generally requires, in order to protect retained data, the application by the telecommunications undertakings of *appropriate technical and organisational measures* and the limitation of access to this data only to authorized employees. The said measures are not specifically standardised for the purposes of storage of retained data.

In the absence of more detailed specific rules on storage of retained data, the operators and providers that stores them should apply rules emanating from the Personal Data Protection Act on duties of data controllers to safeguard personal data (Articles 36-39 and the Regulation by the Minister of Interior – see p.5, above).

As regards data security with respect to transmission to authorised entities provisions on data retention contain, also rather generally formulated, safeguards concerning persons authorized to request access and requirements for use of telecom networks related in particular to identification of a person as well as technical and organisational safeguards against unauthorised access. These rules are presented in detail in p.13 below. Moreover, the respective statutory acts on authorized entities (ex. the Police) stipulate that making available of telecommunications data via a telecom network shall take place without the presence of employees of a telecom entity or with their presence to the necessary extent, if such an option is provided for

in the agreement between a chief of a state service authorized to access to data and this entity. Therefore more detailed requirements on data security at the stage of transmission may be regulated in those agreements.

13. In your answer to question 43, you mention that " The data may be made available via telecom networks if certain conditions related to identification of the accessing person and of the data, as well as to technical and organizational safeguards against unauthorized access are met.". Can you explain these conditions any further? Where in the law can these rules be found?

The rules on conditions for making available retained data to authorised entities via telecom networks are contained in the provisions of respective statutory acts on such entities (the Police, the Border Guard, the Military Police, the Fiscal Control, ABW, CBA, SKK). Those conditions, which are similar in each of these acts, covered in principle two basic sets of requirements: 1) related to identification of the accessing person and of the data; 2) technical and organizational safeguards against unauthorized access.

For example, the Police Act in Art.20c para.2 p.3 stipulates that: telecommunications data are made available via telecom network to a policeman who has a written authorization of the Chief Commander of the Police, District Commander of the Police or a person authorized by them. Under Art.20c para.5 p.1 making available to the Police of the telecommunications data may be performed via telecom network if used networks guarantee: *a) possibility of identification of the person obtaining an access to data, the categories of data accessed and the time of access; b) technical and organization safeguards preventing access to data of unauthorized persons.*

Almost identically worded provisions can be found in: Art.10b para.1 p.3 and para.4 p.1 of the Border Guard Act; Art.36b para.2 p.3 and para.6 of the Fiscal Control Act; Art.30 para.2 p.3 and para.4 p.1[27] of the Military Police Act; Art.28 para. 2 p.3 and para.4 of the ABW Act; Art.18 para.2 p.3 and para.4 p.1 of the CBA Act; Art.32 para.2 p.3 and para.6 p.1 of the SKK Act.

Wording of all these provisions was shaped by the act of 24.04.2009 amending the TL, which transposed the Directive into Polish law.

14. Please describe the rules for co-operation among the different bodies entitled to gain access to the retained data and between these and other public authorities in detail: which rules apply to the exchange of traffic and location data between these bodies, and how is data exchange between them effected in practice?

Co-operation of authorized entities has not been regulated in detail within the specific context of data retention. There is however a rule on such a co-operation in the Fiscal Control Act which stipulates that the fiscal intelligence makes available information obtained i.a. on the basis of Art.36b para.1 of Act that concerns its

[27] This provision requires mentioned guarantees with regard not only to telecom network but also to computer systems.

access to retained data to: 1) duty and tax organs; 2) courts and prosecutors in relation to a pending case; 3) state organs, services and institutions competent to perform operational and investigative acts, 4) other organs when the law so provides for (ex. under the Anti Money Laundering Act there is a duty to provide the General Inspector of Finance Information with all information necessary to prevent criminal offence of money laundering or financing of terrorism).

