

**A C T**

of 10 June 2016

**on anti-terrorist activities and on the amendments to other acts<sup>1)</sup>**

Chapter 1

**General provisions**

**Article 1.** The Act specifies the rules of performing anti-terrorist activities as well as the cooperation among the organs entitled to conduct such activities.

**Article 2.** Whenever the Act mentions:

- 1) antiterrorist Activities - the term should be understood as activities of the organs of public administration which are aimed at preventing events of a terrorist nature, preparations to take control over such events by means of planned undertakings, reaction in case such events occur and removal of their effects, including the recovery of the resources aimed at reacting to such events;
- 2) counter-terrorist activities - the term should be understood as activities against perpetrators, as well as persons preparing or assisting in committing an offence of a terrorist nature, performed with the aim to eliminate the immediate threat to life, health or property, with the use of specialist forces or means, as well as specialist operational tactics;

---

<sup>1)</sup> The present act amends the following acts: Act of 6 April 1990 on Police, Act of 12 October 1990 on the protection of state border, Act of 12 October 1990 on Border Guard, Act of 24 August 1991 on fire protection, Act of 3 February 1995 on the protection of farm and forest li, Act of 6 June 1997 – Criminal Code, Act of 22 August 1997 on the protection of people and property, Act of 29 August 1997 – Banking Act, Act of 26 October 2000 on commodity exchanges, Act of 16 March 2001 on Government Protection Bureau, Act of 24 August 2001 on Military Gendarmerie and military law and order forces, Act of 24 May 2002 on the Agency in Internal Security and Intelligence Agency, Act of 3 July 2002 – Aviation Law, Act of 27 March 2003 on spatial planning and management, Act of 11 September 2003 on professional military services, Act of 27 May 2004 on investment funds, Act of 16 July 2004 – Telecommunication law, Act of 29 July 2005 on trading in financial instruments, Act of 9 June 2006 on Central Anti-Corruption Bureau, Act of 9 June 2006 on Army Counter-Intelligence Service and Army Intelligence Service, Act of 9 June 2006 on the service of the officers of o Army Counter-Intelligence Service and Army Intelligence Service, Act of 14 July 2006 on entry into, stay and exit from the territory of the Republic of Poland of citizens of member states of the European Union and members of their families, Act of 8 September 2006 on State Medical Rescue Services, Act of 26 April 2007 on crisis management, Act of 27 August 2009 on Customs Service, Act of 5 November 2009 on cooperative savings and loan banks, Act of 9 April 2010 on Penitentiary Service, Act of 15 April 2011 on medical treatment activities, Act of 24 May 2013 on means of direct force and firearms, Act of 12 December 2013 on foreigners and Act of 18 March 2016 on the special solutions related to the organization of the visit of His Holiness Pope Francis to the Republic of Poland and the World Youth Days – Kraków 2016.

- 3) infrastructure of public administration - the term should be understood as systems and facilities which are necessary for ensuring the safe and continuous functioning of the organs of public administration;
- 4) critical infrastructure - the term should be understood as critical infrastructure, referred to in Article 3 Paragraph 2 of the Act of 26 April 20017 on crisis management (Journal of Laws of 2013, item 1166, and of 2015 item 1485, and of 2016, item 266);
- 5) Minister Coordinator of Special Services - the term should be understood as Minister - Member of the Council of Ministers whose remit, provided for in Article 33 Paragraph 1 of the Act of 8 August 1996 on the Council of Ministers (Journal of Laws of 2012 item 392, and of 2015 item 1064) includes tasks related to the functioning of special services as formulated in the Act of 24 May 2002 on the Agency of Internal Security and the Intelligence Agency (Journal of Laws of 2015 item 1929 and 2023, and of 2016 items 147 and 437);
- 6) scene of the event of a terrorist nature - the term should be understood as an open or closed space where an event of a terrorist nature has taken place, or where its effects have taken or were to take place, as well as a space where threats related to the event of a terrorist nature are present;
- 7) event of a terrorist nature - the term should be understood as a situation suspected to have developed as a result of an offence of a terrorist nature as it has been specified in Article 115 § 20 of the Act of 6 June 1997 – Criminal Code (Journal of Laws item 553, with later amendments <sup>2)</sup>), or a threat of such an offence.

## Chapter 2

### **Anti-terrorist activities preventing events of a terrorist nature**

**Article 3.** 1. The Head of Internal Security Agency (ABW), henceforth referred to as "Head of ABW", is responsible for the prevention of events of a terrorist nature.

---

<sup>2)</sup> Amendments to the mentioned Act have been announced in the Journal of Laws of 1997 item 840, of 1999 item 729 and 931, of 2000 item 548, 1027 and 1216, of 2001 item 1071, of 2003 item 1061, 1142, 1750, 1935 and 2255, of 2004 item 219, 626, 889 and 2426, of 2005 item 732, 757, 1109, 1363, 1479 and 1493, of 2006 item 1409, 1592 and 1648, of 2007 item 589, 850, 859 and 1378, of 2008 item 560, 782, 1056, 1080 and 1344, of 2009 item 504, 533, 1317, 1323, 1474, 1540 and 1589, of 2010 item 46, 227, 229, 625, 626, 842, 857, 1018, 1021, 1228, 1474 and 1602, of 2011 item 78, 130, 202, 245, 381, 549, 678, 767, 964, 1135, 1280, 1381 and 1431, of 2012 item 611, of 2013 item 849, 905, 1036 and 1247, of 2014 item 538, of 2015 item 396, 541, 1549, 1707 and 1855 and of 2016 item 189, 428 and 437.

2. The minister competent for internal affairs is responsible for the preparations aimed at taking control over events of a terrorist nature by means of planned undertakings, as well as reacting in case of the occurrence of such events, and for the recovery of resources aimed to be used in the reactions to such events.

**Article 4.** 1. Organs of public administration, owners and holders of facilities, installations, and equipment of public administration infrastructure, as well as critical infrastructure, cooperate with the organs, services and institutions competent in issues of security and crisis management when performing anti-terrorist activities.

2. The entities referred to in Paragraph 1 are to, without delay, convey to the Head of ABW the information they possess about the terrorist threats to the infrastructure of public administration or the critical infrastructure, including threats to the functioning of the system and the energy, water and sewage, heating, telecommunication and IT grids, which are important from the point of view of the security of the state.

3. In case information is acquired about the possibility of the occurrence of an event of a terrorist nature posing a threat to the public administration infrastructure or critical infrastructure, the life and health of people, property of a substantial scale, national heritage or the environment, the Head of ABW can issue orders to the organs and entities referred to in Paragraph 1 hereof and which are under threat of such events. The orders issued are aimed at counteracting, removing or minimizing the threats, as well as conveying information necessary for this aim. The organs and entities referred to in the first sentence hereof, shall inform the Head of ABW about the actions undertaken in this respect.

4. The Head of ABW shall, without delay, inform the Minister Coordinator of Special Services, should such a person be appointed, about the undertaken actions referred to in Paragraph 3 hereof.

**Article 5.** 1. In order to perform the tasks referred to in Article 3 Paragraph 1 hereof, the Head of ABW coordinates the analytical and information Activities undertaken by the special services referred to in Article 11 of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency, as well as the exchange of information transferred by the Police, Border Guard, Government Protection Bureau, State Fire Department, Customs Service, General Inspector of Financial Information, General Inspector of Revenue Control, Military Gendarmerie and the Government Security Centre, regarding threats of a terrorist nature, as

well as data about the persons referred to in Art 6 Paragraph 1, by collecting, processing and analyzing these data.

2. The minister competent for internal affairs shall specify, in agreement with the minister competent for public finances and the Minister of National Defense, and upon consulting the Head of the ABW, a catalogue, in the form of an ordinance, of events of a terrorist nature, taking into consideration the need to classify the information referred to in Paragraph 1 hereof.

3. The entities referred to in Paragraph 1 hereof, shall upon receiving, and without delay, convey to the Head of ABW the information on the execution of the anti-terrorist activities, classified according to the catalogue of events of a terrorist nature.

**Article 6.** 1. In order to perform the tasks referred to in Article 3 Paragraph 1, the Head of ABW shall, fully observing the requirements of protecting classified information, maintain a register including information about:

- 1) persons involved in activities on behalf of terrorist organisations or organisations connected with terrorist activities or members of such organisations;
- 2) wanted persons involved in terrorist activities or persons suspected of committing offences of a terrorist nature, with regard to whom an arrest or a search warrant has been issued or a wanted letter has been decided on, as well as persons who are wanted and subject to the European Arrest Warrant.;
- 3) persons with regard to whom there is a justified suspicion that they may be involved in activities aimed at committing an offence of a terrorist nature, including persons who might present a threat to civil aviation;
- 4) persons participating in terrorist training or undertaking a journey with the aim to commit an offence of a terrorist nature.

2. The Head of ABW shall, as the need may be, convey the information referred to in Article 5 Paragraph 3, as well as information included in the list referred to in Paragraph 1 hereof, also in the form of current analyses about the possibility of the occurrence of an event of a terrorist nature to:

- 1) entities referred in Article 5 Paragraph 1,
- 2) other entities of public administration – within the remit of their competence.

3. The Head of ABW shall, without delay, convey to the President of the Republic of Poland, the Prime Minister, the minister competent for internal affairs, the Minister of National Defence, the minister competent for foreign affairs, the Minister Coordinator of

Special Services, should such as person be appointed, information which could have significant importance on the prevention of events of terrorist nature. The provision of Article 18 Paragraph 1 of the Act of 24 May 2002 on the Agency of Internal Affairs and the Intelligence Agency is applied accordingly.

4. The Head of ABW shall specify, by means of an ordinance and with consideration of all the requirements pertaining to the protection of classified information:

- 1) the scope of information collected in the register referred to in Paragraph 1 hereof;
- 2) the means of maintaining the register referred to in Paragraph 1 hereof;
- 3) the mode of obtaining information from the register referred to in Paragraph 1 hereof by entities referred to in Art 5 Paragraph 1.

**Article 7.** 1. In order to perform the tasks referred in Art 3 Paragraph 1, the Head of ABW coordinates:

- 1) the surveillance and intelligence activities undertaken by the special services referred to in Art 11 of the Act of 24 May 2002 on the Agency of Internal Security and the Intelligence Agency, as well as by the Police, Border Guard, General Inspector of Treasury Control, the Military Gendarmerie, and
- 2) the activities performed by customs officers of observing and recording, with the use of technical means, the image of events in public spaces and the audio accompanying these events.

2. The Head of ABW can issue recommendations to the entities referred to in Paragraph 1, with the aim to remove or minimise the terrorist threat which has occurred.

**Article 8.** 1. In order to recognise, prevent and combat offences of a terrorist nature, the Head of ABW may order the following covert activities to be undertaken, for a period no longer than three months, with regard to a person who is not a citizen of the Republic of Poland, and with regard to whom there is a fear of possible involvement in terrorist activities:

- 1) obtaining and recording the content of conversations by technical means, including with the use of telecommunication networks;
- 2) obtaining and recording the content of the image and sound of persons from premises, means of public transportation and other venues other than public spaces;

- 3) obtaining and recording the content of correspondence, including correspondence kept by means of electronic communication
- 4) obtaining and recording the data contained in IT data carriers, telecommunication end devices, as well as information and tele-information systems;
- 5) obtaining access and controlling the content of consignments.

2. A telecommunication business, operator of post services, or an electronic services provider are obliged to ensure free technical and organizational conditions allowing the Agency of Internal Security (Agencja Bezpieczeństwa Wewnętrznego), henceforth referred to as “ABW”, to perform the activities referred in Paragraph 1 hereinabove.

3. A provider of electronic services who is a micro-enterprise or a small enterprise in light of the provision of the Act of 2 July 2004 on the freedom of business activities (Journal of Laws of 2015 item 584, with later amendments<sup>3)</sup>) shall ensure the technical and organizational conditions necessary for the ABW to perform the activities referred to in Paragraph 1 hereinabove, accordingly to the infrastructure in place.

4. The Head of ABW shall, without delay, inform the Minister Coordinator of Special Services, should such a person be appointed, as well as the Prosecutor General about the order referred in Paragraph 1 hereinabove. The Prosecutor General may order to stop the activities referred to in Paragraph 1.

5. The activities referred to in Paragraph 1 hereinabove may be prolonged following the terms provided for in Article 27 of the Act of 24 May 2002 on the Agency of Internal Security and the Intelligence Agency.

6. The Head of ABW shall, without delay, inform the Prosecutor General about the results of the activities referred to in Paragraph 1 upon their completion and, upon the request of the Prosecutor General, also about the course of these activities, presenting the materials then gathered.

7. The Head of ABW shall present the Prosecutor General with all the materials gathered in the course of performing the activities referred to in Paragraph 1. The Prosecutor General shall make a decision on the scope and means of using the materials presented.

---

<sup>3)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and of 2016 item 65, 352 and 615.

Provision of Article 238 § 3–5 and Article 239 of the Act of 6 June 1997 – Code of Criminal Procedure (Journal of Laws item 555, with later amendments<sup>4)</sup>) is applied accordingly.

8. The Prosecutor General orders the destruction of materials obtained in the course of the activities referred to in Paragraph 1, which do not contain evidence of the offence, or which are not important from the perspective of the security of the state.

9. The Head of ABW shall, without delay, perform a witnessed and recorded destruction of the materials referred to in Paragraph 8 hereinabove. The Head of ABW shall inform the Prosecutor General of the event.

10. The Prime Minister shall, by means of an ordinance, specify the means of documenting the activities referred to in Paragraph 1 hereinabove, as well as the means of retaining and transmitting instructions and information, as well as of retaining, transmitting, processing and destroying the materials obtained in the course of performing these activities, together with sample copies of forms and registers, taking into consideration the need to ensure the classified nature of the activities performed and the materials gathered.

