COMMISSIONER FOR HUMAN RIGHTS

Adam Bodnar

Warsaw, 18 February 2016

II.519.109.2015.KLS/VV/AG

Constitutional Tribunal

Warsaw

On the basis of Article 191 para 1 pt. 1 of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws No. 78, item 483 as amended) and art. 16 para 2 pt. 2 of the Act of 15 July 1987 on the Commissioner for Human Rights (Journal of Laws of 2014, item 1648 as amended), I request to declare the non-consistence of:

I.

- Article 19 para 9 of the Act of 6 April 1990 on the Police (Journal of Laws of 2015, item 355, as amended);
- Article 9e para 10 of the Act of 12 October 1990 on the Border Guard (Journal of Laws of 2014, item 1402, as amended);
- Article 36c para 7 of the Act of 28 September 1991 on Fiscal Control (Journal of Laws of 2015, item 553, as amended);

The Office of the Commissioner for Human Rights
al. Solidarności 77
00-090 Warsaw

Phone (+48 22) 55 17 700
Infoline 800 676 676
biurorzecznika@brpo. gov.pl
www.rpo.gov.pl

- Article 31 para 10 of the Act of 24 August 2001 on Military Police and Military Law Enforcement (Journal of Laws of 2013, item 568, as amended);
- Article 17 para 9 of the Act of 9 June 2006 on the Central Anticorruption Bureau (Journal of Laws of 2014, item 1411, as amended)

- in so far as they allow the extension of operating surveillance for consecutive periods whose total length cannot exceed 12 months, which in turns means the ability to conduct operating surveillance for 18 months –with Article 2, Article 47, Article 49, Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution of the Republic of Poland;

II.

- Article 19 para 15h of the Act of 6 April 1990 on the Police;
- Article 9e para 16h of the Act of 12 October 1990 on the Border Guard;
- Article 36c para 7 of the Act of 28 September 1991 on Fiscal Control;
- Article 31 para 16h of the Act of 24 August 2001 on Military Police and Military Law Enforcement;
- Article 27 para 15j of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency;
- Article 31 para 14h of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service;
- Article 17 para 15h of the Act of 9 June 2006 on the Central Anticorruption Bureau

- in so far as they use a vague criterion of the "interest of the criminal justice system" and do not specify the weight of circumstances to be determined on the basis of materials that may to contain information referred to in Article 178a, Article 180 § 2 and Article 180 § 3 of the Code of Criminal Procedure –with Article 2 of the Constitution, with Article 42 para 2, Article 47, Article 49, Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution and Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

III.

- Article 20c para 1 and Article 20cb para 1 of the Act of 6 April 1990 on the Police,

- Article 10b para 1 and Article 10bb para 1 of the Act of 12 October 1990 on the Border Guard,
- Article 36b para 1 and Article 36bb para 1 of the Act of 28 September 1991 on Fiscal Control,
- Article 30 para 1 and Article 30c para 1 of the Act of 24 August 2001 on Military Police and Military Law Enforcement,
- Article 28 para 1 and Article 28b para 1 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency,
- Article 32 para 1 and Article 32b para 1 of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service,
- Article 18 para 1 and Article 18b para 1 of the Act of 9 June 2006 on the Central Anticorruption Bureau,
- Article 75d para 1 and Article 75db para 1 of the Act of 27 August 2009 on the Customs Service,

with Article 2, 30, 47, 49, 51 para 2 in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the Charter of Fundamental Rights of the European Union

IV.

- Article 20c para 3 in conjunction with Article 20c para 2 of the Act on the Police,
- Article 10b para 3 in conjunction with Article 10b para 2 of the Act on the Border Guard,
- Article 36b para 3 in conjunction with Article 36b para 2 of the Act on Fiscal Control,

- Article 30 para 3 in conjunction with Article 30 para 2 of the Act on Military Police and Military Law Enforcement,
- Article 28 para 3 in conjunction with Article 28 para 2 of the Act on the Internal Security Agency and the Foreign Intelligence Agency,
- Article 32 para 3 in conjunction with Article 32 para 2 of the Act on the Military Counterintelligence Service and the Military Intelligence Service,
- Article 18 para 3 in conjunction with Article 18 para 2 of the Act on the Central Anticorruption Bureau,
- Article 75d para 3 in conjunction with Article 75d para 2 of the Act on Customs Service,

with Article 2, Article 20 and with Article 47 and Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution of the Republic of Poland.

V.

- Article 20ca of the Act on the Police,
- Article 10ba of the Act on the Border Guard,
- Article 36ba of the Act on Fiscal Control,
- Article 30b of the Act on Military Police and Military Law Enforcement,
- Article 28a of the Act on the Internal Security Agency and the Foreign Intelligence Agency,
- Article 32a of the Act on the Military Counterintelligence Service and the Military Intelligence Service,
- Article 18a of the Act on the Central Anticorruption Bureau,
- Article 75da of the Act on Customs Service in so far as they do not provide for the introduction of a mechanism of real, independent control of data sharing –

- with Article 2, 47, 51 para 2 in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the Charter of Fundamental Rights of the European Union.

VI.

- Article 20c of the Act on the Police,
- Article 10b of the Act on the Border Guard,

- Article 36b of the Act on Fiscal Control,
- Article 30 of the Act on Military Police and Military Law Enforcement,
- Article 28 of the Act on the Internal Security Agency and the Foreign Intelligence Agency,
- Article 32 of the Act on the Military Counterintelligence Service and the Military Intelligence Service,
- Article 18 of the Act on the Central Anticorruption Bureau,
- Article 75d of the Act on Customs Service

- in so far as these provisions do not indicate the categories of people whose data can be obtained in the manner specified in the statutes, do not regulate the obligation to provide information to people whose data were obtained and do not specify the period during which the authorised bodies may process the acquired data – with Article 2, 30, 47, para 49, 51 para 2, 3, 4 in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the Charter of Fundamental Rights of the European Union.

VII.

- article 28 para 7 of the the Internal Security Agency and the Foreign Intelligence
- Article 32 para 9 of the Act on the Military Counterintelligence Service and the Military Intelligence Service

- in so far as they do not provide for the destruction of any other telecommunications, postal and on-line data than just those irrelevant for the ongoing criminal investigation – with Article 51 para 2 of the Constitution in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 51 para 1 of the Charter of Fundamental Rights of the European Union.

Article 13 and Article 16 of the Act of 15 January 2016 on the Amendment to the Police Act and Some Other Acts (Journal of Laws of 2016, item 147) – in so far as they require to apply provisions that ceased to apply by virtue of the Constitutional Tribunal's judgement of 30 July 2014, ref. K 23/11 –with Article 2 and Article 190 para 1 and 3 of the Constitution of the Republic of Poland.

STATEMENT OF REASONS

The Act of 15 January 2015 on the Amendment to the Police Act and Some Other Acts (Journal of Laws of 2016, item 147), which introduced most of the provisions challenged in this application, implements – in the opinion of the proponents – the judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11. In this judgement, the Constitutional Tribunal has ruled on the non-compliance of a number of provisions governing the application of operating surveillance by the police services and special services with the Constitution of the Republic of Poland. In the opinion of the Commissioner for Human Rights, the provisions which are the subject of this application not only do not implement the cited judgement of the Constitutional Tribunal, but also gravely violate constitutional human rights and freedoms, and the standards set out in international law.

There is no doubt that operating surveillance is a tool used by special forces around the world. It allows the actual conduct of activities to which these services have been established. It would be difficult, if not impossible, to ensure the security of the state and its citizens without allowing the use of secret operational techniques. One cannot forget that criminal organisations, as a rule, do not use transparent and predictable methods that use widely available measures used in legal activities. An attempt to ensure effective protection against criminal activity, involving only the use of overt methods would be doomed to fail from the start. This is even more evident if one takes into account the main sources of security threats present today. Terrorist activities on such a scale would not be possible without the use of new technologies, especially the Internet and other telecommunications techniques. It is understandable that efficient fight against these phenomena requires not only the use of these information channels, but also accessing information exchanged by persons engaged in activities that threaten security. The Commissioner for Human Rights does not contest – in principle – the possibility, and even the need for using operational surveillance. What is more, the Commissioner notes that more often than not it is the use of activities from the scope of operational surveillance that can contribute to the protection of human freedoms and rights.

Police services and special services in a democratic state are geared toward providing the state and its citizens with security, i.e. protection against internal and external threats. Safety is undoubtedly located high in the hierarchy of goods protected by law. It is rightly pointed out in legal writings that safety is a state, which "gives the individual the feeling of an elementary value, which is its existence and a guarantee of

preservation and continuity of that existence, it allows further development and self-improvement" (M. Ławrynowicz-Mikłaszewicz, *Bezpieczeństwo jako prawo człowieka w kontekście stosowania środków przymusu bezpośredniego i broni palnej przez uprawnione podmioty*, „Przegląd Prawniczy, Ekonomiczny i Społeczny" 2014, no. 4, p. 64). However, one cannot forget that operational and investigative activities, in their essence, significantly interfere with fundamental freedoms and human rights. Not always and not in any area can such an interference be justified by security reasons. Safety is, without a doubt, one of the most important legal goods, but not the only one. It also is not absolute, which means that it may be subject to restrictions due to collisions with other goods. In other words, actions aimed at protecting the safety of citizens cannot interfere in other legal goods, including human rights and freedoms in particular. Too large a range of permissible interference would lead undoubtedly to the risk of significant abuse involving the use of broad powers by state authorities in order to exercise a right not so much common, but rather particular.

The legal instruments surrounding operational surveillance must be constructed on the basis of an informed and in-depth study of the collision of protected goods, in this case the most important goods for a political community, spanning human dignity, common good and the principle of democratic rule of law. (these dilemmas are pointed out by M. Safjan, in: M. Safjan, Wyzwania dla państwa prawa, *Warsaw 2007, pp. 61-62).* The authorities protecting human rights, including the Commissioner for Human Rights, are appointed to conduct intensive checks, verifying whether the confines of proportionality of using operational and investigative activities in a democratic state have not been breached. Restrictions imposed on police services and special services may result, to a certain extent, in an increased risk of danger, however, a far-reaching limitation of these risks would be possible only through the construction of an omnipotent, and – ultimately – totalitarian state.

It should be noted that the discussed provisions do not apply to the issue of operational and investigative activities conducted in the framework of criminal proceedings, in the manner laid down in the Code of Criminal Procedure. Rather, the challenged provisions are a manifestation of something that Dobrosława Szumiłło-Kulczycka describes as an erosion of the settled regimen of applying the activities discussed here. The main manifestation of this erosion is the abandonment of the belief that "one of the differences between operational and investigative activities, and procedural measures is the inadmissibility of using materials obtained using the former in criminal proceedings" (D. Szumiło-Kulczycka, *Czynności*

operacyjno-rozpoznawcze iich relacje do procesu karnego, Warsaw 2012, p. 17). Consequently, the provisions that are the subject of this application govern activities outside of the scope of criminal procedure, which could lead to criminal proceedings, but do not involve such a necessity. The literature emphasizes that operational surveillance play a subsidiary role in relation to criminal proceedings, they precede preparatory proceedings, providing justification to initiate preparatory proceedings (see K. Eichstaedt, Zarządzenie przez sąd kontroli operacyjnej w ujęciu procesowym, Prokuratura i Prawo 2003, 9, p. 28).

