Strasbourg, 13 May 2016 **CDL-REF(2016)036**

Opinion No. 839 / 2016 Engl.Only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

POLAND

ACT
of 15 January 2016
AMENDING
THE POLICE ACT AND CERTAIN OTHER ACTS

POLICE ACT
of 6 April 1990
(Consolidated text)

EXTRACTS
FROM THE POLISH LEGISLATION
DEVELOPING THE NOTION OF METADATA

JOURNAL OF LAWS
OF THE REPUBLIC OF POLAND

Warsaw, 4 February 2016

Item 147

ACT[1]
of 15 January 2016

amending the Police Act and certain other acts[2]

Art. 1. The Police Act of 6 April 1990 (Journal of Laws 2015, item 355, as amended[3]) is amended as follows:

1) in art. 19
   a) para. 1:
      - the introduction to the enumeration is replaced by:
      'In the event that preliminary investigations are carried out by Police to obtain and record evidence and to prevent, detect and determine perpetrators prosecuted on public indictment for any intentional crimes:',

      - point 8 is replaced by:
      '8) prosecuted under international agreements ratified with prior consent granted by the Act and set out under Polish criminal law,',

   b) para. 6 is replaced by:
      '6. The operational controls are performed confidentially and consist of:
      1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;
      2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
      3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
      4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
      5) gaining access to and checking the contents of mail.',

   c) para. 6a and 6b are added after para. 6 as follows:
      '6a. the actions referred to in para. 6 point 2 on extracting and recording images in the inside spaces referred to in art. 15, para. 1 point 4a, are not part. of the operational controls.

[1] Translation made by the Council of Europe.
[2] The present Act amends the Act of 12 October 1990 on the Border Guard, the Act of 28 September 1991 on Fiscal Controls, the Act of 21 August 1997 on the Military Court System, the Act of 27 July 2001 on the Common Court System, the Act of 24 August 2001 on the Military Police and Military Law Enforcement Units, the Act of 24 May 2002 on the National Security Agency and the Intelligence Agency, the Act of 18 July 2002 on the provision of services supplied by electronic means, the Telecommunications Act of 16 July 2004, the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, the Act of 9 June 2006 on the Central Anti-Corruption Bureau and the Act of 27 August 2009 on the Customs Office.
[3] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 529, 1045, 1066, 1217, 1268, 1890, 2023 and 2281.

6b. Carrying out the actions referred to in para. 6a, does not require the consent of the court.',

d) para. 9 is replaced by:

'9. In justified cases, when new circumstances relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the district court, upon written request from the Commander-in-Chief of the Police made after receiving written consent from the Prosecutor General may, also after the date of expiry of the periods referred to in para. 8, issue further rulings on prolonging the operational controls for consecutive periods whose total duration cannot exceed 12 months.',

e) para. 9a is added after para. 9 as follows:

'9a. the Commander-in-Chief of the Police, Commander of the Central Investigations Bureau or the Commander of the Voivodship Police can authorise their deputy to make the requests referred to in para. 1, 3, 8 and 9 or to order operational controls in accordance with para. 3.',

f) para. 12 is replaced by:

'12. Telecommunication companies, postal operators and suppliers of services provided by electronic means are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by Police.',

g) para. 12a is added after para. 12 as follows:

'12a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[4]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by Police as appropriate for their infrastructure.',

h) para. 15f-15j are added after para. 15e as follows:

'15f. In the event that the materials referred to in para. 15:

1) contain information referred to in art. 178 of the Code of Criminal Proceedings, the Commander-in-Chief of the Police, Commander of the Central Investigations Bureau or the Commander of the Voivodship Police shall order their immediate, collective and official destruction;

2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code, or any confidential information related to the professions or its duties referred to in art. 180 § 2 of the Code of Criminal Proceedings, the Commander-in-Chief of the Police, Commander of the Central Investigations Bureau or the Commander of the Voivodship Police shall pass on those materials to the prosecutor.

15g. In the event referred to in para.15f point 2, the prosecutor, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 15f point 2;

[4] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code.

15h. Immediately after the prosecutor files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 15g point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings.

15i. The prosecutor is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 15g point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings apply in that appeal.