**Article 9.** 1. Officers of ABW, Police and the Border Guard are entitled to take fingerprints or record the face image of a person who is not a citizen of the Republic of Poland in case when:

- 1) there is a doubt as to the identity of this person or
- 2) there is a suspicion that the border of the Republic of Poland has been crossed illegally, or there is a doubt as to the declared purpose of the person's stay in the territory of the Republic of Poland, or
- 3) there is a suspicion of an intended illegal stay in the territory of the Republic of Poland, or
- 4) there is a suspicion of the person's connection with and event of a terrorist nature, or
- 5) the person may have participated in terrorist training.

---

<sup>4)</sup> Amendments to the mentioned Act have been announced in the Journal of Laws of 1999 item 931, of 2000 item 580, 717, 852 and 1027, of 2001 item 1071 and 1149, of 2002 item 676, of 2003 item 155, 1061 and 1188, of 2004 item 514, 626, 889, 2405 and 2641, of 2005 item 70, 461, 680, 821, 1181, 1203, 1363, 1416 and 1479, of 2006 item 118, 467, 659, 708, 711, 1009, 1013, 1192, 1647 and 1648, of 2007 item 116, 432, 539, 589, 664, 766, 849 and 903, of 2008 item 162, 648, 686, 802, 1133, 1308, 1344, 1485, 1571 and 1651, of 2009 item 39, 104, 171, 585, 716, 1051, 1178, 1323, 1375, 1474 and 1589, of 2010 item 46, 626, 669, 826, 842, 1228 and 1307, of 2011 item 245, 246, 273, 654, 678, 829, 1135, 1280, 1430, 1431, 1438 and 1645, of 2012 item 886, 1091, 1101, 1327, 1426, 1447 and 1529, of 2013 item 480, 765, 849, 1247, 1262, 1282 and 1650, of 2014 item 85, 384, 694, 1375 and 1556, of 2015 item 21, 290, 396, 1185, 1186, 1334, 1788, 1855 and 2281 and of 2016 item 178 and 437.

2. The organ which has taken the fingerprints or recorded the person's facial image, shall transmit to the Commander in Chief of the Police the following:

- 1) image of the fingerprints or the facial image;
- 2) personal data of the person whose fingerprints or facial image have been taken;
- 3) information about the legal basis for taking the fingerprints or a record of the facial image.

3. The Commander in Chief of the Police:

- 1) enters the transmitted pictures, images and information referred to in Paragraph 2 hereinabove in the Police data bases;
- 2) makes the transmitted pictures, images and information available to the organs referred to in Paragraph 1, and allows them to be processed and updated for the purpose of the proceedings conducted by the said organs.

4. The Prime Minister shall specify, by means of an ordinance, the manner and mode of:

- 1) collecting the images of the fingerprints and recordings of the facial image of the person who is not a citizen of the Republic of Poland,
- 2) transmitting to the Commander in Chief of the Police the collected images of the fingerprints, the recorded facial image, and the information specified in Paragraph 2.

– bearing in mind the need to ensure efficient collection of fingerprint and facial images, as well as faithful imaging of the fingerprints and the facial images, and their transmission, without delay, to the appropriate organ of the Police.

**Article 10.** In order to perform the task referred to in Article 3 Paragraph 1, the Head of ABW may have free access to:

- 1) the data and information gathered in public registers and records kept, in particular, by:
  - a) the entities referred to in Article 5 Paragraph 1,
  - b) ministers managing the sectors of governmental administration,
  - c) Head of the Office for Foreigners,
  - d) President of the Office of Electronic Communication,
  - e) President of the Office for Civil Aviation,
  - f) President of the National Atomic Energy Agency,
  - g) Social Insurance Office,
  - h) President of the Agricultural Social Insurance Fund,
  - i) Financial Supervision Authority,



j) Land Surveyor General,

k) local authorities

– as well as organisational units subordinate to the above, or overseen by the above,

2) the image of events recorded by image recording equipment located in public venues, by public roads and other public places, and receive free copies of the recorded image

– with all due consideration for the terms and mode specified in Article 34 of the Act of 24 May 2002 on the Agency in Internal Security and the Intelligence Agency.

**Article 11.** 1. In case of the introduction of the second or higher state of alert pursuant to Article 15 Paragraph 1, the area under the state of alert is subject to a control of the safety measures of the facilities there located. Such control of the safety measures is performed by:

1) the Police – in facilities of critical infrastructure;

2) Military Gendarmerie – in facilities belonging to the cells and organizational units subordinate to the Minister of National Defense or supervised by the Minister of National Defense, or administered by these cells and organisational units.

2. The Head of ABW may, in agreement with the minister competent for internal affairs, issue a recommendation to the Police to undertake special security measures with regard to selected facilities which would be relevant to the type of threat of the occurrence of an event of a terrorist nature.

**Article 12.** 1. As part of the obligation to provide telecommunication services as stipulated in Article 179 Paragraph 2 of the Act of 16 July 2004 – The Telecommunication Law (Journal of Laws of 2014, item 243 with later amendments<sup>5)</sup>), the provider of the telecommunication services is obliged to ensure telecommunication, and in particular with emergency numbers, in connection with events, and in particular mass events or gatherings at which events of a terrorist nature or threats to the safety and public order may occur. The telecommunication services provider is thus, at the request of the minister competent for IT issues or the organ responsible for public law and order, obliged to install, for a period no longer than 30 days, and also in construction objects which are not permanently fixed to the ground, temporary radio communication installations with antenna support constructions, and in particular a base station of mobile telecommunication network.

2. The mounting of temporary installations referred to in Paragraph 1 hereinabove does not require a building permit specified in Article 28 Paragraph 1 of the Act of 7 July 1994 –

---

<sup>5)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 827 and 1198, of 2015 item 1069, 1893 and 2281 and of 2016 item 147 and 542.

The Building Law (Journal of Laws of 2016, item 290), or a notification referred to in Article 30 Paragraph 1 of the same law.

3. The use of the installations specified in Paragraph 1 is only possible after having notified the organ competent for environmental protection specified in Article 152 Paragraph 1 of the Act of 27 April 2002 – The Law on Environmental Protection (Journal of Laws of 2013 item 1232 with later amendments <sup>6)</sup>), together with the results of the measurements referred to in Article 122a Paragraph 1 of the law, confirming the maintenance of the level of electromagnetic fields below admissible levels.

4. The property where the telecommunication services provider is installing the temporary installation can, for the benefit of the provider, be encumbered with servitude, so that the provider can perform the installation and use, according to its purpose, the equipment specified in Paragraph 1 on the encumbered property during the period specified in Paragraph 1.

5. If the owner of the property refuses to conclude an agreement on servitude referred to in Paragraph 4, the provider of telecommunication services files an application to the appropriate Poviata Governor (Starosta) requesting the establishment of servitude as referred to in Paragraph 4.

6. The Poviata Governor (Starosta) is, by means of an administrative decision, obliged to establish servitude for the period referred to in Paragraph 1. The Starosta shall issue the decision not later than within 7 days from the day of the submission of the application.

7. The decision referred in Paragraph 6 is subject to immediate execution.

8. The servitude expires upon the expiry of the period referred to in Paragraph 1 at the latest.

9. Upon the expiry of the servitude, the telecommunication services provider has the duty to remove the installation.

10. For the servitude as well as the damages resulting from the take-over of the property, a compensation is due in the amount agreed on with the owner, perpetual usufructuary or person with the entitlement to other rights in rem to the property and the telecommunication services provider to whom the property had been made available. In case no agreement is reached within the period of 30 days beginning with the date of expiry of making the property

---

<sup>6)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2013 item 1238, of 2014 item 40, 47, 457, 822, 1101, 1146, 1322 and 1662, of 2015 item 122, 151, 277, 478, 774, 881, 933, 1045, 1223, 1434, 1593, 1688, 1936 and 2278 and of 2016 item 266.

available, the Starosta performing the task on behalf of the governmental administration shall initiate proceedings aimed at establishing the compensation.

11. The higher instance organ in case of the decision referred to in Paragraph 6 is the Voivode (Governor of the Voivodship).

**Article 13.** 1. The entities referred to in Article 5 Paragraph 1 may, in agreement with the Head of ABW, second their employees or officers of their subordinate units or organs, or from the units and organs which they supervise, as well as soldiers selected to dedicated positions in the Army Counter-Intelligence Service or the Army Intelligence Service, to work for or to serve ABW so as to perform the task referred to in Article 3 Paragraph 1, on terms specified in the agreement concluded by the manager of the seconding institution and the Head of ABW.

2. In the case of the secondment of employees to work at ABW, Article 42 § 2 of the Act of 26 June 1974 – Labour Code (Journal of Laws of 2014 item 1502, with later amendments<sup>7)</sup>) is not applicable.

3. The Prime Minister shall specify, by means of an ordinance:

- 1) the terms and mode of seconding the employee, officer or soldier, as well as the place, nature and scope of official duties to be performed by the seconded employee, officer or soldier,
- 2) the method of payment of the salary or wages and other pecuniary benefits to which the seconded employee, officer or soldier is entitled, including the division into the salary or wages and the amounts paid by ABW and the organizational unit from which the employee, officer or soldier has been seconded

– bearing in mind the effective organisation of the execution of official duties by the seconded employees, officers and soldiers.

### Chapter 3

#### **Alert levels**

**Article 14.** 1. In case of a threat of the occurrence of an event of a terrorist nature or in case of the occurrence of such an event, one of the four alert levels may be introduced:

- 1) first alert level (level ALFA);

---

<sup>7)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1662 and of 2015 item 1066, 1220, 1224, 1240 and 1268.

- 2) second alert level (level BRAVO);
- 3) third alert level (level CHARLIE);
- 4) fourth alert level (level DELTA).

2. In case of a threat of the occurrence of an event of a terrorist nature regarding the IT and communications system of the organs of public administration, or the IT and communications systems being part of the critical infrastructure, or in the case of the occurrence of such an event, one of the four levels of CRP alert can be introduced:

- 1) first CRP alert level (level ALFA–CRP);
- 2) second CRP alert level (level BRAVO–CRP);
- 3) third CRP alert level (level CHARLIE–CRP);
- 4) fourth CRP alert level (level DELTA–CRP).

3. The first level referred to in Paragraph 1 point 1 and Paragraph 2 point 1 may be introduced in case information is obtained about the possible occurrence of an event of a terrorist nature, whose type and scope is difficult to foresee.

4. The second level referred to in Paragraph 1 point 2 and Paragraph 2 point 2 may be introduced in case of the occurrence of an increased and predictable threat of an event of a terrorist nature, whose specific aim, however, has not been identified.

5. The third level referred in Paragraph 1 point 3 and Paragraph 2 point 3 may be introduced in case of:

- 1) the occurrence of an event confirming the probable target of the event of a terrorist nature, aiming at:
  - a) public safety or order, or
  - b) security of the Republic of Poland, or
  - c) security of another state or an international organisation, and posing a potential threat to the Republic of Poland, or
- 2) obtaining credible and confirmed information about a planned event of a terrorist nature in the territory of the Republic of Poland, or
- 3) obtaining credible and confirmed information about a planned event of a terrorist nature, whose effects may touch on Polish citizens staying abroad or Polish institutions or Polish infrastructure located beyond the borders of the Republic of Poland.

6. The fourth level referred to in Paragraph 1 point 4 and Paragraph 2 point 4 may be introduced in case of:

- 1) the occurrence of an event of a terrorist nature causing threat to:
  - a) public safety or order, or
  - b) security of the Republic of Poland, or
  - c) security of another state or an international organisation, and posing a potential threat to the Republic of Poland, or
- 2) when the obtained information indicates an advance phase of preparations to an event of a terrorist nature in the territory of the Republic of Poland, or
- 3) when the obtained information indicates an advance phase of preparations to an event of a terrorist nature which may be aimed at Polish citizens staying abroad or at Polish institutions, or Polish infrastructure located beyond the borders of the Republic of Poland, and the collected information at the same time indicates the inevitability of such event.

7. A higher or lower CRP level of alert may be introduced with the omission of the intermediate levels.

8. The levels referred to in Paragraphs 1 and 2 may be introduced separately or together.

9. In case when different levels of alert and different levels of CRP alert are introduced, the tasks assigned to the higher level should be executed.

10. The levels of alert and the levels of CRP alert are introduced for a time necessary to minimise the threats and effects of the events due to which they were introduced.

**Article 15.** 1. The alert levels or the CRP alert levels are introduced, changed and revoked by the Prime Minister, in the form of an ordinance, depending on the threat of the event of a terrorist nature, and upon obtaining an opinion from the minister competent for internal affairs and the Head of ABW; in cases which cannot be delayed – by the minister competent for internal affairs upon obtaining an opinion from the Head of ABW and immediately informing the Prime Minister of the fact. The above applies to:

- 1) the entire territory of the Republic of Poland;
- 2) an area of one or a few units of the territorial division of the country;
- 3) an area defined in a manner other than that of territorial division of the country;
- 4) specific facilities of the organizational units of public administration, prosecution, courts, or other facilities of public administration infrastructure or critical infrastructure;

5) cases when the effects of the event of a terrorist nature can touch on Polish citizens staying abroad the Republic of Poland, or Polish intuitions or Polish infrastructure located beyond the borders of the Republic of Poland, other than the foreign posts of the Republic of Poland in the understanding of the Act of 27 July 2001 on foreign service (Journal of Laws item 1403 with later amendments<sup>8)</sup>).