Operational surveillance is of discreet nature and may consist in:

1) obtaining and recording of conversations held using technical means, including telecommunications networks;
2) obtaining and recording image and sounds of persons from premises, means of transport and places other than public places;
3) obtaining and recording the contents of correspondence, including correspondence exchanged by means of electronic communication;
4) obtaining and recording of data contained on digital media, telecommunications terminal equipment, IT and ICT systems;
5) obtaining access and controlling the contents of consignments.

The legislature included, within the scope of the Act of 15 January 2016 on the Amendment to the Police Act and Some Other Acts, not only activities from the scope of operational surveillance, but also obtaining data that do not constitute the contents of, respectively, telecommunications, postal items or transmissions within a service provided by electronic means, called Internet data, telecommunications data and postal data. The scope of the amendment raises particular concerns of constitutional nature.

Activities carried out within the framework of widely understood operational surveillance, and therefore also the collection of telecommunications, Internet and postal data, are confidential in nature.

It should be noted that, on the one hand, the confidentiality of ongoing activities determines their effectiveness, however, on the other hand, it limits an individual's possibility to exercise the protection of their rights and freedoms guaranteed by the Constitution, as the citizen has no knowledge that state authorities interfered in their rights and freedoms. As noted in the judgement of the Constitutional Tribunal of 12 December 2005: "An essential feature of operational activities is also their confidential or secret nature (T. Hanausek, Kryminalistyka. Zarys wykładu, Krakow 12 p. 2005, which is a premise of their efficiency, but at the same time causes the interested party, unbeknownst to the operating surveillance conducted in relation to them, is not in a position, for reasons purely factual, to initiate procedures and guarantees, the use of which is dependent on their knowledge and initiative" (judgement of the Constitutional Tribunal of 12 December 2005, ref. K 32/04).

Individual tribunals have developed minimum requirements, that must be cumulatively met by provisions restricting rights and freedoms, governing operational and investigative activities. In order to illustrate this statement with examples, the Commissioner for Human Rights wishes to refer to the case-law of the ECHR, which repeatedly stressed that the interference with private life and and correspondence not only consists in individual measures of covert control directed against designated entities, but also the strategic monitoring of connections and the acquisition of related personal data of communicating entities. This issue was dealt with in Weber and Saravia v. Germany, which challenged the German provisions regulating the strategic monitoring of telecommunications connections consisting in recording telephone calls of an indeterminate circle of speakers, and subsequent identification, using keywords, of information contained in these conversations, which can potentially identify perpetrators or the plans to commit crimes (judgement of the ECtHR of 29 June 2006 in *Wever and Saravia,* case no. 54934/00). According to the ECtHR there was an interference in the "secrecy of telecommunications" protected by Article 8 of the ECHR. In the light of ECtHR's case-law, collecting and storing data on individuals by state services, irrespective of the manner in which they have been collected also constitutes an interference in the realm of privacy of an individual. (see judgement of the ECtHR of 4 May 2000 in Rotary v. Romania, application no. 28341/95, § 43-44 of the statement of reasons and judgement of 2 September 2010 in Uzun v. Germany, § 46 of the statement of reasons). The ECtHR gathering data on individuals, regardless of how they will be used in the future is sufficient to establish interference with the right guaranteed by Article 8 of the ECHR. However,

the ECtHR did not negate the general acceptability of covert collection of information about individuals by public authorities, but even pointed to their necessity, as a tool allowing to efficiently guarantee safety and protection of institutions of a democratic state against sophisticated forms of threats, especially espionage and terrorism (see, among others, judgement of the ECtHR of 6 September 1978 in Klass and others v. Germany, case no. 5029/71).

At the same time, it should be noted that the Constitutional Tribunal, as well as the Court of Justice of the European Union (CJEU) did not negate the need to grant the powers to acquire knowledge, collect and gather information about citizens in a covert manner to the competent authorities (see, for example, judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11 or CJEU judgement of 8 April 2014 in joined cases C-293/12 Digital Rights Ireland and C-594/12 Kartner Landesregierung and others; ECtHR judgement of 29 June 2006 in Weber and Saravia v. Germany, case no. 54934/00 or recently judgement of 4 December 2015 in Zakharow v. Russia, case no. 14881/03).

When discussing the issues addressed in this application, one also has to refer to the law of the European Union, and in particular to the provisions of the Charter of Fundamental Rights of the European Union, which sets out the right to privacy in Article 7 and the right to the protection of personal data in Article 8. In accordance with Article 52 para 1 of the CFR, any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The right to the protection of personal data is also protected in the European Union under Article 16 of the Treaty on the Functioning of the European Union.

It should be noted that the application of the Charter of Fundamental Rights of the European Union in this case must take into account the contents of Article 51 para 1, in accordance with which, the provisions of the Charter are addressed to Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties. In this case, the CFR applies due to the existence of the following directives, which are applicable in respect

of the limitation of rights relating to the right to privacy, especially in the area of telecommunications data and Internet data:

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, OJ L 201, 31.7.2002, p. 37, as amended), in particular Article 15 para 1 thereof in conjunction with Article 5 of Directive Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market
- (Directive on electronic commerce, OJ. EC-L 178 of 17.7.2000, p. 1, as amended), in particular Article 3 para 4 thereof in conjunction with Article 3 para 1 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31), in particular Article 1 and Article 7 thereof.

The legislature, therefore, was obligated to examine the compatibility of the Act of 15 January 2016 on the Amendment to the Police Act and Some Other Acts, which introduced the amendments challenged in the application, for compliance with the provisions of the aforementioned directives, in particular in the context of the proportionality of limitations to the right to privacy and the right to protection of personal data. The need to verify the proposed regulation for their suitability and necessity arises therefore also with European Union law.

Having regard to the previous findings of the Constitutional Tribunal, the ECtHR, as well as the CJEU relating to the provisions governing the acquisition of information about individuals by public authorities in a democratic state of law, it is possible to compile a list of minimum requirements that must be met by provisions restricting rights and freedoms. Such a compilation was made, among others, by the Constitutional Tribunal in its judgement of 30 July 2014, in case K 23/11. Those in particular should be recalled, that directly relate to the challenged provisions of the Act on the Police and the other indicated acts, and which will be cited in the remainder of the Commissioner's application. In particular:

1) data concerning individuals cannot be gathered, stored and processed without a clear and precise statutory basis;
2) state authorities empowered to carry out operational surveillance must be precisely indicated;
3) provisions should clearly specify the conditions for the use of operational and investigative activities, and limit it only to the detection of serious crimes and their prevention;
4) not only the measures of covert information collection should be indicated, but also the types of information gathered by means of specific measures;
5) activities within the scope of operational surveillance and other activities consisting of data collection should be a subsidiary mean of obtaining information or evidence;
6) a statute should specify the maximum period of conducting operational and investigative activities, which should not infringe the principle of necessity arising from the principle of proportionality (Article 31 para 3 of the Constitution of the Republic of Poland);
7) a statute should precisely normalize the procedure of managing operational and investigative activities, including the requirement to obtain the consent of an independent body for covert acquisition of information;
8) it is necessary to specify in a statute the rules of conduct concerning materials collected over the course of operational and investigative activities
9) it is necessary to ensure the security of the collected data;
10) it is necessary to standardise the procedure of informing individuals about covert acquisition of information about them, as well as to introduce procedures allowing to challenge operational and investigative activities.

After the compilation of the list cited above, subsequent judgements of the CJEU and the ECtHR have been announced, which focussed on tie issue of mass information collection. In this context, one should bring up the judgement of the CJEU of 6 October 2015 in case C-362/14 in the case Maximillian Schrems, where the CJEU admittedly evaluated the validity of a particular decision of the European Commission, but also referred to the problem of the absence of remedies available to the citizen in the case of transmitting his data to a third country, even for the purposes of the protection of public safety, which does not meet the minimum requirements relating to the protection of personal data. The annulled decision did not specify any

restrictions in terms of the access of US public authorities to the personal data transmitted on its basis. In particular, the CJEU explained that a regulation which allows public authorities to gain general access to the contents of electronic messages must be considered a violation of the main essence of the fundamental right to respect for private life (para 94 of the CJEU judgement in case C-362/14 Maximillian Schrems).

The Commissioner for Human Rights would also like to draw attention to a case settled by the European Court of Human Rights on 4 December 2015 (Zakharov v. Russia, application no. 47413/06). In its judgement, the ECtHR considered that there has been a violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and the covert system of controlling telephone calls from cell phones in Russia violates the right to respect for private life and correspondence. Although the complainant has not demonstrated that his conversations were under surveillance or that operators provided his data to unauthorised persons, the ECtHR decided to carry out an abstract analysis of the law. From the judgement it appears that the ECtHR drew attention, in particular, to a breach of conventional standards found in the absence of any clarification of the circumstances in which the authorities can eavesdrop on conversations of citizens, the lack of a legal order for concluding surveillance, when the conditions justifying its use ceased, the lack of standardisation of procedures of storing and destroying recorded data, which in practice meant the perpetual storage of such data, the lack of procedures for authorising such surveillance, or finally, the lack of regulation of the principles of informing citizens about the conduct of surveillance and the legal remedies available to citizens in the event of surveillance pertaining to their mobile phones. Furthermore, in the not-yet-final judgement in Szabó and Vissy v. Hungary (judgement of 12 January 2016, application no. 37138/14), the ECtHR found that the natural response of the national activities to the phenomenon of terrorism and crime is to take action, also preventive in nature, with a view to their eradication, in particular by mass monitoring of means of communication. The Court, however, raised concerns as to whether national legislation provided for guarantees, which would be sufficiently precise, efficient and understandable in relation to the management, execution and implementation of the specified permissions. In particular, the Court recognised that the Hungarian regulations:

- do not specify the categories of persons that could be subject to covert surveillance, and in particular they do not require the indication of any connection to terrorist threats,

- the services, which request a permit from the Minister of Justice to conduct surveillance, do not have to justify in any detailed way whether the collection of such information is necessary, which – in the Court's view – can easily lead to abuse,
- they determine the maximum duration of surveillance insufficiently, which – in effect – can lead to a situation in which it is not limited in any way,
- no legal remedies available to persons whose communications were monitored have been stipulated – in particular, the Court has not considered the obligation to submit semi-annual reports to a parliamentary committee to be an appropriate measure.

This judgement is not yet final as of the time of submission of this application to the Constitutional Tribunal, nevertheless it confirms the direction of consideration adopted by the ECtHR and maintains the existing ruling practice.

The evaluation of the constitutionality of the contested provisions must also be preceded by considerations on the possibility of the Constitutional Tribunal controlling the lack of regulation and qualifying this absence as a proper or relative legislative omission. In the opinion of the Constitutional Tribunal, a proper legislative omission (so-called "lacuna") consists in the failure to adopt a legislative act, even though the obligation to its adoption results from constitutional norms (cf. judgement of the Constitutional Tribunal of 3 December 1996, ref. K 25/95).