The rules on different forms of co-operation either in general context or in the specific context (ex. money laundering) are numerous. They are normally included in the statutory acts concerning each of authorized entities. Details are often regulated in agreements between different state services.[28] For example the Police Act stipulates that the Police may use data on persons, including in electronic form, obtained by other authorities, services and state institutions in the course of operational and investigative acts and process those data, without the knowledge and consent of a person concerned (Art.14 para.4). Conditions and procedure for providing the Police of these information are determined in the regulation by the Prime Minister issued in 2002[29] (which was not amended after enactment of data retention rules). The regulation says that authorized entities (to conduct operational and investigative acts) are obliged to provide the Police personal data obtained during performance of such acts, except when this could lead to disclosure of identity of a person that helps a given authorized entity or impossibility of fulfilment of its statutory tasks. The data request should be made in writing or with the use of a computer equipment and systems. The data should be delivered by heads of a given organizational unit of authorized entity or by persons authorized by them. Provision of information should be noted in a specified manner.

There is no available information how retained data exchange is effected in practice.

15. Please give more details about which (and how) EU legislative acts and international treaties on cross-border co-operation (i.e. rules specifically designed for data retention as well as general rules applicable to data retention) are applied in Poland.

Poland applies EU legislative acts and international treaties to which Poland is a party on cross-border co-operation in criminal matters. The provisions related to such co-operation are included in the Part XIII of the KPK *Procedure in criminal cases in international relations* – Chapters 61-67 (Articles 578-615).

One of the most fundamental international treaties to which Poland is a party is the European Convention on Mutual Assistance in Criminal Matters of 1959. Poland

---

[28] For example: the agreement between the Minister of Finance and the Chief Commander of the Police of on the co-operation between the Police and the Customs Service; the agreement of the Chief Commander of the Police and the General Inspector of Fiscal Control on the co-operation between the Police and organs of the fiscal control.

[29] The regulation of 02.03.2002 by the Prime Minister on the scope, conditions and procedure of providing the Police information on persons, obtained by entities authorized to perform operational and investigative acts during performance of these acts and on the form of authorization constituting the basis for making available personal data to policemen, Dz.U. No 24, item 245.

ratified also two Additional Protocols of 1978 and 2001. In order to complement the provisions of the Convention Poland has concluded additional agreements on co-operation in criminal matters with Slovenia (1997), Austria and Germany (2003).

In 2005 Poland ratified the Convention on Mutual Assistance in Criminal Matters between Member States of the EU of 2000 with the Additional Protocol of 2001. Governmental declaration on binding force of the Convention and Protocol includes information on how this act is applied: - a central authority for the purpose of Art.6 para.2 and 8 is the Ministry of Justice; - competent authorities for the purpose of Art.6 para.6 are with regard to Articles 12 and 14 The Police Chief Commander, with regard to serious fiscal criminal offences – also the Minister of Finance, and with regard to Art.13 – the General Public Prosecutor; - authorities competent for application of Articles 18, 19, 20 para.1-3 and 5 are territorially competent district public prosecutors, - the role of contact points in line with Art.20 para.4 is performed by territorially competent district commanders of the Police.

Poland has also concluded and ratified many other multilateral and bilateral treaties on the co-operation in criminal matters.

The most known example of application of EU legislative acts in criminal matters is the Framework Decision on the European Arrest Warrant (EAW). The provision in the KPK that was initially introduced to apply EAW, was declared by the Constitutional Court in 2005 contrary to the Constitution, that in the time banned the extradition of a Polish citizen. Following this decision, the Constitution was amended, and since 2006 it allows for extradition of a Polish citizen if such a possibility emanates from ratified international treaty or a statutory act implementing the legal act of the international organisation of which Poland is a Member State. Provisions on application of EAW were added to the KPK (Chapters 65a and 65b – Articles 607a-607zc). In Poland EAW is often applied. Poland belongs to Member States that issue the biggest amount of EAW in the UE.

Poland implemented also the Framework Decision on joint investigation teams (such teams are also provided for in Art.13 of the Convention on Mutual Assistance in Criminal Matters between Member States of the EU and Art.20 of the Additional Protocol of 2001 to the European Convention of 1959) – Articles 589b-589f of the KPK. The code includes also provisions adopted in implementation of: - the Framework Decision on the application of the principle of mutual recognition to financial penalties (Chapters 66a and 66b – Articles 611fa – 611fm); the Framework Decision on the application of the principle of mutual recognition to confiscation orders (Chapters 66c and 66d – Articles 611fn – 611fze). The KPK contains also provisions on co-operation with the International Criminal Court (Chapter 66e – Articles 611g – 611s).