2. The alert levels are introduced, changed and revoked by the Prime Minister, in the form of an ordinance, depending on the threat of the event of a terrorist nature, and upon obtaining an opinion from the minister competent for foreign affairs and the Head of the Intelligence Agency; in cases which cannot be delayed – by the minister competent for foreign affairs upon obtaining an opinion from the Head of the Intelligence Agency and immediately informing the Prime Minister of the fact. The above applies to:

- 1) specific foreign posts of the Republic of Poland in the understanding of the Act of 27 July 2001 on foreign service;
- 2) IT and communications systems of the minister competent for foreign affairs.

3. The Prime Minister shall, without delay, inform the President of the Republic of Poland and the Speaker of the Sejm of the Republic of Poland as well as the Speaker of the Senate of the Republic of Poland about the introduction, change, or revocation of the alert level or the CRP alert level.

4. The introduction of an alert level or a CRP alert level serves as a basis for the organs of public administration and the heads of services and institutions competent in issues of security and crisis management to execute:

- 1) undertakings specified in the provisions issued pursuant to Paragraph 5 and 6 and resulting from their statutory competences;
- 2) undertakings and procedures of crisis management, had they been envisaged for each of the alert level or CPR alert level in connection with the occurrence of an event of a terrorist nature and have not been specified in the provisions issued pursuant to Paragraphs 5 or 6.

5. The Prime Minister shall specify, in the form of an ordinance, the detailed scope of undertakings performed by the organs of public administration and the heads of services and institutions competent in issues of security and crisis management, as part of the statutory competencies, for the different levels of alert introduced pursuant to Paragraph 1, as well as

---

<sup>8)</sup> Amendments to the mentioned Act have been announced in the Journal of Laws of 2004 item 2703, of 2006 item 1217, 1218 and 1600, of 2008 item 1505, of 2009 item 1277, of 2015 item 1220 and 1274 and of 2016 item 34.

the CRP alert levels, taking into account the need to ensure good flow of information and to minimize the effects of the events of a terrorist nature.

6. The minister competent for foreign affairs shall specify, in the form of an ordinance, the detailed scope of undertakings to be performed by the heads of the foreign posts of the Republic of Poland pursuant to the Act of 27 July 2001 on foreign service, with respect to the different levels of alert introduced pursuant to Paragraph 2, taking into account the need to ensure good flow of information and to minimize the effects of the events of a terrorist nature.

**Article 16.** 1. In case of the introduction of a level of alert or a CRP level of alert pursuant to Article 15 Paragraph 1, the Head of ABW shall convene a coordinating team composed of the representatives delegated by the entities specified in Article 5 Paragraph 1 and Article 6 Paragraph 2 point 2.

2. The Head of ABW may, depending on the type of event of terrorist nature, nominate to participate in the coordination team representatives of other organs referred to in Article 6 Paragraph 2 point 2, as well as a representative of the Prosecutor General, all delegated by these organs.

3. The coordination team is responsible for recommending changes or a revocation of the alert level, as well as forms and scope of the cooperation of services and organs being part of the coordination team and participating in the works of this body.

## Chapter 4

### **Anti-terrorist activities on the scene of the events of a terrorist nature, including counter-terrorist activities.**

**Article 17.** The responsibility for the command over the anti-terrorist activities undertaken by the competent services or organs as part of their statutory duties on the scene of the event of a terrorist nature lies with the “commander of Activities”, as s/he shall be henceforth referred to, who has been:

- 1) appointed by the Commander in Chief of the Police and, in cases allowing for no delay – a Police officer appointed by the competent local voivodship chief of Police, particularly in case when other services or organs are present at the scene of the event of a terrorist nature;

- 2) appointed by the Minister of National Defense, and in cases allowing for no delay – a soldier of the Military Gendarmerie appointed by the Commander in Chief of the Military Gendarmerie in case of an event of a terrorist nature in areas or facilities belonging to the cells and organisational units subordinate to the Minister of National Defense or supervised by the Minister of National Defense, or administered by these cells and organisational units.

**Article 18.** 1. The minister competent for foreign affairs, in cooperation with the Minister Coordinator of the Special Services, should such a person be appointed, coordinates the activities of the competent services and organs in case of an event of a terrorist nature outside of the Republic of Poland but aimed against the citizens or assets of the Republic of Poland, with the exclusion of events referred to in Paragraph 2.

2. The Minister of National Defense coordinates, in cooperation with the minister competent for foreign affairs, the activities of the competent services and organs in case of an event of a terrorist nature outside of the Republic of Poland but aimed at the soldiers and assets of the Armed Forces of the Republic of Poland.

3. When performing the task referred to in Paragraph 1 or 2, the minister competent for foreign affairs or the Minister of National Defense can, in particular, request information, reports and options of the proposed solutions from the competent services and organs, as well as to be consulted on the actions to be taken.

**Article 19.** 1. If it is justified by the situation on the scene of the event of a terrorist nature, the commander of activities may, within the scope and time necessary to effectively perform the anti-terrorist activities:

- 1) order the evacuation of places or property from the scene of the event of a terrorist nature and its surroundings to a designated site, facility, or area;
- 2) introduce a ban for third persons to be present at the scene of the event of a terrorist nature and its vicinity;
- 3) order to halt all road or railway traffic, as well as public mass transportation means at the scene of the event of a terrorist nature and its vicinity;
- 4) demand free use of real estate or free take-over for use of any moveable assets, including means of transportation, as well as items and devices necessary to perform counter-terrorist activities;



5) demand assistance from institutions, organizations, entrepreneurs and natural persons or have the capacity to give them instructions.

2. Institutions, organizations, entrepreneurs and natural persons have the duty to execute the instructions and requests addressed to them by the commander of activities as stipulated in Paragraph 1.

3. The State Treasury holds civil liability for the damages caused due to the application of the entitlements specified in Paragraph 1 point 4 and 5 pursuant to the terms specified in the Act of 23 February 1964 – Civil Code (Journal of Laws of 2016, items 380 and 585).

**Article 20.** 1. Upon the introduction of the third or fourth level of alert, the minister competent for internal affairs may, on his/her own initiative or the initiative of the Head of ABW or the Commander in Chief of the Police, introduce a ban on public gatherings or mass events in the area or the facility subject to the level of alert, if such a measure is necessary for the protection of the lives and health of people or public safety.

2. The proper organs of public administration shall immediately, upon the announcement of the ban referred in Paragraph 1:

- 1) issue a decision on the ban of gatherings or a decision on the dissolution of gatherings, pursuant to the Act of 24 July 2015 – Law on Gatherings (Journal of Laws of 2015 item 1485),
- 2) refuse to issue a permit to organize a mass event or issue a decision on the ban to organize a mass event or to break a mass even, pursuant to the Act of 20 March 2009 on the safety of mass events (Journal of Laws of 2015, item 2139)

– in reference to all the gatherings and mass events in the area and time of the alert level being in force.

3. The decision issued by the competent organs of public administration pursuant to Paragraph 2 can be appealed against to the local regional court with the competent jurisdiction.

**Article 21.** 1. In case of the introduction of the third or fourth alert levels pursuant to Article 15 Paragraph 1, should the use of units and subunits of the Police turn out to be insufficient, or may turn out as insufficient, it is possible to use units and subunits of the Polish Armed Forces in support of the Police, appropriately to their specialist training, equipment and weapons in possession, as well as the current needs.

2. The deployment of the Polish Armed Forces, and in particular the start of the planning, information acquisition and cooperation with the organs of public administration, can take place upon the introduction of the third or fourth levels of alert and before the decision referred to in Paragraph 3.

3. The decision to use the Polish Armed Forces, which is not subject to announcement, in circumstances referred in Paragraph 1, is issued by the Minister of National Defense on the motion of the minister competent for internal affairs who specifies the scope and form of the assistance. The Minister of National defense informs, without delay, the President of the Republic of Poland and the Prime Minister about the decision.

4. The decision referred to in Paragraph 3 specifies the following:

- 1) the composition of units and subunits that are to be used in the assistance, their tasks and their number;
- 2) the area in which the units and subunits to be used in the assistance will be performing their tasks, as well as the time of performing these tasks;
- 3) the possible limitations in the use of own assets being part of the equipment of the units and subunits which are to be used for assistance.

5. The President of the Republic of Poland may issue a decision on the change or a revocation of the decision referred to in Paragraph 3.

6. The units and the subunits of the Polish Armed forces may use and apply the means of direct force and firearms pursuant to the rules specified for and to be observed by the soldiers of the Military Gendarmerie.

7. The units and the subunits of the Polish Armed forces used as assistance for the units or subunits of the Police remain in the chain of command of the Polish Armed Forces.

8. The organ coordinating the activities undertaken by the units and subunits of the Police, as well as units and the subunits of the Polish Armed Forces in a situation referred in Paragraph 1 is:

- 1) the Chief of Police of local jurisdiction – in case of activities undertaken by the units and subunits of the Police, as well as units and subunits of the Polish Armed Forces in the area of one of the voivodships;
- 2) The Commander in Chief of the Police – in case of Activities undertaken by the units and subunits of the Police, as well as units and subunits of the Polish Armed Forces in an area larger than the voivodship.

9. The Council of Ministers shall specify, in the form of an ordinance, the detailed terms and means of organizing the collaboration of the units and subunits of the Police with the units and subunits of the Armed Forces, taking into account the protection of the information exchanges, as well as the logistical support.

**Article 22.** 1. As part of the counter-terrorist activities, should it be necessary to counteract the direct, unlawful, and sudden attack against the life or health of a person, and when the use of a firearm in a manner inflicting the least possible damage is insufficient, and counteracting such an attack in any other manner is impossible, it is admissible, taking into account all the circumstances of the event of a terrorist nature and all possibilities of counter-terrorist activities, to use a firearm against the person committing the attack, which may result in the death or the immediate threat to this person's life or health. Such use shall be referred to henceforth as "special use of a weapon".

2. The special use of a weapon takes place according to the terms specified in the Act of 24 May 2013 on the means of direct force and firearms (Journal of Laws, item 628 and 1165, as well as of 2014, 24 and 1199), with the reservation of distinctions provided for in the article hereof.

3. In case of the special use of weapons, the provision of Article 7 Paragraph 1 and Article 48 of the Act referred to in Paragraph 2 are not applicable.

4. The special use of a weapon may be performed by officers of the Police, the Border Guard, Agency of Internal Security, soldiers of the Military Gendarmerie or soldiers of the Polish Armed Forces, who are members of groups performing counter-terrorist activities, henceforth referred to as the "counter-terrorist groups".

5. The decision to allow for the special use of a weapon can be made and revoked by the commander of activities. The commander of activities shall, without delay, transmit the decision to the commander of the counter-terrorist group, and inform the organ designating the commander of activities of the decision made.

6. Upon receiving the decision on the admissibility of the special use of a weapon, the commander of the counter-terrorist group may issue an order of the special use of the weapon by the officers or soldiers of the counter-terrorist group, defining the target and the means of the special use of a weapon.

7. The special use of a weapon is documented by the commander of the counter-terrorist group who, immediately upon the completion of the counter-terrorist activities, draws up a

protocol on the special use of a weapon, applying respectively Article 54 Paragraphs 1 and 2 referred to in Paragraph 2 hereof, and presents it to the commander of activities.

## Chapter 5

### **Specific provisions on the preparatory proceedings**

**Article 23.** 1. In case of a suspicion or attempt of committing or preparing an offence of a terrorist nature, in order to detect or detain a person, or to bring in the suspect by force, as well as in order to identify items which can serve as evidence in the case or which are subject to seizure in criminal proceedings, the prosecutor can decide on:

- 1) performing a search of the premises and other places located in the area indicated in the decision,
  - 2) arrest the suspected person
- if there are justified reasons to suspect that the suspected person or the items mentioned are present in this area.

2. In order to find the items referred to in Paragraph 1, it is also possible to perform the search of the persons, their clothes and personal items present in the area indicated in the decision.

3. The searches and arrests referred to in Paragraphs 1 and 2 can be performed at any time of day or night.

4. The decision of the prosecutor should be presented to the person on whom the search is to be performed.

5. With respect to the scope not regulated by means of this article, the search and arrest are regulated by provisions of the Act of 6 June 1997 – The Code of Criminal Procedure.

**Article 24.** 1. In case of a suspicion of an offence of a terrorist nature, should the good of the preparatory proceedings require so, the decision to present charges can be made on the basis of the information obtained during the surveillance and intelligence activities, including the Activities referred in Article 8.

2. In the case referred to in Paragraph 1, the court may, upon a motion of the prosecutor, apply the measure of remand custody for a period no longer than 14 days. The independent condition for remand custody is the justifiable demonstration of the commitment, attempt or preparation of an offence of a terrorist nature.

3. Remand custody can be prolonged according to the rules specified in Article 263 of the Act of 6 June 1997 – The Code of Criminal Procedure.

4. With respect to the scope not regulated by means of this article, remand custody is regulated by provisions of the Act of 6 June 1997 – The Code of Criminal Procedure.