In the Tribunal's jurisdiction, there is a lack of competence to rule on an omission by the legislature, that is, when a given issue has been left completely outside legal regulations. In turn, relative legislative omission involves the adoption of an incomplete regulation – in the adopted and applicable legal act the legislature regulates an issue in an incomplete, partial manner. In this case, it is permitted to control the incomplete regulation, which – from the point of view of constitutional principles – has too narrow scope, or due to the object and purpose of the regulation omitting relevant content (Constitutional Tribunal in its judgement of 13 June 2011, ref. SK 41/09). As noted by the Tribunal, "the allegation of unconstitutionality may therefore apply both to what the legislature has regulated in an act, and what it has omitted, but it should have regulated in accordance with the Constitution" (judgement ref. K 25/95). The division on proper legislative omissions, which do not fall within the Tribunal's jurisdiction, and partial regulations examined by the constitutional court has been reflected in many judgements of the Constitutional Tribunal (e.g. judgement of 6 May 1998,

ref. K 37/97, judgement of 24 October 2001, ref. SK 22/01, judgement of 19 May2003, ref. K 39/01 or judgement of 9 December 2008, ref. SK 43/07).

These arguments have become the basis for the evaluation of the provisions carried out by the Commissioner for Human Rights. In their remaining scope, the provisions governing operational surveillance have been challenged by the Commissioner for Human Rights in its application of 4 December 2015 (ref. K32/15). Despite the amendment of the provisions governing operational surveillance, the first and third pleas in law raised in the application of 4 December 2015 remain valid. The second plea in law required a correction, therefore it has been included in this application.

I. The non-conformity of Article 19 para 9 of the Act of 6 April 1990 on the Police; Article 9e para 10 of the Act of 12 October 1990 on the Border Guard; Art. 36c para 7 of the Act of 28 September 1991 on Fiscal Control; Article 31 para 10 of the Act of 24 August 2001 on Military Police and Military Law Enforcement;

Article 17 para 9 of the Act of 9 June 2006 on the Central Anticorruption Bureau - in so far as they allow the extension of operating surveillance for consecutive periods whose total length cannot exceed 12 months, which in turns means the ability to conduct operating surveillance for 18 months – with Article 2, Article 47, Article 49, Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution of the Republic of Poland;

The provisions challenged in this part of the application govern the issue of the duration of operational surveillance. The amended provisions of the Acts on the Police, Border Guard, Fiscal Control, Military Police and Military Law Enforcement, the Central Anticorruption Bureau provide that operational control may be renewed beyond its basic duration, if new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime have appeared during the application of operating surveillance. In such cases, courts can issue subsequent regulations on the extension of operating surveillance for consecutive periods whose total length cannot exceed 12 months.

In the opinion of the Commissioner for Human Rights, the provisions governing the duration of operational control and inconsistent with Article 2, Article 47, Article 49, Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution.

The possibility of a disproportionately long term of using operational surveillance in the first place infringes the principle of democratic rule of law and, above all, the resulting principle of citizens' trust in the state and the principle of the rule of law.

As concluded by the Constitutional Tribunal: "(...) the principle of trust in the state and the law laid down by it is based on the requirement of legal certainty, therefore such a combination of characteristics conferred by the law, which provide the individual with legal certainty; they allow the individual to decide on their actions on the basis of complete knowledge of the circumstances surrounding the actions of state authorities and the legal consequences the individual's actions may entail" (judgement of the Constitutional Tribunal of 14 June 2000, P 3/00). The principle of trust in the state cannot be understood only in a formal way, as the procedurally correct adoption of provisions, and the publication thereof, regardless of their content. The substantive aspect of legislative activities, taking into account the scope of regulatory activities of the legislature, its contents and the decisions taken in relation to democratic standards and the rule of law, is of fundamental importance from the perspective of the citizen and their relation to the state. There's a reason it is called otherwise the principle of the citizens' loyalty to the state. The substantive aspect of the principle of the citizens' trust in the state is pointed out *expressis verbis* by Wojciech Sokolewicz: "The principle of trust (loyalty) refers not only to the procedure and form of the adopted law. The entire process of the application of the law, beginning with its interpretation, should be carried out in compliance with this principle" (W. Sokolewicz, *Komentarz do art. 2,* [in:] L. Garlicki (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, vol. V Warsaw 2007, p. 34. Cf. also judgement of the Constitutional Tribunal of 27 November 1997, ref. U 11/97). As it seems, the principle of citizens' trust in the state should be understood even wider. It consists of not only formally appropriate process of legislation, the introduction of vacatio legis and the stability of interpretation. The principle of loyalty is realized already at the stage of the formulation of the content of the provisions. There is no way to maintain the relationship of trust and loyalty, if a state is shaping up its powers in such a way as to seriously interfere in the freedom and rights of citizens, not indicating the limits of the use of these powers, or setting limits in excess of the principle of proportionality. This problem is noticeable in the context indicated in this application. The transfer of the message to citizens that they could be kept under surveillance by the police and state services for eighteen months certainly builds no confidence trust between the state and its citizens. A major influence on the problems in this relationship is that the citizen will not,

even subsequently, be informed of operational surveillance activities carried out in respect of him. The information will not be provided even if no circumstances have been found that might have justified the initial suspicion, which led to the filing of the request to the Court and the launch of operational surveillance. The Constitutional Tribunal, in its judgement of 30 July 2014, allowed the differentiation between standards of conduct in terms of operational investigation, especially if it is carried out by the states responsible for state security. However, this does not mean that the state can totally abandon the requirement, resulting from human rights, to determine a maximum period of conducting operational and investigative activities against individuals. This period could be longer than in the case of the other services, but it should be specified.

Taking the above into account, in the opinion of the Commissioner for Human Rights, the period of operations within the scope of operational surveillance, referred to in the provisions, exceeds the framework necessary in a democratic state of law.

The possibility of using operational surveillance over such a long period raises serious doubts from the perspective of freedom and human rights. Therefore, it is necessary to reconstruct the list of goods interfered with by the legislature, as well as the goods colliding with them, which could justify the introduced regulation. The final settlement of such a shaped collision is possible on the basis of Article 31 para 3 of the Constitution, and so using the principle of proportionality.

The first apparent benchmark is the right to privacy. In accordance with Article 47 of the Constitution, 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. The literature mentions that the legal protection covers all aspects of an individual's life in the areas indicated in Article 47 of the Constitution. The right to privacy has repeatedly been a benchmark in the proceedings before the Constitutional Tribunal, also in matters relating to the collection and processing of information about an individual. In its judgement of 20 January 2015, the Constitutional Tribunal noted that: "Acting as one of the basic elements of the axiology of the democratic rule of law, constitutional protection of privacy is, in particular, the opportunity to make independent decisions on the disclosure to other parties of information about oneself, as well as control over the information, even if they are in possession of other people (information autonomy of individuals) and the possibility of self-determination about one's personal life in an objective, subjective and time context (decision-making autonomy of an individual). In the sphere of informational autonomy, constitutional norms

guarantee the protection of an individual against acquiring, processing, storing and disclosing, in a way that violates the rules of suitability, necessity and proportionality in the strict sense, including information about: a) health (cit. judgements ref. U 5/97, U 3/01); b) financial situation (cit. judgements ref. K 21/96, K 41/02); c) family situation (cit. judgements ref. SK 40/01, K 20/03);d) political or social past (cit. judgements ref. K 24/98, K 01/07, K 31/04); e) name or image (cit. judgement ref. K 17/05, K 25/09) or any other information necessary for the activities of public authorities (cit. judgements ref. K 4/04; K 45/02, K 54/07, K 33/08). In the sphere of decision-making autonomy, constitutional norms guarantee the protection of an individual against interference in the decisions of an individual - made in violation of the rules of suitability, necessity and proportionality in the strict sense - among others, about: a) own life or health (cit. judgement ref. SK 48/05, K 16/10); b) shaping family life (cit. judgements ref. K 1/98; K 18/02);c) the education of children in conformity with one's own convictions (i.a. quoted judgement ref. U 10/07) d) the birth of a child (cf. judgement ref. K 26/96) "(Constitutional Tribunal's judgement of 20 January 2015, ref. K 39/12). In light of this decision there can be no doubt that the autonomy of information and decision-making autonomy of an individual must be taken into account when assessing the compatibility of the challenged provisions with the Constitution of the Republic of Poland. It is also obvious that the operating surveillance activities interfere in such a reconstructed human autonomy, rooted in the principle set out in Article 47 of the Constitution.

The right to privacy was also one of the fundamental benchmarks of the proceedings leading to the judgement of the Constitutional Tribunal of 30 July 2014. In light of this decision it is clear that it is unacceptable to presume the competence of public authority in the area of interference in the privacy of the individual. Not only state authorities, but also private entities must refrain from such interference. The findings of the Constitutional Tribunal leave no doubt: "(...) obtaining information on the private lives of individuals by public authorities, especially covertly, must be limited to necessary situations, permitted in a democratic state only for the protection of constitutionally recognized values and in accordance with the principle of proportionality. Conditions for the collection and processing of data by public authorities must be regulated in a statute in a most transparent way, which excludes arbitrariness and discretion of their use" (judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11; cf. also Supreme Court judgement of 25 June 2015, ref. V CSK 507/14, Legalis no. 1337785).

While reconstructing the benchmark from Article 47 of the Constitution, it is impossible not to refer to Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, which states as follows: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." This provision has repeatedly been the subject of consideration by the European Court of Human Rights, in the context of the issue of operational and investigative activities. In its judgement of 28 June 2007, the Court found that the right to privacy and the clause of Article 8 § 2 of the Convention requires that any privacy restrictions involving the conduct of operational and investigative activities against an individual resulted from that are clear, precise, accessible to the individual. Moreover, the frame of the surveillance should be reasonable (ECtHR judgement of 28 June 2007, in The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, No. 62540/00). The Court in that judgement expressly pointed out that the rules must specify the duration of the surveillance (Cf. also other judgements concerning operational surveillance and data retention: judgement of ECtHR of 4 May 2000 in Rotaru v. Romania, No. 28341/95; judgement of the ECtHR of 16 February 2000, in Amann v. Switzerland, No. 27798/95). The European Court of Human Rights, in its judgement of 21 June 2011, stated that "private life may even include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life” (ECtHR judgement of 21 June 2011, in Shimovolos v. Russia, No. 30194/09). It is impossible not to refer also to Article 17 of the International Covenant on Civil and Political Rights. The UN Human Rights Committee has repeatedly appealed to this pattern, indicating weaknesses in the operational and investigative activities conducted by the state (cf. opinions on the reports submitted by the states pursuant to art. 40 of the ICCPR: USA - opinion of 18 December 2006, ref. CCPR/C/USA/CO/3/Rev. 1, pt. 21; the Netherlands - opinion of 25 April 2009, ref. CCPR/C/NLD/CO/4, pt. 15; Sweden - opinion of 7 May 2009, ref. CCPR/C/SWE/CO/6, pt. 18; France - opinion of 17 April 2015, Ref. CCPR/C/FRA/CO/5, pt. 13).