The provisions that may be of relevance in the context of access and use of the retained data are those implementing the Framework Decision 2003/577/JHA of 22.07.2003 on the execution in the EU of orders freezing property or evidence: Chapters 62a – 62b, Articles 589f – 589u of the KPK, added in 2005.

In case material objects, correspondence, dispatches, lists of telephone calls or other communications, or data stored in a computer system or on a carrier, including electronic mail correspondence, or property subject to freezing in order to secure fulfilment of an order on confiscation are on the territory of another EU Member State – the Polish court competent to deal with the case or a prosecutor may request directly from judicial authority in this state to execute an order to freeze or secure them. Such a request is made on the basis of KPK provisions and international treaties on mutual assistance in criminal matters. All documents sent shall be translated into official language of the executing state or another language indicated by this state. Delivery of the request and documents may be done also with the means of automatic transfer of data, in a way allowing to verify their authenticity. In case of difficulties with identification of the competent authority of the executing state the court or prosecutor may also make a request to competent organisational unit of the European Judicial Network. Delivered evidence should be returned immediately after the usage, if it was requested so or if the object should be returned to the victim or to other person. If the order to freeze an evidence or property is repealed, the court or prosecutor shall immediately inform the competent authority of the EU Member State. An order to freeze an evidence or property is subject to appeal. If under the law of the executing state this state is liable for damages caused by the execution of an order to freeze an evidence or property issued by a Polish court or prosecutor, the Treasury of the State, at the request of the competent organ of the executing state, shall reimburse an amount of paid compensation for damages, unless they are the consequence only of an action or renunciation by an authority of this state.

The KPK regulates also the case of a request of a competent judicial authority from an EU Member State to execute an order to freeze property or evidence directed to Polish authorities. Such requests may concern the same objects as mentioned above, including lists of telephone calls or other communications, or data stored in a computer system or on a carrier, including electronic mail correspondence. Such requests shall be executed immediately by the competent regional court or prosecutor, provide requested objects are in Poland, If the court or prosecutor that obtained the request is not competent to deal with it, the request shall be forwarded to the competent authority. The judicial authority of the EU Member State that made a request shall be informed about it. One may refuse to execute an order on freezing evidence if:

1) the act in relation to which the order has been issued does not constitute a criminal offence under the Polish law, unless under the law of the issuing State it is one of the criminal offences listed in Art.3 para.2 of the Framework Decision 2003/577/JHA punishable in the issuing State by custodial sentence of a maximum period of at least three years; however this rule shall not apply if the act does not constitute a criminal offence due to lack or different regulation of certain taxes, duties, customs and exchange in Poland;

2) the evidence may not be frozen due to factual circumstances, in particular due to loss, destruction or impossibility to trace it; in such case the competent court or

prosecutor shall consult the authority that issued the order to obtain information helpful in searching of the object;

3) the certificate, that includes all relevant information necessary for proper execution of the order, has not been enclosed to the order, or the certificate is incomplete or manifestly incompatible with the order;

4) it is evident from the content of the certificate that the order to be executed concerns the act of the person, with regards to which criminal proceedings were finished with legal validity;

5) the execution of the order is impossible due to refusal of information and documents concerning persons who have an immunity.

An order on execution of the foreign order on freezing evidence or property shall be issued immediately, if possible not later than in 24 hours after delivery of the foreign order. An order on execution shall be delivered with an instruction on rights provided for in the law of the issuing State. Without prejudice to these rights, the persons whose rights has been infringed may appeal against an order on execution and against acts related to freezing of evidence or property. The competent judicial authority of issuing State shall be immediately informed about the appeal and the decision issued in the official language of this state or other language indicated. The court or prosecutor that issues the order to execute an order on freezing evidence or property may suspend the execution if: - it could impede another pending criminal case, for the time necessary to secure proper conduct of this case; - evidence or property concerned was frozen before for the purposes of another pending criminal case. The competent judicial authority of the issuing State shall be immediately, if possible within 24 hours, notify about the order on execution and eventually on its suspension. Such a notification may be delivered with the use of means of automatic data transfer, in a way allowing to verify authenticity of documents transferred. In the course of execution of an order to freeze evidence or property one should fulfil the request of the issuing authority to apply specific way of proceedings or special form, if this is not contrary to the rules of legal order in Poland. The protocol of freezing evidence or property shall be immediately delivered to the competent judicial authority of the issuing State. The evidence or property remains frozen until the decision to execute the request of the issuing State for transfer of the evidence for confiscation is taken. The court or prosecutor, after consultation with the competent judicial authority of the issuing State, may set for this authority a deadline to transfer such a request. If the court or prosecutor envisages to release evidence or property from freezing, it should inform so the competent judicial authority of the issuing State and offer it an opportunity to submit its comments. If the authority does not put forward arguments sufficiently justifying further freezing, the court or prosecutor shall issue an order to release the object from freezing. Such an order shall be issued also if the issuing state notifies that the freezing order has been lifted. A copy of the release order shall be delivered to persons concerned.