## Chapter 6

### Changes in the currently binding provisions

**Article 25.** The following amendments are introduced to the Act of 6 April 1990 on Police (Journal of Laws of 2015 item 355, with later amendments<sup>9)</sup>):

- 1) To Article 1 Paragraph 2, after point 3 a point 3a is added:  
“3a) conducting counter-terrorist activities in the understanding of the Act of ... on counter-terrorist activities and amendments to selected other Acts (Journal of Laws Paragraph ...);”;
- 2) To Article 18:
  - a) in Paragraph 1:
    - in point 3 the comma is deleted and point 4 is repealed,
    - the common part is formulated as follows:  
“should the Police units or subunits turn out to be insufficient, units and subunits of the Polish Armed Forces, hereinafter referred to as “Armed Forces”, may be used for assistance,”
  - b) Paragraph 4 receives the following wording:  
“4. The assistance referred to in Paragraph 1 may also be provided in the form of threat prevention performed independently by the units and subunits of the Armed Forces in case the units and subunits of the Police do not have the capacity to prevent these threats effectively.”;
- 3) In Article 18a, Paragraph 1 receives the following wording:  
“1. In case of threat to safety and public order, if the Police forces are insufficient, or may turn to be insufficient to perform their tasks of safety and public order protection, the Prime Minister, upon request of the Minister competent for internal

---

<sup>9)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 529, 1045, 1066, 1217, 1268, 1890, 2023 and 2281 and of 2016 item 147 and 437.

affairs, following consultation with the Minister of National Defence, may order the use of soldiers of Military Gendarmerie to provide assistance to the Police”;

- 4) In Article 18a, Paragraph 1 receives the following wording:

“1. In case of threat to safety and public order, if the Police forces are insufficient, or may turn to be insufficient to perform their tasks, the Minister competent for internal affairs may order the use of Border Guard officers to provide assistance to the Police.”;

- 5) In Article 18c, Paragraph 1 receives the following wording:

”1. In cases such as the ones referred to in Article 18 Paragraph 1 or Article 21 Paragraph 1 of the Act of ... on anti-terrorist activities, as well as amendments to some other Acts, the Commander in Chief of the Police or the voivodship commander of the Police can order the Police to use devices which block the telecommunication in a given area for a period necessary to eliminate the threat or its effects, taking into consideration the need to minimize the effects of there being no telecommunication services available.”

**Article 26.** In the Act of 12 October 1990 on the protection of the state borders (Journal of Laws of 2015 item 930 and 1336) in Article 16:

- 1) Paragraph 3 point 2 receives the wording:

“2) to order a temporary suspension or restriction of traffic in specified border crossings, taking into account the need to ensure security of the state or public safety, as well as the protection of life or health of people, and the prevention of the expansion of an epidemic among animals.”;

- 2) after Paragraph 3a, Paragraph 3b is added in the following wording:

“3b. The minister competent for internal affairs can issue a decision on an up to seven days temporary suspension or restriction of traffic in the specified border crossings in case of the introduction of the second or higher level of alert referred to in Article 14 of the Act of ... on anti-terrorist activities and amendments to some other Acts (Journal of Laws, item. ...). The decision is enforceable immediately.”.

**Article 27.** In the Act of 12 October 1990 on the Border Guard (Journal of Laws of 2014 item 1402, with later amendments<sup>10)</sup>):

1) in Article 9e Paragraph 10a receives the following wording:

“The Commander in Chief of the Border Guard or the commander of a unit of the Border Guard can entitle his/her deputy to submit requests mentioned, respectively, in Paragraphs 1, 4, 9 and 10, or to the command of operational control pursuant to Paragraph 4.”;

2) In Article 9f after Paragraph 4, Paragraph 4a is added in the following wording:

“4a. In justified cases, when performing the activities referred to in Paragraph 1 there appear circumstances which are important for the purpose of verifying the previously acquired credible information about an offence, as well as to identify the perpetrators and obtaining evidence of the offence, the Commander in Chief of the Police in case of offences referred to in Paragraph 1 points 1–5, or commander of the division of the Border Guard in case of offences referred to in Paragraph 1 points 2–5 may, upon receiving a written consent from the competent prosecutor of the given jurisdiction, order to continue the activities for a further period upon the termination of the time periods referred to in Paragraph 4.”;

3) in Article 11d, Paragraph 1 receives the following wording:

“1. In case of a threat to the security and public order in the territorial scope of the border crossing, as well as the frontier zone, and should the forces of the Border Guard be insufficient or may turn to be insufficient to perform the tasks related to the protection of security and public order, or should it be justified by the degree of the threat, the Prime Minister may, on the motion of the minister competent for internal affairs in agreement with the Minister of National Defense, order the use of soldiers of the Military Gendarmerie in order to provide assistance to the Border Guard.”

**Article 28.** In the Act of 24 August 1991 on fire protection (Journal of Laws of 2016 item 191 and 298) in Article 14, Paragraph 1 point 3, a point 3a is added in the following wording:

“3a) biological emergency rescue;”.

---

<sup>10)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1822, of 2015 item 529, 1045, 1066, 1217, 1268, 1322, 1336, 1607, 1642, 1830, 1890, 2023 and 2281 and of 2016 item 147, 437 and 615.

**Article 29.** In the Act of 3 February 1995 on the protection of farm and forest land (Journal of Laws of 2015 items 909, 1338 and 1695) in Article 7 and after Paragraph 1 a Paragraph 1a is added in the following wording:

“1a. The provision referred to in Paragraph 1 is not applicable to the areas where no local spatial plans have been prepared.”

**Article 30.** In the Act of 6 June 1997 – Criminal Code (Journal of Laws item 553, with later amendments<sup>11)</sup>) the following amendments are introduced:

- 1) in Article 115 in § 20 the introduction to the list receives the following wording:  
“A offence of a terrorist nature is a criminal offence punishable by deprivation of liberty with the maximum period of at least three years, committed with the aim to:”;
- 2) in Article 117 § 2 is repealed;
- 3) in Article 118 § 3 is repealed;
- 4) after Article 126b, Article 126c is added in the following wording:  
“Article 126c. § 1.  
Whoever makes preparations for the offence specified in Article 117, Article 118 or Article 120,  
is subject to deprivation of liberty for a period of at least 3 years.  
§ 2. Whoever makes preparations for the offence specified in Article 118a § 1 or § 2, Article 122 or Article 123,  
is subject to deprivation of liberty for a period of up to 10 years.  
§ 3. Whoever makes preparations for the offence specified in Article 124 § 1 or Article 125,  
is subject to deprivation of liberty for a period of up to 3 years.”;
- 5) after Article 224a, Article 224b is added in the wording:  
“Article 224b. In case of a conviction for a committed offence provided for in Article 224a, the court adjudicates:
  - 1) a fine for the benefit of the State Treasury in the amount of at least PLN 10 000 and

---

<sup>11)</sup> Amendments to the mentioned Act have been announced in the Journal of Laws of 1997 item 840, of 1999 item 729 and 931, of 2000 item 548, 1027 and 1216, of 2001 item 1071, of 2003 item 1061, 1142, 1750, 1935 and 2255, of 2004 item 219, 626, 889 and 2426, of 2005 item 732, 757, 1109, 1363, 1479 and 1493, of 2006 item 1409, 1592 and 1648, of 2007 item 589, 850, 859 and 1378, of 2008 item 560, 782, 1056, 1080 and 1344, of 2009 item 504, 533, 1317, 1323, 1474, 1540 and 1589, of 2010 item 46, 227, 229, 625, 626, 842, 857, 1018, 1021, 1228, 1474 and 1602, of 2011 item 78, 130, 202, 245, 381, 549, 678, 767, 964, 1135, 1280, 1381 and 1431, of 2012 item 611, of 2013 item 849, 905, 1036 and 1247, of 2014 item 538, of 2015 item 396, 541, 1549, 1707 and 1855 and of 2016 item 189, 428 and 437.



- 2) a cash benefit referred to in Article 39 point 7 in the amount of at least PLN 10 000.”;
- 6) in Article 255a the present wording is now marked as § 1 and § 2 is added in the following wording:

“§ 2. Whoever in order to commit an offence of a terrorist nature participates in a training which makes such an offence possible,  
is subject to the limitation or the deprivation of liberty up to 3 years.”;
- 7) after Article 259, Article 259a and Article 259b are added in the following wording:

“Article 259a. Whoever crosses the border of the Republic of Poland with the purpose of committing in a territory of a different country an offence of a terrorist nature or an offence specified in Article 255a or Article 258 § 2 or 4,  
is subject to the deprivation of liberty from 3 months to 5 years.  
Article 259b. Upon a motion of the prosecutor, the court shall apply an extraordinary mitigation of the penalty, and may even conditionally suspend the execution of the penalty adjudicated to the perpetrator for the offence specified in Article 259a, who had voluntarily refrained from:

  - 1) committing in the territory of another country an offence of a terrorist nature or an offence specified in Article 255a or Article 258 § 2 or 4 and has revealed all the important circumstances of the offence before the offence prosecution organs or has prevented the intended offence from being committed;
  - 2) aiding and abetting other persons to commit the offence specified in Article 259a and has revealed before the offence prosecution organs all important circumstances of the offence, and in particular information about the person who has committed the offences as specified in Article 259a.”.

**Article 31.** In the Act of 22 August 1997 about the protection of persons and property (Journal of Laws of 2014 item 1099, 2015 item 1505 and 2016 item 65) the following amendments are introduced:

- 1) in Article 5 Paragraph 2 point 4, the full stop is replaced with a comma and point 5 is added in the following wording:

“5) the facilities, including buildings, equipment, installations, and services contained in the list of the facilities, installations, equipment and services which are part of the critical infrastructure.”;

- 2) in Article 7:
- a) Paragraph 1 receives the following wording:  
“1. The head of the unit who directly manages the areas, facilities and equipment included in the list which is referred to in Article 5 paragraph 5, or a person entitled by him/her, have the duty to agree on the protection plan of these areas, facilities and equipment with the competent voivodship chief of police, and in the case of threats of a terrorist nature, with the territorially competent director of the delegation of the Agency of Internal Security”,
  - b) in Paragraph 2 point 2 receives the following wording:  
“2) contain an analysis of the state of potential threats, including threats of terrorist nature and the current state of security of the unit;”;
- 3) in Article 36 Paragraph 1 point 5 letter ‘a’ receives the following wording:  
“a) within the limits of the protected facilities and areas – in the cases referred to in Article 45, point 1, letters a–c and point 2, as well as Article 47, points 3, 6 and 7 of the Act of 24 May 2013 about the means of direct force and firearms, with the exclusion of cases of counteracting activities directly aimed at the attack referred to Article 45 letters 1–c of this Act,”.

**Article 32.** In the Act of 29 August 1997 – Banking Law (Journal of Laws of 2015 item 128, with later amendments<sup>12)</sup>) in Article 105 Paragraph 1 point 2, the letter z is added in the following wording:

- "z) The Head of the Agency of Internal Security, pursuant to the mode and terms provided for in Article 34a of the Act of 24 May 2002 r. about the Agency of Internal Affairs and the Intelligence Agency (Journal of Laws of 2015 item 1929 and 2023, as well as 2016 items 147, 437 and...);”.

**Article 33.** In the Act of 26 October 2000 on commodity exchange (Journal of Laws of 2014 item 197, with later amendments<sup>13)</sup>), after Article 54 Paragraph 1 point 7, point 7a is added in the following wording:

- “7a) The Head of the Agency of Internal Security, in the mode and pursuant to the terms specified in Article 34a of the Act of 24 May 2002 on the Agency of Internal

---

<sup>12)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 559, 978, 1166, 1223, 1260, 1311, 1348, 1357, 1513, 1634, 1830, 1844, 1854, 1864 and 2281 and of 2016 item 615.

<sup>13)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 478, 1223, 1260, 1505 and 1618 and of 2016 item 178.

Security and the Intelligence Agency (Journal of Laws of 2015 items 1929 and 2023 as well as 2016, items 147, 437 and ...);”.

**Article 34.** The following changes are introduced to the Act of 16 March 2001 on the Government Protection Bureau (Journal of Laws of 2016, item . 552):

1) in Article 14 Paragraph 2 receives the following wording:

“2. In cases referred to in Article 45 point 1 letters a–c and e, point 2 and point 3 letter a as well as in Article 47 point 1, point 2 letter a, points 3 and 5–7 of the Act of the 24 May 2013 about the means of direct force and firearms, the officer may use the firearm or make use of it.”;

2) in Article 128, Paragraph 2 receives the following wording:

“2. In cases referred to in Article 45 Paragraph 1, letters a–c and e, point 2, point 3 letter a and point 4 letter a, as well as in Article 47 point 1, point 2 letter a, points 3 and 5–7 of the Act of 24 May 2013 on the means of direct force and firearms, members of the Marshall Guard may use firearms or make use of it.”.

**Article 35.** In the Act of 24 August 2001 on Military Gendarmerie and the military enforcement organs (Journal of Laws of 2016, items 96, 147, 178 and 437) the following amendments are introduced:

1) in Article 4, Paragraph 1 point 3, point 3a is added in the following wording:

“3a) performing counter-terrorist activities pursuant to the Act of ... on anti-terrorist activities, as well as the amendments to some other Acts (Journal of Laws item . ...), in areas of facilities owned by cells and organisational units subordinate to the Minister of National Defense or supervised by the Minister of National Defense, or administered by these cells and organisational units;”;

2) in Article 17, Paragraph 1 point 10, point 10a is added in the following wording:

“10a) the observation and recording with the use of technical means of the events in public spaces and, in case of surveillance and intelligence as well as administrative operations conducted pursuant to this Act – also with the sound accompanying these events;”;

3) in Article 31, Paragraph 10a receives the following wording:

“10a. The Commander in Chief of the Military Gendarmerie or the commander of a division of the Military Gendarmerie may entitle their deputy to file a request referred

to in Paragraphs 1, 4, 9 and 10, or to order an operational control pursuant to Paragraph 4.”;

- 4) in Article 42, Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45, point 1 letters a–c and e, points 2, 3 and Paragraph 4, letters a and b, as well as in Article 47, points 1–3 and 5–7 of the Act of 24 May 2013 on the means of direct force and firearms, the soldiers of the Military Gendarmerie may use firearms or make use of it.”.