With this in mind, the Commissioner for Human Rights has no doubt that the provisions challenged in this application constitute an interference with the rights of the reconstructed from Article 47 of the Constitution and Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The provisions that are the subject of this plea in law also raise serious doubts in the light of Article 49 of the Constitution, which states that: "The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute." Freedom of communication already in its essence contains confidentiality involving the "prohibition of forcing recipients to disclose the content of received messages, and on the prohibition addressed to all other parties, including public authorities, of attempting to inform about these contents without the consent of the addressee. What's more, it also includes the confidentiality of the fact that one is the addressee of specific messages at all" (P. Sarnecki, *Komentarz do art. 49,* [in:] L. Garlicki (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* vol. III, Warsaw 2003, p. 3). Freedom and confidentiality of communication is closely linked with human dignity, defining it as an autonomous legal entity, essentially using his freedom and forming relationships with other people. The use of operational surveillance interferes with the freedom and privacy of communication. The determination that it is a good very similar to human dignity, strongly rooted in it, allows to say that any interference must be justified and solidly anchored in another good highly vested in the constitutional hierarchy of protected goods. Such conditions must apply with the provisions governing the duration of operational surveillance. The longer the period of permissible conduct such operations, the greater the justification referring to the constitutional system of goods must be.

According to the Commissioner for Human Rights, 18-month-long long periods of surveillance by the aforementioned services constitute a breach of Article 49 of the Constitution.

Another benchmark is found in Article 51 para 2 of the Constitution, which prohibits the acquisition, collection and sharing of information on citizens other than necessary in a democratic state ruled by law. This provision is a natural consequence of the right to privacy (P. Sarnecki, *Komentarz do art. 51,* [in:] L. Garlicki (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* vol. III, Warsaw 2003, p. 2). Difficulties may be arise when setting out the criteria for the selection of data that are "necessary in a democratic state of law." The literature suggests the following directive of interpretation: "if the scope of similar information systems

becomes too wide for the convenience of the administration (surveillance <<just in case>> of wider social groups, uniform <<information account>> of a citizen arising from the integration of hundreds of administrative data from different fields) or the detail of data leads to the creation of <<personal profiles>> (simplified characteristics of an individual), and finally reaches the covert or overt designation of citizens using identification numbers not by order numbers, but meaningful ones, we have a chance to go beyond what is necessary in a democratic state ruled by law" (I. Lipowicz, [in:] J. Boć, *Konstytucje Rzeczypospolitej Polskiej oraz komentarz do KonstytucjiRP z 1997 r.*, Wroclaw 1998, p. 99). When examining necessity in a democratic state, one should also take into consideration the duration of activities in the field of operational surveillance provided for in the legislation. It does not seem reasonable to assume that in the light of Article 51 para 2 of the Constitution it is possible to conduct operational surveillance without reasonable time limits. In the opinion of the Commissioner for Human Rights, the criterion of reasonable time limits, under Article 51 para 2 of the Constitution, is not met by the statutory provisions listed in petitum of the application.

The interference in the rights and freedoms of man and citizen, reconstructed from Article 47, 49 and 51 para 2 of the Constitution, should be examined in the light of the criteria set out in Article 31 para 3 of the Constitution, which enshrines the principle of proportionality. As repeatedly pointed out by the Constitutional Tribunal in its case-law, the principle of proportionality contained in Article 31 para 3 of the Constitution requires firstly that the restrictions on the exercise of constitutional rights and freedoms be introduced in the form of a statute, which excludes their normalization using acts of lower rank. Secondly, in substantive aspects this principle allows the establishment of only such restrictions, which do not affect the substance of a given freedom or subjective right, and only when there is a need for their introduction in a democratic state for its security or public order, or to protect the environment, health, public morals, or the freedoms and rights of others. Importantly, the scope of the restrictions should be proportionate, i.e. necessary to achieve a particular purpose. Accordingly, three criteria are reconstructed: relevance, necessity and proportionality in the strict sense of the adopted limitations. Such interference is admissible if it is able to bring the intended effects, it is necessary to protect the public interest with which it is associated, and its effects are proportionate to the burdens imposed by it on the citizen (cf. among others. judgement of the Constitutional Tribunal of 3 June 2008, ref. K 42/07, judgement of the Constitutional Tribunal of 29 September 2008, ref. SK 52/05; cf. also K. Wojtyczek, *Zasada proporcjonalności jakogranica prawa karania,* [in:] A. Zoll (ed.), *Racjonalna reforma prawa karnego,* Warsaw2001, p. 297; M. Piechowiak, *Klauzula limitacyjna a nienaruszalność praw i godności*, „Przegląd Sejmowy" 2009, no. 2, pp. 56-57; A. Stępkowski, *Zasada proporcjonalności weuropejskiej kulturze prawnej*, Warsaw 2010, p. 194; A. Zoll, *Konstytucyjne aspekty prawakarnego,* [in:] T. Bojarski (ed.), *Źródła prawa karnego. System Prawa Karnego,* vol. 2, Warsaw 2011, pp. 237-241).

Due to the fact that any regulation concerning the activities of public authorities in the area of operational surveillance leading to restrictions on the exercise of freedoms and rights, the penal legislature must prove in each case that the proposed regulatory decision meets the criteria of the proportionality test. The legislature should first determine the purpose of the proposed standard, demonstrate its necessity in the light of the intended purpose, its usefulness in attaining it, and finally test the preference implied by the collision between the good, which it wants to protect, and the good associated with the rights and freedoms that the planned regulation prejudice.

The legislature bears the burden of proof to demonstrate that a measure interfering with the rights and freedoms of man meets the criteria of the principle of proportionality. In the opinion of the Commissioner for Human Rights, the provisions at issue in this part of the application, to the extent that they determine the duration of the operational surveillance for a total of eighteen months do not meet the criterion of necessity. Also, the principle of proportionality in the strict sense will be maintained only when the interference with the rights and freedoms will take place within a reasonable time frame. It is difficult to assume that police services and special services need until eighteen months to collect material justifying the initiation of criminal proceedings. One has to remember that the Code of Criminal Procedure also provides for the possibility of using measures from the field of operational surveillance, however, in a manner surrounded by procedural safeguards, in the regime of criminal procedure.

In the opinion of the Commissioner the following provisions are also unconstitutional: Article 27 para 9 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (Journal of Laws of 2015, item 1929, as amended) and Article 31 para 7 of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of 2014, item 253, as amended) in so far as they do not define the upper limit of the duration of operational surveillance.

The issue has become the subject of a plea in law in the Commissioner's application to the Constitutional Court of 4 December 2015. (Ref. No. K 32/15).

II. The non-conformity of Article 19 para 15h of the Act of 6 April 1990 on the Police; Article 9e para 16h of the Act of 12 October 1990 on the Border Guard; Article 36c para 1h of the Act of 28 September 1991 on Fiscal Control; Article 31 para 16h of the Act of 24 August 2001 on Military Police and Military Law Enforcement; Article 27 para 15j of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency; Article 31 para 14h of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service; Article 17 para 15h of the Act of 9 June 2006 on the Central Anticorruption Bureau - in so far as they use a vague criterion of the "interest of the criminal justice system" and do not specify the weight of circumstances to be determined on the basis of materials that may to contain information referred to in Article 178a, Article 180 § 2 and Article 180 § 3 of the Code of Criminal Procedure – with Article 2 of the

Constitution, with Article 42 para 2, Article 47, Article 49, Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution and Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

The provisions contested in this part of the application provide a mechanism requiring the courts to issue an order concerning the approval for the use in criminal proceedings of materials containing information constituting secrets related to profession or functions referred to in Article 180 § 2 of the Criminal Procedure Code, not covered by the prohibitions laid down in Article 178a and Article 180 § 3 of the Criminal Procedure Code with the exception of information on offences referred to in Article 240 § 1 of the Penal Code, whenever it is necessary for the interest of the justice system, and this fact can not be determined on the basis of other evidence. The issue of such order takes place on the basis of a request filed by a prosecutor or the Public Prosecutor General (depending on factual and legal arrangement of a given case) to use the aforementioned materials in criminal proceedings.

In the context of legislation which is the subject of this application, it must first be noted that so far a uniform and perpetuated the practice of jurisprudence in the application of operational surveillance to persons obliged to to observe professional secrecy has not been developed. There are also no uniform rules for dealing with materials containing information covered by professional secrecy. From the judicial practice it shows that courts often do not even have considered whether the person subject to the operational surveillance are not covered by evidence bans. Such conclusions can be drawn, among others, from the letter of 19 December 2013 addressed by the Constitutional Court to the presidents of all courts of appeal, as well as the presidents of district courts established in the cities that are the seats of appellate courts (Section 3.11.1 of the Constitutional Tribunal's judgement of 30 July 2014, ref. K 23/11).

In addition, in the aforementioned judgement, the Constitutional Tribunal drew attention to the need to require prior consent for the acquisition of telecommunications data of persons obliged to observe professional secrecy. As the Constitutional Tribunal indicates, it is necessary to introduce regulations enabling the sharing of such data to police services and state security authorities only after obtaining the consent to the provision of information by an independent body.

The provisions indicated in this plea of law are one of the most extreme and the most severe forms of interference in the freedoms and rights of individuals. They touch a particularly sensitive matter related to the

professional activity of an individual. The unique nature of the information relating to the professional conduct or the duties of a particular position is determined by the fact that these messages mostly affect financial and private interests of great importance for the operation and safety of the wide groups of individuals. In addition, even when these messages are only relevant to individual entities, they are often relevant in relation to issues fundamental to their functioning, such as the protection of private life and financial interests, criminal liability and civil liability.

The provisions indicated in this plea provide for the obligation of admitting the use of materials covered by professional secrecy or related to performed duties in criminal proceedings by a court. Such an admission should occur whenever it is necessary for the interest of the justice system, as long as the circumstance can not be determined on the basis of other evidence.

An identical criterion is used by Article 180 § 2 of the Code of Criminal Procedure, which provides for the possibility of questioning of persons obliged to preserve notary secrets, attorney-client privilege, tax advisory, medical, journalist or statistical secrets. There is a fundamental difference between these regulations, consisting in the fact that while in the case of Article 180 § 2 of the Code of Criminal Procedure, it is the court who decides on the admissibility of interfering with professional secrecy in order to use certain information for the purpose of criminal proceedings, the mechanism provided for in the provisions of the challenged act, the court decides not on the release from such secrecy, but only on the admissibility of certain information previously obtain as a result of a breach of professional secrecy in criminal proceedings.
Obtaining secret information can occur without the special permission of the court, and the results of that surveillance of relevance for the emergence of criminal responsibility are only secondarily "legalized" by the court through their approval for use in criminal proceedings. Moreover, the challenged provisions – in contrast to Article 180 of the CPC – do not provide for any possibility of appeal against the court's decision on the admission of evidence based on information covered by professional secrecy.