The request to transfer frozen evidence or to execute a request to enforce confiscation shall be dealt with on the basis of instruments of mutual legal

assistance in criminal matters (i.e. provisions of Chapter 62 of the KPK and international treaties) and – in relations with Members States of the EU – on the basis of Chapter 66d of the KPK that implements the Framework Decision 2006/783/JHA of 06.10.2006 on the application of the principle of mutual recognition to confiscation orders. It is not allowed to refuse execution of such a request on the basis that the act in relation to which the request has been made does not constitute a criminal offence under the Polish law, if under the law of the issuing State it is one of the criminal offences listed in Art.3 para.2 of the Framework Decision 2003/577/JHA punishable in the issuing State by custodial sentence of a maximum period of at least three years.

Finally if the Treasury of the State is liable for damages caused by the execution of orders freezing evidence or property issued by the judicial authority of the EU Member State, the Treasury of the State shall request the competent authority of the issuing State to reimburse amount paid as a compensation of damages, unless they have been caused only by action or renunciation of Polish organs.

16. Which public bodies are responsible for supervising that *the bodies entitled to obtain access to the data retained* (police etc) act within the law? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?

As far as the Police is concerned the Chief Commander is the central government administration authority competent for issues related to the protection of people's safety and maintenance of public safety. He reports to the Minister competent for internal affairs. The Police Chief Commander is appointed and dismissed by the Prime Minister, at the request of the Minister competent for internal affairs.

Similar solution exists with regard to The Border Guard and its Chief Commander.

The Chief Commander of the Military Police reports to the Minister of National Defence, and is appointed and dismissed by the same organ.

The General Inspector of the Fiscal Control is appointed and dismissed by the Prime Minister at the request of the Minister of Finance, who is also the superior organ of the fiscal control.

Chiefs of ABW and CBA are appointed and dismissed by the Prime Minister, after the opinion of the President of Poland, governmental Committee on Special Services, and parliamentary (Sejm's) Committee on Special Services. Chiefs of ABW and CBA report to the Prime Minister, however are also supervised by the Sejm.

The Chief of SKK is appointed and dismissed by the Prime Minister, after the opinion of the President of Poland, governmental Committee on Special Services, and parliamentary (Sejm's) Committee on Special Services. The Chief of SKK reports in principle to the Minister of National Defence, however the yearly report of the Chief of SKK should be presented to the Prime Minister. Activities of the Chief of SKK are subject to supervision by the Sejm.

In conclusion, supervision over the Police, the Border Guard, the Military Police and the Fiscal Control is governmental in nature. Supervision over special services authorised to obtain retained data (ABW, CBA, SKK) is also performed by the Sejm (lower house of the Parliament), therefore there is an element of independent control, although generally these services are subordinated to government.

The public prosecution became independent of the government after structural reform in 2010. Before this date the Minister of Justice was at the same time the General Public Prosecutor. Currently the General Public Prosecutor is independent. He/she is appointed by the President among two candidates each nominated by the National Council of the Judiciary and the National Council of Public Prosecution.

In addition, activities of all organs of governmental administration, state legal persons and other state entities (including *authorized entities*) are subject to control regarding the legality, economic prudence, efficiency and diligence by the Supreme Chamber of Control (*Najwyższa Izba Kontroli – NIK*). NIK is subordinated to the Sejm and is independent of a government. The President of NIK is appointed by the Sejm, with the consent of the Senate for the 6 years term of office; he/she may not be a member of a political party, trade union or conduct any other public activity incompatible with the dignity of his office. NIK's control activities are performed upon the request by the Sejm or its organs, the President of Poland, the Prime Minister or under its own initiative.