**Article 36.** The following changes are introduced to the Act of 24 May 2002 on the Agency of Internal Security and the Intelligence Agency (Journal of Laws of 2015, items 1929 and 2023 and of 2016, items 147 and 437):

- 1) in Article 5, in Paragraph 1 point 2, point 2a is added in the following wording:

“2a) the recognition, prevention and detection of threats aimed at the security of the IT and communications systems of the organs of public administration important to the continued functioning of the state, or the systems of the IT and communications network included in the uniform list of facilities, installations, equipment and services being part of the critical infrastructure, as well as the IT and communication systems of owners and holders of the facilities, installations, and equipment of the critical infrastructure referred to in Article 5b, Paragraph 7 points 1 and 4 of the Act of 26 April 2007 on crisis management (Journal of Laws of 2013, item 1166, of 2015, item 1485, as well as of 2016, item 266);”;

- 2) in Article 6, Paragraph 1 point 7, point 7a is added in the following wording:

“7a) the recognition, prevention and detection of events of a terrorist nature aimed at citizens or the property of the Republic of Poland outside of the borders of the state, with the exclusion of events of a terrorist nature aimed at soldiers or property of the Polish Armed Forces;”;

- 3) after Article 22a, Article 22b is added in the following wording:

“Article 22b. 1. Should the information or materials obtained by the ABW in course of their execution of tasks referred to in Article 5, Paragraph 1:

- 1) indicate that the offence of espionage has been committed, or
- 2) justifiably demonstrate an activity aimed at committing an offence of a terrorist nature

– the Head of ABW, in case when it is justified by the security of the state, may refrain from the duty to notify the competent prosecutor of the justified suspicion of an offence

and of the person who, in light of the information and materials gathered by the ABW, may be its perpetrator.

2. The Head of ABW may refrain from the duty specified in Paragraph 1 in the case when the perpetrator suspected of espionage or of an offence of a terrorist nature has consciously and voluntarily:

- 1) revealed all circumstances of the offence committed or of the activities conducted
- 2) had committed him/herself to engage in a covert cooperation with ABW.

3. The Head of ABW may refrain from the duty referred to in Paragraph 1 upon seeking an opinion of the Prosecutor General or the Minister Coordinator of Special Services, should such a person be appointed.

4. Refraining from the duty specified in Paragraph 1 refers to public officers performing the activities specified in this article.

5. The provision of Paragraph 1 is not applicable in case the perpetrator of the offence of espionage or the person suspected of an offence of a terrorist nature:

- 1) has committed a deliberate offence against one's life or another deliberate offence resulting in the death of a person or a substantial detriment to one's health, or
- 2) participated as an accomplice in such an offence or attempted to commit it, or
- 3) induced a third person to commit a prohibited act referred to in Paragraph 1.

6. In case the perpetrator of the offence of espionage or the person suspected of an offence of a terrorist nature continues, despite having begun a covert collaboration with ABW, activities which are to the detriment of the Republic of Poland and in violation of the terms of this collaboration, or has committed one of the offences stipulated in Paragraph 5, or has participated as an accomplice in such an offence, or had induced a third person to commit the offence, the Head of ABW notifies the competent prosecutor of the fact.

7. The Head of ABW notifies the competent prosecutor also in the case when it is revealed that the perpetrator of the offence of espionage or the person suspected of an offence of a terrorist nature who began a covert collaboration with ABW, has consciously refrained from revealing all the circumstances of the offence or the activities referred to in Paragraph 1.

8. In case of a threat to the life or health of the person referred to in Paragraph 1, or persons indicated by this person, the Head of ABW shall apply with regard to this person or the persons indicated by this person the necessary protective measures

appropriate to the threat, as well as the necessary assistance including financial aid in justified cases. Provision of Article 35, Paragraph 3 and Article 36 are applied respectively.

9. The Head of ABW shall withdraw the protection or assistance in case of:

- 1) a deliberate violation by the person subject to protection or assistance, referred to in Paragraph 8, of the rules or recommendations in the scope of this protection or assistance.;
- 2) the occurrence of at least one circumstance referred to in Paragraph 5–7.

10. In case the protection or assistance is withdrawn in the cases referred to in Paragraph 9, the perpetrator of the offence of espionage or an offence of a terrorist nature is obliged to return to the Head of ABW the equivalent of the benefits received as part of such assistance, as well as the documents referred to in Article 35, Paragraph 3, should such have been issued to this person. The provision is applicable accordingly to the protected persons referred to in Paragraph 8.”;

- 4) in Article 25, Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45, point 1, letters a–c and e, points 2, 3 and point 4, letters a, b and letter c, the first indent, as well as in Article 47, point 1, point 2 letters a and points 3–7 of the Act of 24 May 2013, the ABW officer may use a firearm or make use of it.”;

- 5) in Article 26 Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45, point 1, letters a–c and e, points 2, 3 and letter a, as well as in Article 47, points 1, 6 and 7 of the Act of 24 May 2013 on the means of direct force and firearms, the ABW officer may use a firearm or make use of it.”;

- 6) after Article 32, Article 32a–32e is added in the following wording:

“Article 32a. 1. In order to prevent and counteract, as well as combat events of a terrorist nature which are aimed against IT and communication systems of public administration organs and which are important to the continued functioning of the state, or IT and communication networks included in the unified list of facilities, installations, equipment and services being part of the critical infrastructure, as well as IT and communication systems of the owners, holders of independent and dependent facilities, installations, and equipment of critical infrastructure referred to in Article 5b, Paragraph 7, points 1 and 4 of the Act of 26 April 2007 on crisis management, or data processed in

these systems, and to prevent and detect offences of a terrorist nature in this area, as well as prosecute their perpetrators, ABW may perform a security assessment of these IT and communication systems, henceforth referred to as “security assessment”.

2. Security assessments are performed according to an annual schedule of security assessments, which is agreed on with the minister competent for IT. In justified cases, the security assessment can be performed regardless of the schedule.

3. ABW informs the entity managing the IT and communications system referred to in Paragraph 1 about being included in the system of the annual security assessments.

4. The security assessment involves security tests conducted on the telecommunication and IT system in order to verify their vulnerabilities, i.e. the weaknesses of the asset or the security measures of the telecommunication and IT systems which can be abused by jeopardizing the integrity, confidentiality, accountability and accessibility of this system.

5. The security assessment is performed in line with the principle of minimum disturbance in the functioning of the IT and communications system and minimum restriction to its availability, and cannot lead to any damages in the IT and communications system subject to assessment.

6. In order to minimise the negative effects of the security assessment, ABW comes to an agreement with the entity referred to in Paragraph 1 on the framework conditions for the performance of the assessment, and in particular the date of the beginning, the schedule and the scope, as well as the type of security tests to be run as part of the security assessment.

7. ABW may produce and acquire equipment and computer software referred to in Article 269b of the Criminal Code, and use these in order to determine the vulnerability of the assessed systems to potential offences referred to in Article 165 § 1, point 4, Article 267 § 3, Article 268a § 1 or 2 in connection with § 1, Article 269 § 2 or Article 269a of the Criminal Code.

8. By using the equipment or computer software referred to in Paragraph 7, ABW may obtain access to information of which it is not an addressee by cracking or bypassing the electronic, magnetic, IT or any other safety measure, or may obtain access to the IT and communications system in whole or in part.

9. The information obtained by ABW as a result of the security assessment conducted, remain a legally protected secret and cannot be used in the execution of the

statutory tasks of ABW, and are subject to an immediate witnessed and recorded destruction.

10. Upon completion of the security assessment, ABW prepares a report which is presented to the entity subject to the security assessment. The report contains a summary of the activities performed as part of the security assessment, as well as an indication of the detected vulnerabilities of the IT and communications system, i.e. the weaknesses of the asset or the security measure of the IT and communications system which can be taken advantage of.

11. Should the detected weakness occur in other IT and communications system, ABW shall, without delay, inform the minister competent for IT about the detected vulnerability, and about the possibility of its occurrence in other IT and communications systems.

12. The Head of ABW shall specify, in the form of an instruction, the types of the security tests and the conditions and manner in which they are to be run, taking into consideration the need for the security assessment to be complete.

Article 32b. 1. In case information is obtained about the occurrence of an event of a terrorist nature in reference to systems or data referred to in Article 32a, Paragraph 1, the Head of ABW may request the entities referred to in Article 5, Paragraph 1, point 2a to provide information about the construction, functioning, and operational rules of the IT and communication systems in place, including computer passwords, access codes, and other data providing access to the system, and further use them so as to prevent or react to events of a terrorist nature in connection with the systems or data referred to in Article 32a Paragraph 1, and to prevent and detect offences of a terrorist nature in the area, as well as to prosecute their perpetrators.

2. The information and data referred to in Paragraph 1 are subject to protection provided for in the provisions on the protection of classified information, and can be available only to the ABW officers carrying out surveillance and intelligence operations in the case, and to their superiors, entitled to perform an oversight of these activities.

3. The State Treasury bears liability for the damages caused as a result of the infringement of Paragraph 2 pursuant to the rules provided for in the Civil Code.



Article 32c. 1. The court, having received a written request from the Head of ABW submitted upon a written consent from the Prosecutor General may, by means of a decision,:

- 1) order to block
- 2) or request the administrator of the IT and communications system to block
  - access in the IT and communications system to specified IT data or IT and communications services which are related to the event of a terrorist nature, for a time no longer than 30 days, in order to prevent, counteract, and detect offences of a terrorist nature, as well as to prosecute their perpetrators.

2. The request referred to in Paragraph 1 is submitted with materials justifying the need to block access in the IT and communications system to specified IT data or IT and communications services which are related to the event of a terrorist nature.

3. The decision referred to in Paragraph 1 is issued by the Regional Court in Warsaw.

4. In urgent cases and if it can cause an event of a terrorist nature, the Head of ABW may, upon a written consent of the Prosecutor General,:

- 1) order to block
- 2) or request the administrator of the IT and communications system to block
  - access in the IT and communications system to specified IT data or IT and communication services which may be related to an event of a terrorist nature, addressing, at the same time, the court referred to in Paragraph 2, with an application to issue a decision in the case. If the court does not issue a consent within 5 days of the order to block or an instruction requesting the administrator of the IT and communications administrator to block access in the IT and communications system of specified IT data or IT and communications system connected with an event of a terrorist nature, the Head of ABW shall stop the blocking of the IT data and IT and communications services.

5. The administrator of the IT and communications system has the duty to immediately perform the activities specified in the decision of the court, or in the request from the Head of ABW.

6. The request from the Head of ABW referred to in Paragraph 1, should include, in particular:

- 1) the number of the case and its cryptonym, if such has been assigned;

- 2) a description of the event of a terrorist nature with its legal qualification, if possible;
- 3) the circumstances justifying the need to block access to the specified IT data or IT and communication services in the IT and communications system;
- 4) the data allowing to unequivocally identify the subject or object that the blocking of access to the IT data or IT and communications services is to be applied, with an indication of the place and the means of its application;
- 5) the objective and time of the blocking of access to IT data or IT and communications services.

7. The block is imposed for a period no longer than 3 months. The court referred to in Paragraph 2 may, upon a written request from the Head of ABW and upon a written consent from the Prosecutor General, issue, for a period of no longer than three more months, a decision on the one-time prolongation of the blocking, if the reasons for its imposition have not subsided.

8. Provisions of Paragraph 2 and are applicable respectively to the application referred to in Paragraphs 4 and 7. Before issuing a decision, the court, referred to in Paragraphs 1, 4 and 7, acquaints itself with the materials serving as grounds for the request.

9. The requests referred to in Paragraph 1, 4 and 7, are considered by the court in a one-judge panel, and the activities of the court related to the consideration of these requests should be performed in conditions designed for the transmission, retention and provision of access to classified information, as well as with the appropriate application of provisions issued pursuant to Article 181 § 2 of the Code of Criminal Procedure. Only the prosecutor and the Head of ABW can participate in the sitting of the court.

10. The Head of ABW and the Prosecutor General are entitled to a complaint against the decision of the court referred to in Paragraph 1, 4 and 7. The provisions of the Code of Criminal Procedure are applied respectively in case of a complaint.

11. The blocking of access to IT data and IT and communications services related to events of a terrorist nature is stopped in case:

- 1) the court does not, within the period of 5 days, issue a permit to block access to IT data and IT and communications services;
- 2) the court does not issue a permit to prolong the blocking of IT data and IT and communications services;

- 3) the period for which the blocking of access to IT data and IT and communications services had been imposed has expired, if the reasons for its imposition have not ceased to exist.

12. The court, the Prosecutor General, as well as the Head of ABW shall, observing all the provisions pertaining to the protection of classified information, maintain electronic registers of the decisions, written permits, instructions and applications regarding the blocking of IT data or IT and communication services related to the event of a terrorist nature.

13. The Head of ABW informs the minister competent for IT about the blocking of IT data or IT and communication services related to the event of a terrorist nature, provided the administrator of the system or the service provider has a seat in the territory of the Republic of Poland.

14. The Prime Minister shall specify, in the form of an ordinance, the manner of blocking the IT data or IT and communication services related to the terrorist event, as well as the manner of retention and transmission of requests and instructions, taking into consideration the need to ensure a classified means of the activities undertaken and the materials obtained.

Article 32d. 1. The Head of ABW keeps a register of events violating the security of the IT systems referred to in Article 5 Paragraph 1 point 2a.

2. The register referred to in Paragraph 1, contains information including:

- 1) the identification of the entity for whom the IT system operates, as well as the probable beginning date and the time for which the security of the system had been infringed;
- 2) the date and the time when the infringement of the security of the system was detected, as well as the probable beginning date and the time for which the security of the system had been infringed;
- 3) identification of the source of the event infringing the security of the system;
- 4) description of the detected infringement of the security of the system, as well as the activities of the entity causing the infringement of security;
- 5) description of the damages which have emerged in the system, or which may emerge as a result of the event infringing the security of the system.