The solution adopted as a result of the amendment of the Police Act and some other acs seems to gravely violate the principle of a democratic state ruled by law expressed in Article 2. Although the regulation provided for in Article 180 § 2 of the Code of Criminal Procedure provides for a mechanism for alleviating the interference in professional secrecy through the prior control of the legitimacy of such interference by the court, nonetheless many doubts have been raised in relation to this provision by the scientific community of criminal law. The literature has repeatedly pointed out that the social importance of secrecy, referred to in 180 § 2 of the Code of Criminal Procedure, requires the introduction of additional criteria emphasizing the importance and relevance of the information disclosed in a criminal trial (D. Gruszecka, *Komentarz do art. 180 Kodeksu postępowania karnego* [in:] *Kodeks postępowania karnego. Komentarz*, Warsaw 2015, p. 420).

In this context, the decision of the legislator to introduce an abstract value in the form of the interest of the justice system as a criterion for the admissibility of the use of information obtained through a breach of professional secrecy in criminal proceedings should raise serious concerns. A threat to the protection of the rights and freedoms of the individual is enhanced by the fact that the legislature chose not to accurately determine the weight of circumstances, to be determined on the basis of materials likely to contain information referred to in Article 178a, Art. 180 § 2 and Article 180 § 3 of the Code of Criminal Procedure.

The current legal situation seems to create room for freedom unfettered by formal restrictions in terms of interference in the information covered by professional confidentiality of entities endowed with high trust from the society. Meanwhile, the Constitutional Tribunal, in its judgement of 30 July 2014 (K 23/11), clearly indicated that the collection of classified information can only be justified for the purpose of criminal prosecution for serious crimes and threats to national security. Similar position was presented by the European Court of Justice in its judgement of 8 April 2014 (C-293/12). In a series of rulings as to the unconstitutionality of formulating premises defining the permissible interference in the transmission of data in a too general and abstract manner a similar position was taken by the recent judicature of many constitutional courts of EU Member States. (cf. judgement of the Constitutional Court of Bulgaria of 12 March 2015 (8/2014); judgement of the Constitutional Court of Romania, December 8, 2009 (No. 1258); in this spirit also the judgement of the Federal Constitutional Court of Germany of 2 March 2010 (ref. no. 1

BvR 256/08); judgement of the Constitutional Court of Austria (ref. G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012). Ambiguity as to the weight of circumstances to be determined on the basis of materials likely to contain information covered by professional secrecy and the abstractness of the term "interest of the justice system" flagrantly violate the constitutional principle of trust in the state. The discussed regulations do not provide for any safeguards of their rights and freedoms. The essence of operational and investigative activities negates the possibility of informing the persons who are the object of such actions and that is why the primary responsibility of the state in this regard is the establishment of an efficient mechanism of a kind of self-control of its bodies and the protection of individuals from the surveillance activities. If the interference in individuals' rights and freedoms, by definition, is to take place without their knowledge, the role of the state, as the guarantor of rights and freedoms, is to establish a control mechanism by means of a body independent from other state entities interested in obtaining information through surveillance.

Using information covered by professional secrecy for the purpose of criminal proceedings on the basis of extremely vague criteria becomes especially dangerous from the point of view of protection of the rights and freedoms of individuals in the field of information covered by professional secrecy of some of the legal profession. The mechanism of obtaining such information by means of operational surveillance carried out in relation to advocates and legal advisors may lead to a serious violation of one of the fundamental individual rights in a state of law – the right to defence (Article 42 para 2 of the Constitution). In the light of Article 6 para 1 of the Act of 26 May 1982 – The Law on the Advocates' Profession (i.e. Journal of Laws of 2015, item 615): "An advocate is obliged to maintain the confidentiality of everything he learnt in the course of providing legal assistance." In turn, in accordance with Article 3 para 3 of the Act of 6 July 1982 – on Legal Advisors (i.e. Journal of Laws of 2015, item 507): "A legal advisor is obliged to maintain the confidentiality of everything he learnt in the course of providing legal assistance". Due to the fundamental importance of legal professional privilege for the legal situation of persons directly concerned by the confidential information, it is necessary to detail specific requirements as to the mode and circumstances to repeal the obligation to maintain such confidentiality. Meanwhile, the procedure provided for in Article 19 para 15h of the Act on the Police, Article 9e para 16h of the Act on the Border Guard, Article 36d of the Act on Fiscal Control, Article 31 para. 16h of the Act on Military Police and Military Law Enforcement, Article 27 para 15j of the the Internal Security Agency and the Foreign Intelligence, Article 31 para 14h of the Act on

the Military Counterintelligence Service and the Military Intelligence Service and in Article 17 para 15h of the Act on the Central Anticorruption Bureau does not seem to meet any of the above requirements. The interference in professional secrecy alone is handled in the absence of any control mechanism. Equally worrying is the fact that verification of the possibility of using the information covered by professional secrecy for the purpose of criminal proceedings is based on an imprecise criterion of the interest of the justice system. The abstractness of this criterion requires the court ruling on the admissibility of the use of such information to each time weigh two values - the individual's right to defence and the collective interest of the justice system. Leaving aside the accuracy collectivist–objective recognition of the interest of the justice system, it can be assumed that a collision of the aforementioned goods should almost always be decided for the benefit of the above-individual good of major importance for the smooth functioning of the entire state apparatus. The interest of the justice system consists of all possible situational arrangements of legal and factual nature, which can in any way contribute to the realization of basic tasks and objectives of the administration of justice. In this context, there should be no doubt that the ruling on the admissibility of the use for the purposes of criminal proceedings of information covered by legal professional privilege, the court will have to refuse priority to the individual interest for the sake of the interest of the justice system which is one of the aspects of abstract common good. An extremely general recognition of legal rights of a collective nature, which can not be assigned with even a particular set of specific values is an extremely dangerous phenomenon, leading to striking out individually recognized goods by mechanisms executing their adherence. Therefore, the challenged regulations will lead the courts to a simple alternative - either admit the use of materials containing information covered by professional confidentiality in criminal proceedings, or undermine the importance of the correct functioning of the entire justice system and to admit the priority of an individual right to defend each individual is entitled to (unless, of course, a circumstance can not be determined on the basis of other evidence). At the same time, the interest of the justice system itself includes the right to defence as one of the conditions for a fair trial, which stands at the foundation of the interests of the justice system.

Ambiguity of reasons for this, which gives rise to the the obligation, on the side of the court, to immediately admit materials containing information constituting secrets related to the exercise of a profession or function to use in criminal proceedings is also a violation of the constitutionally guaranteed

right of every individual to the protection of private life (Article 47 of the Constitution). There is also no doubt that the ambiguity of circumstances put forward in this regard constitutes a violation of Article 49 and 51 para 2 of the Constitution. The Constitutional Tribunal expressly noted that the constitutional protection conferred by Article 47, Article 49 and Article 51 of the Constitution are covered by "all the ways of transmitting messages in any form of communication, regardless of their physical media (e.g. personal and telephone conversations, written correspondence, fax, text and multimedia messages, e-mail). Constitutional protection covers not only the message, but also all the circumstances of the communication process, which include personal data of the participants in this process, information on selected phone numbers, viewed web pages, data showing the time and frequency of connections, or allowing the geographical localization of call participants, finally, data about the IP number or IMEI number" (judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11). In the same judgement, the Constitutional Tribunal also pointed out clearly that the protection against implicit monitoring of an individual is also within the constitutionally guaranteed freedoms of man and his autonomy of information.

III. The non-conformity of Article 20c para 1 and Article 20cb para 1 of the Act of 6 April 1990 on the Police, Article 10b para 1 and Article 10bb para 1 of the Act of 12 October 1990 on the Border Guard, Article 36b para 1 and Article 36bb para 1 of the Act of 28 September 1991 on Fiscal Control, Article 30 para 1 and Article 30c para 1 of the Act of 24 August 2001 on Military Police and Military Law Enforcement, Article 28 para 1 and Article 28b para 1 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, Article 32 para 1 and Article 32b para 1 of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, Article 18 para 1 and Article 18b para 1 of the Act of 9 June 2006 on the Central Anticorruption Bureau, Article 75d para 1 and Article 75db para 1 of the Act of 27 August 2009 on the Customs Service, with Article 2, 20, 47, 49, 51 para 2 in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the EU Charter of Fundamental Rights

The act amending the Police Act adopted on 15 January 2016 has made changes in Article 20c para 1 of the Act on the Police, Article 10b para 1 of the Act on the Border Guard, Article 36b para 1 of the Act on

Fiscal Control, Article 30 para 1 of the Act on Military Police and Military Law Enforcement, Article 28 para 1 of the Act on the Internal Security Agency and the Foreign Intelligence, Article 32 para 1 of the Act on the Military Counterintelligence Service and the Military Intelligence Service, Article 18 para 1 of the Act on the Central Anticorruption Bureau and Article 75d para 1 of the Act on Customs Service.

In its wording applicable after the amendment of the Police Act, pursuant to Article 20c para 1, the legislature admitted the police the right to obtain data that do not constitute the contents of, respectively, telecommunications, postal items or transmissions within a service provided by electronic means, as well as to process these information without the knowledge and consent of the person concerned. This right has been granted for the prevention or detection of crimes or for the purpose of saving human life or health, or the support of search or rescue operations. The data that the Police has been granted access to are defined, respectively, in:

- Article 180c and Article 180d of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws of 2014, item 243, as amended, hereinafter referred to as: Telecommunications Law) – the so-called "telecommunications data",
- Article 82 para 1 pt. 1 of the Act of 23 November 2012 – Postal Law (Journal of Laws, item 1529, and of 2015, item 1830, hereinafter referred to as: Postal Law) – the so-called "postal data",
- Article 18 para 1-5 of the Act of 18 July 2002 on Providing Services by Electronic Means (Journal of Laws of 2013, item 1422, and of 2015, item 1844, hereinafter referred to as: PSEM Act) – the so-called "Internet data".

Analogous powers to obtain and process data have been granted to other services:

- Border Guard – in order to prevent or detect criminal offences (Article 10b para 1 of the Act on the Border Guard),

- Fiscal control – in order to prevent or detect tax offences or offences referred to in Article 2 para 1 pt 14b and Article 36c para 1 pt. 3 of the Act on Fiscal Control (Article 36b para 1 of the Act on Fiscal Control),

- Military Police – for the prevention or detection of crimes, including fiscal offences, committed by persons referred to in Article 3 para 1 pt. 1, 3, 4, 5, 6 or in order to save human lives or health, or in

support of search or rescue operations (Article 30 para 1 of the Act on Military Police and Military Law Enforcement),

- the Internal Security Agency – in order to carry out tasks referred to in Article 5 para 1 (Article 28 para 1 of the Act on the Internal Security Agency and the Foreign Intelligence Agency),
- the Military Counterintelligence Service – in order to carry out tasks referred to in Article 5 (Article 32 para 1 of the Act on the Military Counterintelligence Service and the Military Intelligence Service),
- Central Anticorruption Bureau – in order to carry out tasks referred to in Article 2 (Article 18 para 1 of the Act on the Central Anticorruption Bureau),
- Customs Service – in order to prevent or detect fiscal offences referred to in Chapter 9 of the Penal and Fiscal Code (Article 75d para 1 of the Act on the Customs Service).