15j. Police authorities are obliged to enforce the order of the court to destroy the materials referred to in para. 15h and to carry out the immediate, collective and official destruction of the materials which are prohibited in criminal proceedings. The Police authorities shall immediately inform the prosecutor when the materials referred to in para. 15g have been destroyed.',

i) para. 16a-16d are added after para. 16 as follows:

'16a. The district court, the Prosecutor General, the district prosecutor and the Police authorities shall keep registers of rulings, written statements of consent, requests and orders related to operational controls.

16b. The Commander-in Chief of the Police shall keep a central register of requests and orders related to the operational controls carried out by Police authorities to the extent foreseen for those registers.

16c. The data contained within documents from the operational controls can be registered individually at the Police organisational units responsible for enforcing orders on operational controls, to the extent foreseen for the registers referred to in para.16a.

16d. The registers referred to in para. 16a-16c, are kept in electronic format, in compliance with the provisions on the protection of confidential information.',

j) para. 20 is replaced by:

'20. The ruling of the court referred to in:

1) para. 1, 3, 8 and 9- may be appealed against by the Police authority that filed a request for that ruling;
2) para. 3 and 15c- may be appealed against by the competent prosecutor, as referred to in para. 1.

The provisions of the Code of Criminal Proceedings shall apply accordingly in the appeal.',

2) art. 20c is replaced by:

'Art. 20c. 1. In order to prevent and detect crimes, safeguard human lives or health or support search and rescue missions, the Police can obtain any other related data that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[5]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data',
3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.

2. The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge. It shall be disclosed:
1) to the police officer indicated in the written request from the Commander-in-Chief of the Police, Commander of the Central Investigations Bureau, Commander of the Voivodship Police or any other person duly authorised by them;
2) upon oral request from the police officer holding a written authorisation from the persons referred to in point 1;
3) through the telecommunications network, to the police officer holding a written authorisation from the persons referred to in point 1.

3. In the event described in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of employees from the telecommunications company, postal operator or supplier of services provided by electronic means, or with their involvement if necessary and if such a possibility exists in the agreement made between the Commander-in-Chief and that entity.

4. The disclosure of information to the Police, as referred to in para. 1, can take place through a telecommunications network, if:
1) the telecommunications networks used ensure that:
a) the person who obtained the information, the type of information and the time in which the information was obtained can be determined,
b) technical and organisational safeguards are in place to restrict access to unauthorised persons;

2) it is justified due to the specific character or scope of the tasks carried out by Police organisational units or of the actions taken by them.

5. The Commander-in-Chief of the Police, Commander of the Central Investigations Bureau and the Commander of the Voivodship Police shall keep registers of requests to obtain telecommunications, postal or internet data, containing information identifying the Police organisational unit and police officer that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with legislation on the protection of confidential information.

6. The data referred to in para. 1 that is relevant for criminal proceedings shall be passed on by the Commander-in-Chief of the Police, Commander of the Central Investigations Bureau or the Commander of the Voivodship Police to the prosecutor with territorial or material jurisdiction. The prosecutor shall decide on the scope and method of use of the data.

7. The data referred to in para. 1 that is not relevant for criminal proceedings should be immediately, collectively and officially destroyed.'

[5] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.

3) art. 20ca and art. 20cb are added after art. 20c as follows:

'Art. 20ca. 1. Controls on Police when extracting telecommunications, postal or internet data are carried out by the district court with jurisdiction over the Police authority that gained access to the data.

2. The Police authority referred to in para. 1 shall send a report to the district court referred to in para. 1 on a six-monthly basis in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained during the reporting period and the type of data that was obtained;
2) the legal classification of the acts for which the telecommunications, postal and internet data was requested or any information concerning data that was obtained to safeguard human lives or health or to support the search and rescue missions.

3. Within the framework of the controls referred to in para. 1, the district court can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the Police.

4. The district court shall inform the Police of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of 20cb para. 1, is not subject to the controls referred to in para. 1.