3. The data referred to in Paragraph 2 is transmitted to the Head of ABW, with the observance of provisions on the protection of classified information, by the

administrators of the IT and communications systems referred to in Article 5 Paragraph 1, point 2a, immediately upon the detection of an event infringing the security in the system.

4. Data from the register are made available to the minister competent for IT, with the observance of provisions on the protection of classified information.

Article 32e. 1. The Head of ABW performs an analysis of the events infringing the security of the IT systems and issues recommendations, henceforth referred to as “recommendations” to the entities referred to in Article 32d, Paragraph 3, with the aim to increase the level of security of the IT systems so as to ensure their integrity, confidentiality, accountability and accessibility.

2. Within one month upon receiving the recommendations, the entities referred to in Paragraph 1 may file reservations to the Head of ABW in reference to the recommended means of increasing the level of security of the IT systems for reason of the negative impact the recommended activities may have on the functioning of the system, or due to the emergence of new vulnerabilities.

3. The Head of ABW addresses the reservations received pursuant to Paragraph 2 within a month upon receiving them and either maintains the recommendations or presents changed recommendations.

4. The entities who have received the recommendations from the Head of ABW inform, within three months upon receiving them, the Head of ABW about the manner and scope in which the recommendations have been considered.

5. Failure to consider the recommendations serves as a basis for the Head of ABW to address the organ supervising the entity referred to in Paragraph 4, with information about the acceptance of the recommendation or with a request to undertake actions aimed at the execution of the recommendations.”;

7) in Article 34 and after Paragraph 2, Paragraph 2a is added with the following wording:

“2a. The administrator of the data sets, referred to in Paragraph 2, provides the Head of ABW, by means of telecommunication, with the information gathered in the data sets, without the need to present each time a name authorization issued by the Head of ABW, presented by an ABW officer with the appropriate official ID referred to in Paragraph 2, provided that the organisational unit of ABW which is the recipient of the information meets the following conditions:

- 1) has the equipment making it possible to make a record in the system of who obtained the data, when were they obtained, with what purpose and what were these data;
- 2) has the technical and organisational security means allowing for the use of data in line with the purpose for which they had been obtained;
- 3) the specificity and scope of the tasks performed justify such provision of access.”;

8) after Article 34, Article 34a is added in the following wording:

“Article 34a. 1. Within the remit of its competence, the ABW may, if it is necessary for the effective prevention of offences specified in Article 5 Paragraph 1 point 2, or for the detection or identification of perpetrators and obtaining of evidence, use the information processed by banks and which are a banking secret, as well as information on the agreements on securities accounts, agreements on money accounts, agreements on insurance policies, and other agreements referring to the trading in financial instruments, provision of payment services or agreements concluded with investment fund contributors, and in particular the data processed by entitled entities pertaining to persons who have concluded such agreements.

2. The provision of Paragraph 1 is applied respectively to:

- 1) entities performing activities pursuant to the Act of 26 October 2000 on commodity exchanges (Journal of Laws of 2014, item 197, with later amendments<sup>14)</sup>);

---

<sup>14)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 478, 1223, 1260, 1505 and 1618 and of 2016 item 178.

- 2) entities performing insurance activities;
- 3) entities performing activities in the scope of the trading of securities and other financial instruments pursuant to the Act of 29 July 2005 on trading of financial instruments (Journal of Laws of 2014, item 94, with later amendments <sup>15)</sup>);
- 4) obliged institutions and entities providing financial services in the understanding of the Act of 16 November 2000 on counteracting money-laundering and financing terrorism (Journal of Laws of 2016, items 299 and 615);
- 5) entities performing Activities in the scope of payment services pursuant to the Act of 19 August 2011 on payment services (Journal of Laws of 2014, item 873, with later amendments <sup>16)</sup>);
- 6) investment funds and investment fund societies conducting business pursuant to the Act of 27 May 2004 on investment funds (Journal of Laws of 2014, item 157, with later amendments <sup>17)</sup>).

3. The information and data referred to in Paragraph 1, as well as the information connected with the transmission of this information and data are subject to protection provided for in the provision on the protection of classified information and can only be available to the ABW officers conducting the surveillance and intelligence activities in the case, as well as to their supervisor, entitled to perform oversight of these activities. Files from the operations including these information and data is also made available to the courts and prosecutors, should it be used in criminal prosecution.

4. The information and data referred to in Paragraph 1 are made available pursuant to a decision issued by the Regional Court in Warsaw upon a written request by the Head of ABW.

5. The request referred to in Paragraph 4 contains the following:

- 1) the number of the case and its cryptonym, if such has been assigned;
- 2) a description of the offence with its legal qualification;
- 3) the circumstances justifying the need to make the information and data available;
- 4) identification of the entity to whom the information and data pertain;

---

<sup>15)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 586, of 2015 item 73, 978, 1045, 1223, 1260, 1348, 1509, 1513, 1634, 1844 and 1890 and of 2016 item 65 and 615.

<sup>16)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1916 and of 2015 item 1764, 1830 and 1893.

<sup>17)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 73, 978, 1166, 1223, 1260, 1311, 1348, 1357, 1513, 1634, 1830, 1844, 1854, 1864 and 2281 and of 2016 item 615.

- 5) the entity obliged to grant access to the information and data;
- 6) type and scope of the information and data.

6. Upon consideration of the request, the Regional Court in Warsaw shall, by means of a decision, allow the access to information and data referred to in Paragraph 1, specifying their type, scope and the entity obliged to provide such access, or refuse to allow the information and data be made available. Provision of Article 27 Paragraph 11 is applicable respectively.

7. The Head of ABW is entitled to a complaint against the decision of the Regional Court in Warsaw as referred to in Paragraph 6.

8. In case the Regional Court in Warsaw allows access to the information and data referred to in Paragraph 1, the Head of ABW shall notify in writing the entity referred to in Paragraph 5, point 5, about the decision of the Regional Court in Warsaw, indicating its date and reference number, as well as the type and scope of information and data which are to be made available, as well as the entity, to whom the information and data pertain, as well as the ABW officer entitled to receive them.

9. Within up to 120 days of providing the information and data referred to in Paragraph 1, the Head of ABW shall inform the entity referred to in Paragraph 5, point 4, about the decision of the Regional Court in Warsaw allowing the access to the said information and data.

10. Upon an application from the Head of ABW, submitted upon receiving a written consent from the Prosecutor General, the Regional Court in Warsaw can postpone, by means of a decision, the obligation referred to in Paragraph 9 for a specified time with the possibility of its prolongation, should it be justifiably demonstrated that by notifying the entity referred to in Paragraph 5 point 4, the pending surveillance and intelligence activities may be jeopardized. The provision of Article 27 Paragraph 11 is applied respectively.

11. If in the period referred to in Paragraph 9 or 10, pre-trial proceedings have been launched, the entity referred to in Paragraph 5, point 4 is notified about the decision of the Regional Court in Warsaw about the provision of access to information and data by the prosecutor or, on his instruction, by the Head of ABW, before the closing of the pre-trial proceedings or, without delay, upon their discontinuance.

12. If the information and data referred to in Paragraph 1, have not provided reason to launch pre-trial proceedings, the Head of ABW shall, without delay, notify the entity referred to in Paragraph 5, point 5.

13. The materials gathered in the mode referred to in Paragraphs 1–10, and which do not constitute information which would confirm the offence, are subject to immediate recorded and witnesses destruction. The destruction of the materials is ordered by the Head of ABW.

14. The State Treasury is held liable for the damages inflicted as a result of the violation of Paragraph 3 pursuant to the terms specified in the Civil Code.

15. The Prime Minister shall specify, by means of an ordinance, the means of processing of the data and information referred to in Paragraph 1, in the data sets, and the types of organizational units of ABW entitled to make use of these sets, as well as sample documents obligatory in the processing of these data, taking into consideration the protection of data against unauthorized access.”;

9) in Article 43:

a) in Paragraph 2, a comma is added in point 6, and point 7 in the following wording:  
“7) the destruction, immobilisation or take-over of control over the flight of a model aircraft or an unmanned aerial vehicle”;

b) Paragraph 3 receives the following wording:

“3. The Activities referred to in Paragraph 2 points 2, 4, 6 and 7, may also be performed in the immediate neighbourhood of the protected equipment, areas or facilities, should this be deemed necessary to ensure their security or the security of the persons inside.”;

10) in Article 44, point 1 receives the following wording:

“1) holds Polish citizenship;”;

11) in Article 60:

a) in Paragraph 1 point 5 receives the following wording:

“5) loss of Polish citizenship.”;

b) in Paragraph 2, the full stop is replaced with a semicolon, and point 9 is added in the following wording:

“9) obtaining the citizenship of another country.”.



**Article 37.** The following changes are introduced in the act of 3 July 2002 – Act on Aviation (Journal of Laws of 2016 item, 605):

1) after Article 126, Article 126a is added in the following wording:

“Article 126a. 1. An unmanned aerial vehicle, including a model aircraft, can be destroyed, immobilised, or a control may be taken over its flight in case when:

- 1) the course of the flight or the functioning of the unmanned aerial vehicle:
  - a) presents a threat to the life or health of a person,
  - b) presents a threat to protected facilities, equipment or areas,
  - c) disrupts the course of a mass event or presents a threat to its participants,
  - d) presents a justified suspicion that it may be used as a means of a terrorist attack;
- 2) the unmanned aerial vehicle flies in the airspace with flight restrictions, in the airspace over the territory of the Republic of Poland where flights of aerial vehicles are prohibited from the level of the terrain to a specified altitude.

2. The destruction of an the unmanned aerial vehicle or taking over control of its flight in the given case and referred to in:

- 1) Paragraph 1 point 1 letters a, b and d – falls within the remit of officers of the Police, the Border Guard, the Government Protection Bureau, Agency of Internal Security, Intelligence Agency, Central Anticorruption Bureau, Army Counter-Intelligence Service, Customs Service, and Penitentiary Service, soldiers of the Military Gendarmerie and of the Polish Armed Forces, as well as employees of specialist armed protection forces,
- 2) Paragraph 1 point 1 letter c – falls within the remit of officers of the Police, the Border Guard, the Government Protection Bureau, Agency of Internal Security, Army Counter-Intelligence Service, soldiers of the Military Gendarmerie and employees of specialist armed protection forces,
- 3) Paragraph 1 point 2 – falls within the remit of the soldiers of the Polish Armed Forces

– pursuant to the terms specified in separate provisions.”;

2) in Article 186b:

a) after Paragraph 4, Paragraph 4a is added in the following wording:

“4a. The manager of the airport performs the tasks in the scope of the protection of the general access zones of the airport, in cooperation with the protection services active in the area of the airport.”,

b) after Paragraph 9, Paragraph 9a is added in the following wording:

“9a. In order to perform its tasks, the Border Guard is entitled to use image recording systems located in the area of the airport, and the recordings from these systems. The copies of the recordings made available to the Border Guard by the airport manager, and not containing evidence which would allow for the launching of criminal proceedings, proceedings in case of petty offence, disciplinary proceedings, or which can be used in cases as part of investigative activities or as evidence in already pending proceedings, are kept by the Border Guard, however for a period no longer than 30 days upon their being made available, following which they are destroyed.”.

**Article 38.** The following changes are introduced to the Act of 27 March 2003 on spatial planning and management (Journal of Laws of 2015 item 199, with later amendments<sup>18)</sup>):

1) in Article 50:

a) Paragraph 1 receives the following wording:

“1. The public purpose investment is located according to the local plan and, in the case of its absence, according to a decision on establishing the location of the public purpose investment. The condition referred to in Article 61 Paragraph 1 point 4, is applicable respectively, with the reservation of Article 61 Paragraph 2a.”,

b) after Paragraph 2b, 2c is added in the following wording:

“2c. The investor in the public purpose investment referred to in Paragraph 2, may apply for a decision to be issued determining the location of the public purpose investment connected with the defence and security of the state or the protection of the state frontier.”;

---

<sup>18)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 443, 774, 1265, 1434, 1713, 1777, 1830 and 1890.

- 2) in Article 61, after Paragraph 2, Paragraph 2a is added in the following wording:

“2a. Provisions of Paragraph 1 points 1–4 are not applied to a public purpose investment which is justified by the need of the defence and security of the state or the protection of the state frontier.”.

**Article 39.** The following changes are introduced to Article 22 of the Act of 11 September 2003 on professional military service (Journal of Laws of 2014 item 1414, with later amendments<sup>19)</sup>):

- 1) in Paragraph 1, point 2 receives the following wording:

“2) the Chancellery of the President of the Republic of Poland, the Chancellery of the Prime Minister, the Bureau of National Security, the Agency of Internal Security, the Intelligence Agency, as well as the common organisational unit of the prosecution,”;

- 2) Paragraph 1a receives the following wording:

“1a. No consent of a professional soldier to serve in the official position of a military prosecutor or in the Agency of Internal Security is required.”.

**Article 40.** The following changes are introduced to the Act of 27 May 2004 on investment funds (Journal of Laws of 2014 item 157, with later amendments<sup>20)</sup>):

- 1) in Article 281 Paragraph 1, after point 8 point 8a is added in the following wording:

“8a) The Agency of Internal Security, if it is necessary for the effective prevention of an offence, its detection and identification of perpetrators, and the obtaining of evidence according to the terms and the mode specified in Article 34a of the Act of 24 May 2002 on the Agency of Internal Security and the intelligence Agency (Journal of Laws of 2015, items, 1929 and 2023 and of 2016, items 147, 437 and ...);”;

- 2) in Article 282 w Paragraph 3 point 3 receives the following wording:

“3) the General Inspector of Financial Information, the Head of the Agency of Internal Security, the Chief of the National Centre of Criminal Information, the tax authorities, the Customs Service organs or organs of tax control – in the scope, mode and terms provided for in separate Acts;”.