Moreover, in accordance with Article 20cb para 1 of the Act on the Police, as well as, respectively, Article 10bb para 1 of the Act on the Border Guard, Article 36bb para 1 of the Act on Fiscal Control, Article 30c para 1 of the Act on Military Police and Military Law Enforcement, Article 28b para 1 of the Act on the Internal Security Agency and the Foreign Intelligence, Article 32b para 1 of the Act on the Military Counterintelligence Service and the Military Intelligence Service, Article 75db para 1 of the Act on Customs Service, the services will be allowed to collect – for the prevention or detection of crimes or for the purpose of saving human life or health, or the support of search or rescue operations (with respective modifications in particular statutes):

- from the list referred to in Article 179 para 9 of the Telecommunications Law – i.e. the electronic directory of subscribers, users or network termination points, taking into account the data obtained at the conclusion of an agreement, referred to in Article 161 of the Telecommunications Law – subscriber's data a provider of publicly available telecommunications services is authorised to process (personal data),
- in the case of a user who is not a natural person – the number of a network termination point and the seat or place of conducting business activity, the legal business name and trading name, as well as the organisational form of this user, in the case of fixed public telecommunications network – also the name of the city and street, where the network termination point provided to the user is located.

When analysing the provisions indicated one should begin by saying that in Article 20c para 1 of the Act on the Police (and similarly the other provisions of the indicated acts) do not fulfil the criteria for

justifying the limiting of the rights and liberties under the Constitution, which questions the compatibility of Article 20c para 1 of the Police Act and the other indicated provisions with Article 2, 30, 47, 49, 51 para 2 of the Constitution in conjunction with Article 31 para 3 and Article 8 of the ECHR, as well as Article 7 and 8 in conjunction with Article 52 para 1 of the CFR EU.

As indicated above, the Act on the Police provides for the admissibility of telecommunications data, postal data and Internet data for the purposes set out in the contested provisions. The acquisition of data, referred to in article 20cb para 1 of the Act on the Police is to serve the same purpose.

When analysing the catalogue of offences for which it is permissible to obtain and process such data in relation to individual services, it is clear that it is excessively wide, which indicates the exceeding of limits referred to in Article 31 para 3 of the Constitution, Article 8 para 2 of the ECHR and Article 52 para 1 of the CFR UE. Article 20c para 1 of the Act on the Police does not indicate individual types of prohibited acts, but uses the general term "offence". This means that the Police can obtain data in relation to all offences that meet the criteria of a crime. Therefore, it will constitute an excessive interference in the right to privacy and the right to protection of personal data, as well as a breach of the principle of autonomy, as expressed in Article 47, 49 and 51 para 2 of the Constitution, which also constitutes a violation of the principle of human dignity referred to in Article 30 of the Constitution.

For similar reasons, the following provisions should be considered incompatible with the indicated above constitutional benchmarks and standards set out in the ratified international agreements:

- Article 10b para 1 and Article 10bb para 1 of the Act on the Border Guard, containing the general term "offence",
- Article 36b para 1 and Article 36bb para 1 of the Act on Fiscal Control, containing a very general reference to fiscal offences,
- Article 30 para 1 and Article 30c para 1 of the Act on Military Police and Military Law Enforcement, containing a general reference to offences, including fiscal offences,
- Article 28 para 1 and Article 28b para 1 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, containing a reference to tasks specified in Article 5 para 1 of the Act on the Internal Security Agency and the Foreign Intelligence Agency;

It should be noted that this reference means that the Internal Security Agency will be able to obtain data not only in order to recognize, prevent and detect criminal offences, but also to implement its other statutorily defined tasks, such as: recognising, preventing and combating threats affecting the internal security of the state and its constitutional order; obtaining, analysing, processing and transmitting information that may have significant implications for the protection of the internal security of the state and its constitutional order to competent authorities; undertaking other actions specified in separate statutes and international agreements,

- Article 32 para 1 and Article 32b para 1 of the Act on the Military Counterintelligence Service and the Military Intelligence, referring to tasks set out in Article 5 of the Act on the Military Counterintelligence Service and the Military Intelligence; this reference means that the Military Counterintelligence Service will be able to obtain data not only in order to recognise, prevent and detect certain crimes, but also in order to carry out its other statutorily defined tasks, such as tasks provided for the Military Counterintelligence Service in other statutes, as well as international treaties, which bind the Republic of Poland;
- Article 18 para 1 and Article 18b para 1 of the Act on the Central Anticorruption Bureau, which allows obtaining data for the execution of tasks referred to in Article 2 of the Act on the Central Anticorruption Bureau. This reference means that the Central Anticorruption Bureau will be able to obtain data not only to recognise, prevent and detect crimes specified in the statute, but also in order to carry out its others statutorily defined tasks, such as conducting analytical activities on the phenomena occurring within the jurisdiction of the Central Anticorruption Bureau and executing other activities specified in separate statutes and international agreements;
- Article 75d para 1 and Article 75db para 1 of the Act on the Customs Service, containing a reference to fiscal offences referred to in Chapter 9 of the Penal and Fiscal Code. It should be noted that the provisions of Chapter 9 determine tax crimes and fiscal misdemeanours against the organization of gambling. The analysis of the list of offences referred to in the provisions of this chapter, leads to the conclusion that at least some of these crimes do not meet the criterion of "sufficient seriousness."

The terms used in these provisions are not only imprecise, but above all, do not comply with the criterion of clarity indicated above. The objective of collecting and processing data specified in such a way

can in fact mean the lack of selectivity both at the stage of starting the collection of Internet data, or the possibility of obtaining data by the services in proceedings on unspecified criminal acts, regardless of their harmfulness. This also means, that it was not guaranteed for the collection and processing of Internet data to be a subsidiary means of obtaining information or evidence about individuals. The lack of subsidiarity of the proposed provisions opens up the possibility of using the telecommunications, postal and Internet data not only when it is really necessary for the detection or prevention of crimes, but also when it is simply the easiest and most convenient solution (cf. judgement of the Constitutional Tribunal in K 32/04 or K 54/07). In conjunction with the provisions on judicial review, which will be discussed further in the application, it should be made clear that the courts will not be able to assess whether reaching for the data in a particular situation was actually necessary and duly justified, which further weakens the level of protection of the privacy of individuals. This issue was also raised by the Constitutional Tribunal in its judgement in case K 23/11 indicating that "the acquisition of classified information about individuals over the course of the operational and investigative activities must be a subsidiary mean, which is used when other solutions are unsuitable or ineffective."

The need to precisely regulate the scope of crimes for which it is permissible to access the data has also been indicated by the ECtHR and the CJEU when interpreting the provisions of the ECHR and the CFR EU. In particular, in the aforementioned case Zakharov v. Russia, the ECtHR pointed out that the premise justifying the finding of violation of Article 8 ECHR is, among others, the lack of clarification of any of the circumstances under which the authorities may conduct surveillance of citizens. In turn, in cases C-293/12 and C-594/12 Digital Rights Ireland, the CJEU, stating the nullity of the retention directive 2006/24/EC in connection with a breach of the requirement of proportionality through the interference in the right to privacy and the right to the protection of personal data, has found that it is not enough to reference "serious crimes" in order to consider the grounds indicated in Article 52 para 1 of the CFR EU to be met and justifying the interference in the rights referred to above.

Therefore, the indicated provisions are incompatible with Article 30, 47, 49, 51 para 2 in conjunction with Article 31 para 3 of the Constitution, as well as with Article 8 of the ECHR and Article 7 and 8 in conjunction with Article 52 para 2 of the CFR EU.

In addition, the indicated provisions also infringe Article 30, 47, 49, 51 para 2 of the Constitution in conjunction with Article 2 of the Constitution containing the principle of the protection of trust in the state and the right set out by it, as well as the principle of certainty through a reference to the definition of the concept of "Internet data", which is not clear and precise, and thus the contested provisions infringe the requirement of predictability of provisions restricting the right to privacy, the right to protection of personal data and the principle of the individuals' autonomy of information. In particular, it should be noted that the concept of "Internet data" is defined through the reference to Article 18 para 1-5 of the Act of 18 July 2002 on Providing Services by Electronic Means (Journal of Laws of 2013, item 1422, as amended). Therefore, this concept includes:

1) personal data of the subscriber necessary for entering in, designing contents, amending or terminating a legal relationship, including the names and surname of the service recipient, the personal number (PESEL) – or if it was not issued – passport number, ID document number or the number of any other document confirming identity, permanent residence address, correspondence address, data used for verifying recipient's electronic signature, electronic addresses of the recipient;
2) other data necessary due to the nature of the provided service of the way of its billing;
3) other data relating to the service recipient, which are not necessary for providing service by electronic means, provided with the consent of the subscriber;
4) the so-called traffic data, characterising the manner of using the service provided by electronic means, including the denotation identifying the service recipient, denotations identifying telecommunications network terminal or tele-information system, which have been used by the service recipient, information about commencement, termination and range of every usage of the service provided by electronic means, information about using of the service provided by electronic means by a service recipient.

The Commissioner for Human Rights wishes to underline that the categories of data referred to in this provision are very general, which may cause ambiguity and lead to a broad understanding of these terms, and – in effect – an excessive interference in fundamental rights. It should be reminded that the law determining the boundaries of state interference in human and citizen rights must meet quality requirements, be available and predictable to individuals – the circumstances and conditions, in which public authorities will access particular data must stem from the law. The precision of legal regulation aims to prevent the risk of the

arbitrariness of actions, inherently beyond the reach of public control. Ambiguities related to the scope of Internet data that can be collected by the services causes that it cannot be considered that the requirement of legal precision has been satisfied.

One must also point out that the indicated wide range of information to which the services will have access, will allow for a broad and precise reproduction of the various aspects of private life. It can also lead to creating personal profile of the people participating in the process of communication, and hence to establish their mode of life, affiliation with social or political organisations, personal preferences or inclinations of people subjected to observation. Acquiring and processing of internet data will not have any relation to any ongoing investigation.

IV. The non-conformity of Article 20c para 3 in conjunction with Article 20c para 2 of the Act on the Police, Article 10b para 3 in conjunction with Article 10b para 2 of the Act on the Border Guard, Article 36b para 3 in conjunction with Article 36b para 2 of the Act on Fiscal Control, Article 30 para 3 in conjunction with Article 30 para 2 of the Act on Military Police and Military Law Enforcement, Article 28 para 3 in conjunction with Article 28 para 2 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, Article 32 para 3 in conjunction with Article 32 para 2 of the Act on the Military Counterintelligence Service and the Military Intelligence Service, Article 18 para 3 in conjunction with Article 18 para 2 of the Act on the Central Anticorruption Bureau, Article 75d para 3 in conjunction with Article 75d para 2 of the Act on Customs Service, with Article 2, Article 20 and with Article 47 and Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution.

Further doubts as to the compatibility of the adopted provisions with Article 2, Article 20 and Article 47 and Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution of the Republic of Poland are raised by those provisions which relate to the conclusion by the telecommunications operators, postal operators or electronic service providers of agreements with the competent bodies of the services (Chief Police Officer and, as appropriate, others in the case of other services).

In particular, it should be pointed out that Article 20c para 3 of the Act on the Police (and, respectively, the other provisions) does not specify the grounds for the conclusion of an agreement, which could mean, in practice, a limitation of the freedom of traders as to refuse the conclusion of an agreement. The provisions of

all these statutes clearly indicate that data sharing has to be done free of charge, which can lead to interference with the principle of freedom of economic activity, expressed in Article 20 of the Constitution by limiting the freedom of undertaking factual and legal actions in the course of business. With regard to the principle of economic freedom resulting from the Article 20 of the Constitution, the Constitutional Tribunal emphasized repeatedly that it is about the activities of individuals (natural persons) and "non-State actors" (or – broadly speaking – non-public actors), which have the right to independently decide to participate in economic life, scope and forms of such participation, including the possible freedom to take different actions of fact and law within the framework of economic activity (cf. judgement of the Constitutional Tribunal, ref K 33/03).

One should also add that the agreements will result in the construction of permanent infrastructure, the so-called "fixed connections", through which services' officers, without the participation of the employees of the service provider or with their necessary participation, will be able freely obtain data indicated in the statutes amended by the Act of 15 January 2016 on the Amendment to the Police Act and Some Other Acts. The provisions allowing for, in practice, unlimited Internet data collection, without the need to subsequently inform individuals whose data were collected, constitute a violation of such fundamental principles as the the rule of law, human dignity and the right to privacy, freedom and the protection of the secrecy of communication or, finally, the protection of personal information. Such a legal situation constitutes a clear violation of Article 47 and Article 51 para 2 of the Constitution. Enabling the police services and special services to maintain fixed infrastructure, leading to a permanent collection of Internet, postal and telecommunications data leads to a constant threat to the right to privacy and the right to protection of personal data. Indeed, it is difficult to argue that privacy and personal data are protected in situations when they can be accessed by officers without any specific conditions and without real control. It is impossible to demonstrate the necessity and proportionality of such regulations. The objectives established by the legislature here, in so far as they are legitimised by the principle of relevance resulting from Article 31 para 3 of the Constitution of the Republic of Poland, can certainly be done in a manner much less dangerous to the citizens, and corresponding to constitutional standards, including in particular those resulting from the benchmarks established in this part of the application.

One must also point out that the obligations imposed on telecommunications operators, postal operators and service providers providing services by electronic means, will in practice apply only to traders established in the territory of the Republic of Poland (Article 3 of the Act on Providing Services by Electronic Means). The fact that the duties referred to in the statute will only apply to a limited circle of actors, does not detract from the seriousness of the allegations raised by the Commissioner for Human Rights. On the contrary, it allows to declare that such a regulation could lead to a situation in which it will be impossible access data held by entrepreneurs established outside the territory of the Republic of Poland, or it will take place without any legal basis at all. This means that the proposed solutions may not be an effective means of preventing and combating crime.

At this stage, those provisions violate the standards of Article 2, Article 20 and of Article 47 and Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution of the Republic of Poland.

V. The non-conformity of Article 20ca of the Act on the Police, Article 10ba of the Act on the Border Guard, Article 36ba of the Act on Fiscal Control, Article 30b of the Act on Military Police and Military Law Enforcement, Article 28a of the Act on the Internal Security Agency and the Foreign Intelligence Agency, Article 32a of the Act on the Military Counterintelligence Service and the Military Intelligence Service, Article 18a of the Act on the Central Anticorruption Bureau, Article 75da of the Act on Customs Service– in so far as they do not provide for the introduction of a mechanism for a real, independent control of data sharing – with Article 2, 47, 51 para 2 in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the Charter of Fundamental Rights of the European Union.

The Act amending the Act on the Police has also added to the aforementioned statutes a provision regulating the exercise of court control over accessing telecommunications, postal and Internet data by the Police and other services. These are – respectively: Article 20ca of the Act on the Police, Article 10ba of the Act on the Border Guard, Article 36ba of the Act on Fiscal Control, Article 30b of the Act on Military Police and Military Law Enforcement, Article 28a of the Act on the Internal Security Agency and the Foreign Intelligence Agency, Article 32a of the Act on the Military Counterintelligence Service and the Military Intelligence Service, Article 18a of the Act on the Central Anticorruption Bureau and Article 75da of the Act

on Customs Service. In accordance with those provisions, control over accessing telecommunications, postal or Internet data is exercised by the district court competent for the seat of the authority of the Police (and other services, with the exception of the Military Police, where control is exercised by the military district court competent due to the established body of the Military Police and the Internal Security Agency and the Central Anticorruption Bureau where the competent court is the District Court in Warsaw and in the case of the Military Counterintelligence Service whose competent court is the Military District Court in Warsaw, Poland), which were provided with the data. The competent body of the Police (and other services) has a duty to provide, without prejudice to the provisions for the protection of classified information, to the competent court, semi-annual reports, including:

1) the number of cases of telecommunications, postal or Internet data acquisition during the reporting period,
2) qualifications of legal acts in connection with which telecommunications, postal or Internet data were requested, or information about obtaining data in order to save human life or health or to support search or rescue activities.

The district court may consult the materials justifying the provision of information to the Police (and other services) of telecommunications, postal or Internet data. The district court shall informs the body of the police (and other services) of the outcome of the inspection within 30 days of its completion. In addition, the regulations lay down a case when data acquisition is not subject to court control (data collected on the basis of article 20cb of the Police Act and, respectively, the provisions of other statutes).

The control procedures indicated in the statutes raise serious doubts of the Commissioner for Human Rights. The issue of ensuring real prior judicial review was considered by the EU Court of Justice in joined cases C-293/12, and C-594/12, where the CJEU concluded clearly – by analysing the provisions of Directive 2006/24/EC – that it has not provided for prior examination of an independent court or an independent administration body, who would be guarding that the sharing and use of data is restricted to cases where it is strictly necessary to achieve the intended purpose and ruled or decided solely upon a justified request made in the context of the proceedings, aimed at the prevention, detection or prosecution of criminal offences. The CJEC considered the lack of prior examination by a court or an independent authority to be an unjustified interference with the fundamental rights laid down in Article 7 and 8 of the CFR EU.

In turn, the Constitutional Tribunal, ruling in K 23/11 in respect of telecommunications data stated clearly that the general constitutional standard does not decide how exactly the access of telecommunications data procedure has to look and, in particular, is it necessary to be in respect of each type of retained data, referred to in Article 180c and Article 180d of the Telecommunications Law to obtain consent to disclosure. Not all data of this kind give rise to the same intensity of interference with the freedoms and human rights. In the Tribunal's view, "the introduction, as a rule, of follow-up inspection – in relation to telecommunications data sharing in the course of the operational and investigative activities – it is not excluded. When regulating this mechanism, the legislature should take account of i.a. the specificity of action and legal responsibilities of individual services, urgent situations in which rapid acquisition of telecommunications data may be necessary to prevent the commission of an offence or its detection. In accordance with the constitutional principle of the functioning of public institutions (preamble of the Constitution) a mechanism should be created that allowed the services responsible for state security and public order to effectively fight against threats. The Tribunal recognises, however, the arguments for the introduction of prior control in some cases. In particular, it may consist in the access to telecommunications data of persons exercising public trust professions, or if there is no urgent action required. These issues, however, must be properly balanced by the legislature".

The provisions relating to individual services indicate the jurisdiction of district courts (or other courts, as appropriate) in a follow-up mode. This control has to rely on an analysis of the semi-annual reports, to be submitted to the courts by the services. It should be noted that in the case of statutes contested in the application, the legislature has not undertaken any balancing as to the need for prior checking, and – with regard to follow-up control - constructed it in such a way that in practice it may be illusory in nature. Semi-annual reports of services directed to the competent court on the basis of the provisions on the protection of classified information will not constitute public information, although it will include information about the number of cases of acquisition of telecommunications, postal or Internet data the nature of the data in the reporting period, as well as the legal qualification of the acts in connection with the conduct of which data is requested. Carrying out control activities by the courts will be optional and not mandatory. In addition, the court – after the inspection – will be able only to inform the controlled service of the results of the control, but it will not be able to order the destruction of the collected data.

It seems that the large scale of the obtained data and a relatively large intervening period, this check may be in fact illusory in nature and does not meet the requirements resulting from the Constitution of the Republic of Poland, and also referred to international agreements. The proposed form of control is therefore insufficient. Follow-up inspection should not be used by default, but can be allowed only exceptionally, in situations where there is a need for immediate action. Challenged provisions shall not in any event provide for prior checks. Thanks to this mechanism, the cases of accessing data could be subject to a fair evaluation in terms of fulfilment of the criteria of necessity, adequacy and appropriateness. It should be underlined that, in accordance with Article 3 para 2 of the Constitution of the Republic of Poland, public authorities may not obtain, collect and share information about citizens other than those necessary in a democratic legal state. The provided form of control does not warrant in any manner the real compliance with these rules and, above all, does not block the possibility of acquiring data even if it was to take place in contravention of these rules.

One should also add that, in accordance with article 20ca para 5 of the Act on the Police (and, respectively, other services) no control shall be carried out in respect of obtaining data, acquired on the basis of article 20cb para 1 of the Act on the Police. It should be at this point indicated that the Police Act, and similarly other statutes, exclude from any control the acquisition of data not only referred to in Article 179 para 9 of the Telecommunications Law, but also the entire Article 161 of the Telecommunications Law, which significantly expands the scope of access to the data excluded from any control. In particular, Article 161 para 3 of the Telecommunications Law contains a reference to unspecified "other data".

VI. The non-conformity of Article 20c of the Act on the Police, Article 10b of the Act on the Border Guard, Article 36b of the Act on Fiscal Control, Article 30 of the Act on Military Police and Military Law Enforcement, Article 28 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, article 32 the Military Counterintelligence Service and the Military Intelligence Service, Article 18 of the Act on the Central Anticorruption Bureau, Article 75d of the Act on Customs Service– in so far as these provisions do not indicate the categories of people whose data can be obtained in the manner specified in the statutes, do not regulate the obligation to provide information to people whose data were obtained and do not specify the period during which the authorised bodies may process the acquired data– with Article 2, 30, 47, 49, 51 para 2, 3, 4 in conjunction with Article 31

para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the Charter of Fundamental Rights of the European Union.

Reservations of the Commissioner for Human Rights are raised by the legislative omissions, or issues that have not been (and should) be dealt with in the statute.