---

<sup>19)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1822, of 2015 item 1066, 1217, 1268 and 1830 and of 2016 item 178 and 308.

<sup>20)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 73, 978, 1166, 1223, 1260, 1311, 1348, 1357, 1634, 1830, 1844, 1854, 1864 and 2281 and of 2016 item 615.

**Article 41.** The following changes are introduced to the Act of 16 July 2004 – Telecommunication Act (Journal of Laws of 2014, item 243, with later amendments<sup>21)</sup>):

1) after Article 60a, Article 60b is added in the following wording:

“Article 60b. 1. The subscriber, with the exclusion of the subscriber using the publically available telephone services provided by means of a public phone or by dialing the access number to the network of the services provider, provides the service provider with at least the following data:

- 1) in case the subscriber is a natural person:
  - a) name and surname,
  - b) PESEL number, should the subscriber have one, or the name, series number and the number of the document confirming the person’s identity and, in the case of a foreigner who is not a citizen of a member state or of the Swiss Confederation – the passport number or number of the residence card;
- 2) in case of a subscriber who is not a natural person:
  - a) name,
  - b) REGON or NIP (tax) identification number, or the number from the National Court Register or from the Business Activity Register, or another register kept in a member state.

2. The subscriber provides the data referred to in Paragraph 1 when concluding an agreement in a hardcopy or an electronic version. The subscriber being a party to the agreement on the pre-paid services in a public telecommunications network, supplies the service provider with the data referred to in Paragraph 1. The data may also be provided in an electronic form or in any other way specified by the provider of these services.

3. The provider of services begins to provide telecommunications services:

- 1) not before the positive verification of the data supplied by the subscriber with the data specified in Paragraph 1:
  - a) point 1, contained in the document confirming the identity of the subscriber who is a natural person,
  - b) point 2, contained in the appropriate register, or

---

<sup>21)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 827 and 1198, of 2015 item 1069, 1893 and 2281 and of 2016 item 147 and 542.

- 2) upon the provision by the subscriber the data specified in Paragraph 1 and upon their electronic verification with the use of:
  - a) means of electronic identification used for verification in the IT system of a national bank,
  - b) data confirmed by means of a safe electronic signature verified by a valid qualified certificate,
  - c) means of electronic identification used for verification in the IT system of the provider of the telecommunications services if the subscriber's data have already been verified in reference with another agreement,
  - d) means of electronic identification used for verification in the IT system which meets the requirements specified in the provision issued pursuant to Article 20a Paragraph 3 of the Act of 17 February 2005 on the computerization of public entities (Journal of Laws of 2014, item 1114 and of 2016, item 352).

4. The service provider can perform the confirmations referred to in Paragraph 3 point 1 letter a also via a third person acting on behalf of the service provider.

5. The minister competent for IT shall indicate, in the form of an announcement, the IT systems which ensure credibility and authorization of their user, referred to in Paragraph 3 point 2 letter d.”;

- 2) in Article 179 after Paragraph 9, Paragraph 9a is added in the following wording:

“9a. The President of the Office of Electronic Communications provides information to the authorized entities about the transferred numbers contained in the data base referred to in Article 71 Paragraph 4, pursuant to the terms and the mode specified in separate provisions. Provision of Paragraph 4b is applied accordingly.”.

**Article 42.** In the Act of 29 July 2005 on trading in financial instruments (Journal of Laws of 2014, item 94, with later amendments<sup>22)</sup>), in Article 149 point 8a, point 8b is added in the following wording:

“8b) The Head of the Agency of Internal Security in the mode and on terms specified in Article 34a of the Act of 24 May 2002 on the Agency of Internal Security and Intelligence Agency (Journal of Laws of 2015, items 1929 and 2023, and of 2016, items 147, 437 and ...);”.

---

<sup>22)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 586, of 2015 item 73, 978, 1045, 1223, 1260, 1348, 1505, 1513, 1634, 1844 and 1890 and of 2016 item 65 and 615.

**Article 43.** The following changes are introduced to the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of 2014, item 253, with later amendments<sup>23)</sup>):

- 1) in Article 5, Paragraph 1:
  - a) in point 1, the letter g receives the following wording:

“g) other than the ones specified in letters a–f, aimed at the security of the defence potential of the country, the Polish Armed Forces or organizational units of the Ministry of Defence, as well as countries which ensure reciprocation,”
  - b) after Paragraph 2, Paragraph 2a is added in the following wording:

“2a) the recognition, prevention and detection of events and offences of a terrorist nature, aimed at the defence potential of the country, the Polish Armed Forces or organizational units of the Ministry of Defence;”
- 2) in Article 6 Paragraph 1 after point 3, point 3a is added in the following wording:

“3a) the recognition, counteraction and prevention of acts of a terrorist nature aimed at the personnel and property of the Polish Armed Forces outside of the territory of the state, as well as combatting such acts”;
- 3) in Article 10:
  - a) after Paragraph 1 Paragraph 1a and 1b are added in the following wording:

“1a. in order to pursue the cooperation referred to in Paragraph 1 point 1, and in particular in order to ensure the safety and the proper execution of the Army Intelligence Service outside of the territory of the country, task teams may be established in the Army Intelligence Service composed of officers of the Army Intelligence Service, professional soldiers appointed to official positions in the Army Intelligence Service, and soldiers serving in the units or subunits of the Polish Armed Forces.

1b. Soldiers serving in the units and subunits of the Polish Armed Forces, being part of the task teams referred to in Paragraph 1a, execute the commands and orders according to the procedures in force in the Army Intelligence Service. These soldiers have the entitlements referred to in Article 26, Article 28 and Article 30.”

---

<sup>23)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 502 and 1055, of 2015 item 1066 and 1224 and of 2016 item 147 and 437.

b) after Paragraph 2, Paragraph 2a is added in the following wording:

“2a. The Minister of National Defence shall specify, by means of an instruction not subject to announcement, the manner and mode of establishing the task teams referred to in Paragraph 1a, and shall designate the soldiers serving in the units or subunits of the Polish Armed Forces to participate in these teams.”;

4) after Article 27, Article 27a is added in the following wording:

“Article 27a. 1. If the information or materials obtained by the Army Counter-Intelligence Service in the course of performing the duties referred to in Article 5 Paragraph 1:

- 1) indicate that the offence of espionage has been committed or
- 2) justifiably demonstrate an activity aimed at committing an offence of a terrorist nature

– The Head of the Army Counter-Intelligence Service may, in case it is justified from the point of view of the security of the state, refrain from the duty to notify the competent prosecutor about the justified suspicion about the offence as well as the person who, in light of the information and materials gathered by the Army Counter-Intelligence Service would be the perpetrator.

2. The Head of the Army Counter-Intelligence Service may refrain from the duty referred to in Paragraph 1 in case the perpetrator of the offence of espionage, or the suspected person of an offence of a terrorist nature, have consciously and voluntarily:

- 1) revealed all the circumstances of the committed act or performed activity;
- 2) committed him/herself to engage in a covert cooperation with the Army Counter-Intelligence Service.

3. The Head of Army Counter-Intelligence Service may refrain from the duty referred to in Paragraph 1 upon obtaining an opinion from the Prosecutor General and the Minister Coordinator of Special Service, if such has been nominated.

4. The decision to refrain from the duty referred to in Paragraph 1 refers to public officers performing activities in the proceedings specified herein.

5. The provision on Paragraph 1 is not applicable if the perpetrator of the offence of espionage or a person suspected of an offence of a terrorist nature:

- 1) has committed a deliberate offence against one’s life or another deliberate offence resulting in the death of a person or a substantial detriment to one’s health, or
- 2) participated as an accomplice in such an offence or attempted to commit it, or

3) induced a third person to commit a prohibited act referred to in Paragraph 1.

6. In case the perpetrator of the offence of espionage or the person suspected of an offence of a terrorist nature continues, despite having begun a covert collaboration with the Army Counter-Intelligence Service, the activities which are to the detriment of the Polish Armed Forces or to the defence capability of the Republic of Poland, what is in violation of the terms of this collaboration, or has committed one of the offences stipulated in Paragraph 5, or has participated as an accomplice in such an offence, or had induced a third person to commit the offence, the Head of the Army Counter-Intelligence Service notifies the competent prosecutor of the fact.

7. The Head of the Army Counter-Intelligence Service notifies the competent prosecutor also in the case when it is revealed that the perpetrator of the offence of espionage or the person suspected of an offence of a terrorist nature who began a covert collaboration with the Army Counter-Intelligence Service, has consciously refrained from revealing all the circumstances of the offence or activities referred to in Paragraph 1.

8. In case of a threat to the life or health of the person referred to in Paragraph 1, or persons indicated by this person, the Head of the Army Counter-Intelligence Service shall apply with regard to this person or the persons indicated by this person the necessary protective measures appropriate to the threat, as well as the necessary assistance including financial aid in justified cases. Provisions of Article 39, Paragraph 3 and Article 40 are applied respectively.

9. The Head of the Army Counter-Intelligence Service shall withdraw the protection or assistance in case of:

- 1) a deliberate violation by the person subject to protection or assistance, referred to in Paragraph 8, of the terms or recommendations in the scope of this protection or assistance;
- 2) the occurrence of at least one circumstance referred in Paragraph 5–7.

10. If the protection or assistance is withdrawn in the cases referred to in Paragraph 9, the perpetrator of the offence of espionage or an offence of a terrorist nature is obliged to return to the Head Army Counter-Intelligence Service the equivalent of benefits received as part of such assistance, as well as the documents referred to in Article 39, Paragraph 3, should such have been issued to this person. The provision is applicable accordingly to the protected persons referred to in Paragraph 8.”;



5) in Article 30 Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45 point 1 letters a–c and e, point 2 and point 4, letters a, b and letter c, the third indent, as well as in Article 47, point 1, point 2 letter a, as well as points 3–7 of the Act of 24 May 2013 on the means of direct force and firearms, the Army Counter-Intelligence Service officer may use a firearm or make use of it.”;

6) in Article 30a Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45 point 1, letters a–c and e, point 2 and point 3 letter a, as well as in Article 47 points 1, 6 and 7 of the Act of 24 May 2013 on the means of direct force and firearms, the Army Counter-Intelligence Service officer may use a firearm or make use of it.”;

**Article 44.** The following changes are introduced to the Act of 9 June 2006 on the service of Army Counter-Intelligence and Army Intelligence officers (Journal of Laws of 2014, item 1106 and 822 as well as of 2015, item 1066, 1217, 1268 and 2023):

1) Article 3 Paragraph 1 receives the following wording:

“1) holding Polish citizenship”;

2) in Article 19:

a) in Paragraph 1, point 5 receives the following wording:

“5) loss of Polish citizenship.”,

b) in Paragraph 2, point 9 is added in the following wording:

“9) obtaining the citizenship of another country.”.

**Article 45.** The following changes are introduced to the Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Law of 2014, item 1411, with later amendments<sup>24)</sup>):

1) in Article 15, Paragraph 2 receives the following wording:

“2. In the cases referred to in Article 45 point, letters a–c and e, point 2, 3 and 4, letters a, b and letter c, second indent m, as well as in Article 47 point 1, point 2 letter a, points 3 and 5–7 of the Act of 24 May 2013 on the means of direct force and firearms, an Anti-Corruption Bureau officer may use a firearm or make use of it.”;

---

<sup>24)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1822, of 2015 item 1066, 1217, 1224, 1268 and 2023 and of 2016 item 147, 437 and 615.

- 2) in Article 30:
  - a) in Paragraph 2 in point 3 the full stop is replaced by a semicolon and a point 4 in the following wording is added:

“4) the destruction, immobilisation or take-over of control over the flight of a model aircraft or an unmanned aerial vehicle”,
  - b) after Paragraph 2a, Paragraph 2b is added in the following wording:

“3. The Activities referred to in Paragraph 2 points 2a, 3, 6 and 4, may also be performed in the immediate neighbourhood of the protected equipment, areas or facilities, should this be deemed necessary to ensure their security or the security of the persons inside.

**Article 46.** The following changes are introduced to the Act of 14 July 2006 on the entry into, residence in and exit from the Republic of Poland of nationals of the European Union Member States and their family members (Journal of Laws of 2014, item 1525 and of 2015, item 1247):

- 1) in Article 73 Paragraph 1 receives the following wording:

“1. The decision to expel an EU citizen or a family member who is not an EU citizen is issued, ex officio or on the request of the Minister of National Defence, Head of the Internal Security Agency, Head of the Intelligence Agency, Head of the Army Counter-Intelligence Service, Head of the Army Intelligence Service, Commander in Chief of the Border Guard, Commander in Chief of the Police, by a voivode with the jurisdiction as to the location of the stay of the EU citizen or a family member who is not an EU citizen, or the location where the disclosure of the fact or incident which is the basis for the application to expel the EU citizen or a family member who is not an EU citizen has taken place.”;
- 2) after Article 73b, Article 73c is added in the following wording:

“Article 73c. 1. The Minister competent for internal affairs shall, upon a motion of the Commander in Chief of the Police, Head of the Internal Security Agency or the Head of the Army Counter-Intelligence Service, issue a decision on the expulsion from the territory of the Republic of Poland of an EU citizen, or family member who is not an EU citizen, with regard to whom it is feared that s/he may be involved in terrorist or espionage activities, or who is suspected of committing one of these offences.

2. The decision referred to in Paragraph 1 is subject to immediate execution.”.

**Article 47.** In the Act of 8 September 2006 on the State Medical Rescue Services (Journal of Laws of 2013, item 757, with later amendments<sup>25)</sup>) in Article 11, Paragraph 3, after point 6, point 6a is added in the following wording:

“6a) in the anti-terrorist units subordinate to the minister competent for internal affairs and which are not medical treatment entities;”.