In particular, in its judgement in case K 23/11 the Constitutional Tribunal stressed that the implicit solicitation by public authorities of information about the individuals requires far-reaching procedural guarantees –essentially there has to exist the obligation to inform individuals about the undertaken operational and investigative measures and the collection information about it, regardless of whether they were persons suspected of violation of the law, or a third party, which accidentally became the object of surveillance. This is particularly important with regard to persons in respect of which a judgement was not issued or which have not been officially provided with criminal allegations, as well as third parties directly concerned by data acquisition. In the opinion of the Tribunal, the legislature should ensure subsequent informing about this fact, because the notification of an individual at the stage of carrying out operational and investigative activities may cause these activities to be ineffective. The need to establish such an information obligation was already raised by the Constitutional Tribunal in its judgement of 25 January 2006, ref. S 2/06. The provision of information is also a pre-requisite for the exercise, by individuals, of the right to access official documents and data sets resulting from the Article 51 para 3 of the Constitution. As noted by the Tribunal, the omission of informing about the acquisition of information about individuals by public authorities, in itself, constitutes a breach of Article 51 para 3 and 4 of the Constitution. If an individual does not know about the collection of certain information, it does not have the ability to gain access to them and cannot require their correction or removal under the conditions referred to in Article 51 para 4 of the Constitution.

The challenged statutes do not establish any procedure which would provide for informing individuals whose data was processed about the acquisition of retention, postal or Internet data. In the opinion of the Commissioner, the individual should have the right to take appropriate legal measures in respect of activities conducted in relation to him, also with regard to the information gathered by the competent services. It is also a requirement clearly defined by the Constitutional Tribunal (judgement of 25 January 2006, ref. S 2/06).

What's more, the proponent did not provide for any provisions detailing the categories of entities which can be be subjected to operational and investigative activities.

Finally, the statutes do not specify the length of time that qualified entities may process the acquired telecommunications, postal and Internet data. This stands in contradiction to the principle of time limitation expressed in Article 26 para 1 pt. 4 of the act on the protection of personal data, according to which the data may be kept in a form which permits identification of the data subject for no longer than is necessary to achieve the purpose of the processing. The statutes provide only that data that does not matter for criminal proceedings, are subject to an immediate witnessed and recorded destruction. The treatment of the data meaningful for a particular proceeding and are used in it has not been settled, including the issue of verification of the need for their further processing. As far as the time of retention of data included in the files of the proceedings will governed by special provisions, there is no regulation governing the period of retention of data processed in systems operated by the police and each service. In practice, this could lead to unjustified, untimely storing of the data. Period of processing telecommunications, postal and Internet data should therefore be specified precisely, so as to eliminate the risk of abuse, in view of the fact that there is no provision for external control of the necessity of further processing of data for the implementation of statutory tasks.

The above legislative omissions consist in the adoption of a regulation incomplete in the above-specified range. According to the Commissioner, these issues should be dealt with in Article 20c of the Act on the Police and in the corresponding provisions of the other statutes. Therefore, it should be considered that the incomplete regulation of the issue afflicting fundamental human rights and liberties should become the subject of control from the point of view of constitutional principles.

VII. The non-conformity of Article 28 para 7 of the Act on the Internal Security Agency and the Foreign Intelligence, Article 32 para 9 of the Act on the Military Counterintelligence Service and the Military Intelligence Service– in so far as they do not provide for the destruction of any other telecommunications, postal and Internet data than just those irrelevant for the ongoing criminal investigation — with Article 51

para 2 of the Constitution in conjunction with Article 31 para 3 of the Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 and 8 in conjunction with Article 52 para 1 of the EU Charter of Fundamental Rights

The provisions added by the Act on the amendment of the Police Act – Article 28 para 7 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, as well as Article 32 para 9 of the Act on the Military Counterintelligence Service and the Military Intelligence Service do not provide for the destruction of any other telecommunications, postal and on-line data than just those irrelevant for the ongoing criminal investigation. The Act allows for the preservation of data, referred to as "vital to the security of the state" (in the case of the Internal Security Agency), and "essential for the defence of the state" (in the case of the Military Counterintelligence Service).

The Constitutional Tribunal, in its judgement in case K 23/11 in item I subsection 8 expressly stated that Article 28 of the Act on the Internal Security Agency and the Foreign Intelligence Agency, as well as Article 32 of the Act on the Military Counterintelligence Service and the Military Intelligence Service in so far as they do not provide for the destruction of data which have no meaning for the ongoing proceedings, are incompatible with Article 51 para 2 in conjunction with Article 31 para 3 of the Constitution. Adopted the law has not removed this non-conformity. In this light, the Commissioner has no doubt that the omission demonstrated here is unconstitutional.

VIII. The non-conformity of Article 13 and Article 16 of the Act of 15 January 2016 on the Amendment to the Police Act and Some Other Acts (Journal of Laws of 2016, item 147)– in so far as they require to apply laws that are no longer in effect by virtue of the judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11 – with Article 2 and Article 190 para 1 and 3 of the Constitution of the Republic of Poland.

In the Act of 15 January 2016, amending the law on the Police and certain other acts transitional provisions have been set out, which, to some extent, maintain in force the current provisions. In accordance with Article 13 of the Act: "In respect of operational surveillance, which was carried out before the date of entry into force of the law and was not completed until that time, the existing provisions shall apply". A similar structure was provided for in Article 16 of the act: "In respect of operational surveillance carried out

on the basis of Article 27 para 1 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency in their current wording, in order to carry out the tasks referred to in Article 5 para 1 pt. 2 subsection b of this statute, not completed until the date of entry into force of this statute, the existing provisions shall apply". The structure of these provisions might indicate that the legislator – in terms indicated in them – wants to maintain in force the provisions of which have been found to be inconsistent with the Constitution and are no longer in force pursuant to the judgement of the Constitutional Tribunal of 30 July 2014, ref. K 23/11. It is indicated by the scope of the Act of 15 January 2016, amending the Act on the Police and certain other acts. The provisions of this act – as pointed out in the explanatory memorandum to the bill – serve to implement the judgement of the Constitutional Tribunal. Thus, it should be considered that by introducing a reference to the "existing provisions" the legislature has in mind the provisions recognized by the Tribunal as unconstitutional. This inference is backed up by the explanatory memorandum to the bill (Explanatory memorandum to the bill, Sejm print no. 154, pp. 15-16). In the assessment of the Commissioner for Human Rights, these provisions are incompatible with Article 2 and Article 190 para 2 and 3 of the Constitution.

It's difficult to find a legal rationale for maintaining in force provisions in respect of which the presumption of constitutionality was validly overturned by the Constitutional Tribunal. The legal structure adopted by the legislature undoubtedly violates the principle of decent legislation, the principle of trust in the state and the principle of legal certainty. It seems that the effects of the judgement of the Constitutional Tribunal on the incompatibility of a provision with the Constitution are twofold. First, this provision is formally removed from legal transactions, immediately after the announcement of the judgement or – in case of a postponement of annulment – at the date indicated in the decision of the Constitutional Tribunal. Secondly, through the non-compliance with the Constitution of a provision, the Tribunal at the same time, declares the non-compliance of the legal norm with the Constitution. Not only is the provision unconstitutional, but also the norms derived from it. The effect of the judgement understood in such a way leads to the limitation of the competence of the legislature in the field of legislation in the area covered by the judgement of the Constitutional Tribunal. It is clear that the legislature could not enact a provision with the same content, which was considered to be incompatible with the Constitution. The legislature, however, not only cannot adopt a provision with the same content, but also the provision with different content that can be

used to derive only the standard recognised previously as unconstitutional. In other words, the result is not only a derogation of the provision, but also of legal norms. In the light of the principle of decent legislation one should therefore be aware that the adoption of norms – even when one changes the wording of the provisions previously deemed unconstitutional – violates the principle of the democratic rule of law. In the context of Article 13 and 16 of the Act 15 January 2016 amending the Act on the Police and Some Other Acts, the infringement of the principle of decent legislation is more obvious. Without as much as an attempt to change the wording of the provisions deemed inconsistent with the Constitution, they are kept in power, prejudicing in this way the judgement of the Constitutional Tribunal. In the light of this principle, a provision considered to be incompatible with the Constitution not only formally, but even substantively – cannot operate in legal transactions.

This conclusion finds additional justification in principle of legal certainty. The case law and literature indicate that legal certainty has to be a guarantee of the stability of the legal order, and also give citizens the confidence that allows them to shape their life matters. (W. Sokolewicz, Komentarz do art. 2, [in:] L. Garlicki (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, vol. V Warsaw 2007, p. 36; cf. also judgement of the Constitutional Tribunal of 15 June 2000, ref. P 3/00). Undoubtedly, correct is the belief of a citizen about the possibility of voiding these provisions, which the Constitutional Tribunal has found to be inconsistent with the Constitution of the Republic of Poland and at the same time has the term postponing their annulment has expired. The legislature's decision to maintain such provisions in force causes an imbalance of legal certainty. It also strikes at the principle of citizens' confidence in the state, especially in the context of Article 190 para 1 and 3 of the Constitution of the Republic of Poland.

In accordance with Article 190 para 1 of the Constitution: "Judgments of the Constitutional Tribunal shall be of universally binding application and shall be final." As stated by Article 190 para 3 of the Constitution: "A judgment of the Constitutional Tribunal shall take effect from the day of its publication, however, the Constitutional Tribunal may specify another date for the end of the binding force of a normative act. Such time period may not exceed 18 months in relation to a statute or 12 months in relation to any other normative act. (...)". These provisions leave no doubt. The endeavour of the legislature to maintain in force the provisions of the statutes in force before the entry into force of the Act of 15 January 2016, Amending the Act on the Police and Some Other Acts, deemed by the Constitutional Tribunal to be inconsistent with the

Constitution of the Republic of Poland, infringes the principle of finality and universal effect of the judgements of the Constitutional Tribunal.

The inference carried out here is confirmed in the judgement of the Supreme Administrative Court of 31 January 2014, in which it was noted that: "From Article 190 para 3 of the Constitution, one can infer that since the Constitution only exceptionally allows for the existence of a legal act incompatible with it, then the rule is its non-validity, i.e. non-execution" (judgement of the Supreme Administrative Court of 31 January 2014, ref. (II) FSK 2752/13).

The institution of the postponing the binding force of a provision is used by the Constitutional Tribunal in order to give the relevant authorities of the state time for the execution of the judgement, and therefore for the introduction of relevant legal changes. This is a unique situation, because a provision exists within the legal system, the non-compliance of which with the Constitution has been legally confirmed. The legislature, without waiting for the expiry of the period of deferment, should immediately adjust the legal situation to the requirements of the Constitution. By constructing transitional provisions in such situations, one should be aware of the ratio legis of the institution of the deferred loss of binding force. The Commissioner for Human Rights sees no reason to refrain from applying the new provisions also to operational surveillance, which was carried out before the date of entry into force of the contested act and was not completed until that time.

In this state of affairs, the provisions contested in this part of the application are incompatible with Article 2 and Article 190 para 1 and 3 of the Constitution of the Republic of Poland.

In view of the above and, in particular, the importance proven doubts as to the conformity of the challenged provisions with the Constitution of the Republic of Poland, I have no doubt that the contested provisions constitute a serious threat to the most important freedoms and human rights.

Wherefore, I petition as written in the petitum.