**Article 48.** The following changes are introduced to the Act of April 2007 on crisis management (Journal of Laws of 2013, item 1166, of 2015, item and of 2016, item 266):

1) Article 3 point 11 receives the following wording:

“11) an event of a terrorist nature – should be understood as a situation referred to in Article 2 point 7 of the Act of ... on anti-terrorist Activities, as well as other Act (Journal of Laws, item. ...).”;

2) Article 12a is repealed;

3) Article 23 is repealed.

**Article 49.** In the Act of 27 August 2009 on Customs Service (Journal of Laws of 2015, item 990, with later amendments<sup>26)</sup>) in Article 66, Paragraph 3 receives the following wording:

“3. In the cases referred to in Article 45 points 1, 2 and point 3 letter a, as well as in Article 47 point 1, point 2 letter a, points 3 and 5–7 of the Act of 24 May 2013 on the means of direct force and firearms, the officers performing activities related to the execution of tasks referred to in Article 2 Paragraph 1 points 4–6, serving in separate organisational units of the Customs Service, or the officers entitled by the Head of the Customs Service to perform these tasks, may use a firearm or make use of it.”.

**Article 50.** In the Act of 5 November 2009 on the cooperative savings and loan banks (Journal of Laws of 2011, item 1450, with later amendments<sup>27)</sup>), in Article 9f, Paragraph 1 point 25, the full stop is replaced with a semicolon and point 26 is added in the following wording:

“26) on the request of the Head of the Internal Security Agency, and pursuant to the mode and terms specified in Article 34a of the Act of 24 May 2002 on the Agency

---

<sup>25)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2013 item 1245 and 1635, of 2014 item 1802, of 2015 item 1887 and 1991 and of 2016 item 65.

<sup>26)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 1045, 1217, 1268, 1269, 1479, 1642, 1830, 1890 and 2023 and of 2016 item 147.

<sup>27)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 978, 1158, 1259, 1311, 1830, 1854, 1864 and 2281 and of 2016 item 615.

of Internal Security and Intelligence Agency (Journal of Laws of 2015, item 1929 and 2023 as well as of 2016 items 147, 437 and ...).”.

**Article 51.** In the Act of 9 April 2010 on the Penitentiary Service (Journal of Laws of 2014 item 1415, with later amendments<sup>28)</sup>), in Article 19, Paragraph 2 receives the following wording:

“2. In cases referred to in Article 45 point 1 letters a, b and e, point 2, point 3 letter a, point 5 and in Article 47 point 3, 6 and 7 of the Act of 24 May 2013 on the means of direct force and firearms, the officer may use a firearm or make use of it.”.

**Article 52.** The following changes are introduced to the Act of 15 April 2011 on medical treatment (Journal of Laws 2015, item 618, with later amendments<sup>29)</sup>):

1) in Article 2, Paragraph 1, point 1a receives the following wording:

“1a) a military unit – an organisational unit which is not a unit maintained by the central budget, and for whom the founding entity is the Minister of National Defence, and which provides health care services, also outside of the territory of Poland, pursuant to the Act of 17 December 1998 on the terms of use of stay of the Polish Armed Forces abroad (Journal of Laws of 2014, item 1510);”;

2) in Article 22, Paragraph 4a:

a) point 2 receives the following wording:

“2) the procedures and standards of medical treatment in the medical treatment facilities specified in point 1”;

b) the shared part receives the following wording:

“– mindful of the need to ensure the health security of people, as well as of the type and place of the activities conducted and the scope of the health care services provided.”;

3) in Article 40 Paragraph 1 receives the following wording:

“1. The unit maintained from the state budget and the military unit, the founding entity of which is the Minister of National Defence, performs medical treatment Activities in the scope of emergency operations, treatment, medical evacuation, and sanitary transport with the use of sanitary vehicles, aircraft, permanent and tabular equipment and medical supplies, medical material means and medications being part of

---

<sup>28)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2014 item 1822 and of 2015 item 529, 928, 1066, 1217, 1268 and 1830.

<sup>29)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 788, 905, 1640, 1697, 1844, 1887, 1918 and 1991.

the equipment of the Polish National Forces, provided to soldiers and civilian personnel, as well as soldiers of foreign armies and their civilian personnel”.

**Article 53.** The following changes are introduced to the Act of 24 May 2013 on the means of direct forces and firearms (Journal of Laws item 628 and 1165 as well as 2014 item 24 and 1199):

1) in Article 47 point 6, the full stop is replaced by a semicolon and point 7 in the following wording :

“7) the destruction or immobilisation of an unmanned aerial vehicle, in cases specified in the Act of 3 July 2002 –Aviation Law.”;

2) in Article 48, Paragraph 3 receives the following wording:

“3. The procedure referred to in Paragraph 1 and 2, or its specific elements, in particular the possibility of giving a warning shot, can be refrained from if:

- 1) their execution would pose a direct threat to the life or health of the entitled person or a third person or
- 2) it is necessary in order to prevent the occurrence of an event of a terrorist nature referred to in Article 2 point 7 of the Act of ... on antiterrorist activities and amendments to other Acts (Journal of Laws item ....), and other means could turn out to be insufficient due to the present circumstances.”

**Article 54.** The following changes are introduced to the Act of 12 December 2013 on foreigners (Journal of Laws item 1650, with later amendments<sup>30)</sup>)

1) Article 310 receives the following wording:

“Article 310. The decision obliging a foreigner to return is issued by:

- 1) ex officio – commander of the Border Guard unit, or the commander of the Border Guard post, who has recognized there being a reason justifying the decision obliging the foreigner to return;
- 2) upon an application from the voivode, Minister of National Defence, Head of the Internal Security Agency, Head of the Intelligence Agency, Head of the Army Counter-Intelligence Service, Head of the Army Intelligence, organ of the Customs Service, voivodships or poviata chief of Police – by the commander of the Border Guard Unit or commander of the Border Guard post, with the jurisdiction as to the

---

<sup>30)</sup> Amendments to the mentioned Act have been announced in the Journal of Laws of 2014 item 463 and 1004, of 2015 item 1274, 1607 and 1767 and of 2016 item 65.

location of the seat of the organ submitting the application or the place of stay of the foreigner.”;

- 2) after Article 329, Article 329a is added in the following wording:

“Article 329a. 1. Minister competent for internal affairs, upon an application from the Commander in Chief of the Police, Head of the Internal Security Agency or Head of the Army Counter-Intelligence Service, issues a decision obliging a foreigner to return with respect to a foreigner who is feared to be involved in terrorist or espionage activities, or who is suspected of committing one of these offences.

2. The decision referred to in Paragraph 1 is subject to immediate execution.”;

- 3) in Article 449, Paragraph 2 point 16, the full stop is replaced by a semicolon and Paragraph 17 is added in the following wording:

“17) the central visa register referred to in Article 449a Paragraph 1.”;

- 4) in Article 449a, Paragraph 2 receives the following wording:

“2. The data processed in the central visa register is made available to consuls.”;

- 5) in Article 450 Paragraph 1, the introduction to the calculation receives the following wording:

“The data processed in the national set of register, registrars, records and lists related to cases pertaining to foreigners, referred to in Article 449 Paragraph 2 points 1–12, 16 and 17, is made available to the following entities, in the scope necessary to perform their statutory tasks:”.

**Article 55.** The following changes are introduced to the Act of 18 March 2016 on the specific solutions related to the organization of the visit of His Holiness Pope Francis in the Republic of Poland and the World Youth Days – Kraków) 2016 (Journal of Laws item 393):

- 1) in Article 11, Paragraph 2 point 1 in letter k, the semicolon is replaced by a comma and a letter l is added in the following wording:

“l) the scope of tasks executed as part of the medical support of the World Youth Days, assigned by the Minister of National Defence;”;

- 2) in Article 13

- a) Paragraph 9 receives the following wording:

“9. The persons from the units subordinate to the Minister of National Defence who have been assigned to the medical support of the World Youth Days, can provide medical assistance to also persons not referred to in Article 40

Paragraph 1 of the Act of 15 April 2011 on medical treatment (Journal of Laws of 2015 item 618, with later amendments<sup>31)</sup>). The execution of these tasks takes place in line with a plan and does not require an agreement referred to in Article 15 Paragraph 1.”,

- b) after Paragraph 9, Paragraphs 10 and 11 are added in the following wording:

“10. With regard to persons referred to in Paragraph 9, the Minister of National Defence shall ensure the civil liability insurance for the damages caused by the activities performed as part of the provided medical assistance referred to in Paragraph 11, or the unlawful desistance of providing such services.

11. The tasks related to the medical services provision during the World Youth Days in the scope of emergency activities, treatment, medical evacuation and sanitary transport by persons referred to in Paragraph 9, shall be performed with the use of sanitary vehicles, aircraft, permanent and tabular equipment and medical supplies, medical material means, as well as medications being part of the equipment of the Polish Armed Forces.”;

- 3) Article 14 receives the following wording:

“Article 14. The medical assistance provided in the hospital tent by the field team with a physician and a field team without a physician, an air ambulance team, a walking patrol team or a mobile patrol team, or in the medical assistance point is documented in a KPP/MCR form. Sample of the KPP/MCR information form is an appendix hereto.”;

- 4) in Article 29 after Paragraph 2, Paragraph 2a is added in the following wording:

“2a. The organiser has the duty to ensure, for the purpose of the operational use of the installations referred to in Paragraph 1, free access to electrical energy and fibre optic connections.”;

- 5) an appendix is added to the Act in the wording specified in the appendix to this Act.

---

<sup>31)</sup> Amendments to the single text of the mentioned Act have been announced in the Journal of Laws of 2015 item 788, 905, 1640, 1697, 1844, 1887, 1918 and 1991.

## Chapter 7

### **Transitional, adapting and final provisions**

**Article 56.** 1. In order to perform the tasks referred to in Article 5 Paragraph 1 point 2a, Article 32a, Article 32d, Article 32e and Article 43 Paragraph 2 Paragraph 4 of the act amended in Article 36, the Head of ABW shall:

- 1) put in an order for the services and technical equipment, IT hardware and software,
- 2) undertaken investment activities,
- 3) ensure the presence of personnel,
- 4) conduct training for ABW officers

– within 24 months upon the present Act comes into force.

2. In the period specified in Paragraph 1, Head of ABW shall perform the tasks specified in Article 5 Paragraph 1 point 2a, Article 32a–32e and Article 43 Paragraph 2 Paragraph 4 of the Act amended in Article 36, taking into consideration the personal and material assets presently at hand.

3. The annual plan of the security assessments referred to in Article 32a Paragraph 2 of the amended in Article 36 will be for the first time developed by the Head of ABW for the year 2017.

**Article 57.** 1. By January 2017, the subscribers of prepaid services who had concluded their agreements before the present act came into force, are obliged to supply the prepaid services providers with the data referred to in Article 60b of the act amended in Article 41, in the wording given by means of this act, and further to verify this information in a manner stipulated in Article 60b Paragraph 3 and 4 of the act amended in Article 41, in the wording given by means of this act.

2. The supplier of prepaid services in a public telecommunications network ceases to provide services to subscribers who:

- 1) have failed to supply the data specified in Article 60b of the act amended in Article 41, in the wording given by means of this act, or
- 2) whose data have not been verified in line with Article 60b Paragraph 3 and 4 of the act amended in Article 39, in the wording given by means of this act.

**Article 58.** 1. The Head of the Office for Foreigners, in agreement with the minister competent for foreign affairs, shall include the data processed in the central visa register



maintained pursuant to Article 449a Paragraph 1 of the act amended in Article 54, into the national set of registers, records and lists of cases pertaining to foreigners, which is referred to in Article 449 Paragraph 2 of this act, within 12 upon this act coming into force.

2. Before the incorporation of the central visa register, which include data coming from the registers maintained by the minister competent for foreign affairs and consuls, and which is referred to in Article 428 Paragraph 1 Paragraph 2 letter c of the act amended in Article 54, in the national set of registers, records and lists of cases pertaining to foreigners, which is referred to in Article 449a Paragraph 1 of the act amended in Article 54, the data processed in the central visa register are made available to the consuls, Head of the Office for Foreigners, as well as the Head of ABW, in the scope necessary for the execution of their statutory tasks.

**Article 59.** 1. In the years 2017–2026, the maximum limit of spending from the state budget, which is the financial effect of the present act of law, is PLN 351.9 mln, with the limits assigned to the successive years being:

- 1) 2017 – PLN 91.9 mln;
- 2) 2018 – PLN 94.2 mln;
- 3) 2019 – PLN 23.6 mln;
- 4) 2020 – PLN 19.6 mln;
- 5) 2021 – PLN 19.6 mln;
- 6) 2022 – PLN 22.6 mln;
- 7) 2023 – PLN 20.6 mln;
- 8) 2024 – PLN 20.6 mln;
- 9) 2025 – PLN 19.6 mln;
- 10) 2026 – PLN 19.6 mln.

2. Thea Head of ABW supervises the spending limits referred to in Paragraph 1, and makes a cost estimate of the limit's use according to the balance at the end of each quarter, and in the case of the fourth quarter – according to the state on 20 November of the given year.

3. In case the spending limit adopted for the given year and referred to in Paragraph 1 is jeopardized or exceeded, and if at the beginning of the calendar year and before the last assessment referred to in Paragraph 2, a part of this annual limit proportionate to this period is exceeded by at least 10%, a corrective mechanism is applied, which is aimed at reducing the spending from the state budget being the financial effect of the present act.

4. The organ competent to introduce the corrective mechanism referred to in Paragraph 3, is the Head of ABW.

**Article 60.** The act comes into force the day following its announcement, with the exception of Article 41, which comes into force 30 days upon its announcement.