Art. 20cb. 1. In order to prevent or detect crimes, safeguard human lives or health or support search and rescue missions, Police can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 20c para. 2-7 apply when granting access to and processing the data referred to in para. 1.';

4) art. 20d is repealed
5) art. 20da para. 1 is replaced by:

'1. In a search for missing persons, the Police can extract telecommunications, postal or internet data and process it without the knowledge or consent of the person concerned; the provisions of art. 20c para. 2-7 apply.',

Art. 2. The Act of 12 October 1990 on the Border Guard (Journal of Laws 2014, item 1402 as amended[6]) is amended as follows:

1) in art. 9e:
   a) para. 1:
      - point 4 is replaced by:

[6] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as item 1822 and in the Journal of Laws 2015 as items 529, 1045, 1066, 1217, 1268, 1322, 1336, 1607, 1642, 1830, 1890, 2023 and 2281.

‘4) specified in art. 183 § 2, 4 and 5, art. 184 § 1 and 2, art. 263 § 1 and 2, art. 278 § 1, art. 291 § 1 and art. 306 of the Penal Code, art. 55 and art. 56 of the Act of 29 July 2005 on counteracting drug addiction (Journal of Laws 2012, item 124 as amended[7]) and art. 44 and art. 46a of the Act of 1 July 2005 on the procurement, preservation and transplantation of cells, tissue and organs (Journal of Laws 2015, item 793, 1893 and 1991) and art.109 item 1 of the Act of 23 July 2003 on the protection and care of historical monuments (Journal of Laws 2014, item 1446 as amended[8]), wherever those crimes are related to transporting illegal goods across the national border.’,

- point 7 is replaced by:
‘7) prosecuted under international agreements ratified with prior consent granted by the Act and set out under Polish criminal law,’,

b) para. 7 is replaced by:
‘7. The operational controls are performed confidentially and consist of:
1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;
2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
5) gaining access to and checking the contents of mail.’,

c) para. 7a and 7b are added after para. 7 as follows:
‘7a. the actions referred to in para. 7 point 2 on extracting and recording images in the inside spaces referred to in art. 11 para. 1 point 7a are not part. of the operational controls.
7b. Carrying out the actions referred to in para. 7a, does not require the consent of the court.’,

d) para. 10 is replaced by:
‘10. In justified cases, when new circumstances, relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the district court, upon written request from the Commander-in-Chief of the Border Guard or the Commander of the Border Guard Unit made after receiving written consent from the Prosecutor General, as referred to in para.1, may, also after the date of expiry of the periods referred to in para. 9, issue further rulings on prolonging the operational controls for consecutive periods whose total duration cannot exceed 12 months.’,

e) para. 10a is added after para. 10 as follows:
‘10a. the Commander-in-Chief of the Border Guard or the Commander of the Border Guard unit can authorise their deputy to make the requests referred to in para. 1, para. 4 point 1, para. 9 and 10 or to order the operational controls in accordance with para. 4 point 1.’,

f) para. 13 is replaced by:

[7] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 28, 875, 1893, 1916 and 2014.
[8] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 397, 774 and 1505.

‘13. Telecommunications companies, postal operators and suppliers of services provided by electronic means are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Border Guard.’.

g) 13a is added after para. 13 as follows:

‘13a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[9]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Border Guard as appropriate for their infrastructure.’,

h) 16f-16j are added after para. 16e as follows:

‘16f. In the event that the materials referred to in para. 16:

1) contain information referred to in art. 178 of the Code of Criminal Proceedings, the Commander-in-Chief of the Border Guard or the Commander of the Border Guard unit shall order their immediate, collective and official destruction;

2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code, or any confidential information related to the profession or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings, the Commander-in-Chief of the Border Guard or the Commander of the Border Guard unit shall pass on those materials to the prosecutor.

16g. In the event referred to in para.16f point 2, the prosecutor, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 16f point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code.

16h. Immediately after the prosecutor files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 16g point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings.

16i. The prosecutor is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 16g point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings apply in that appeal.

16j. Border Guard authorities are obliged to enforce the order of the court to destroy the materials referred to in para. 16h and to carry out the immediate,

[9] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

collective and official destruction of the materials which are prohibited in criminal proceedings. The Border Guard shall immediately inform the prosecutor when the materials referred to in para. 16g have been destroyed',

i) para. 17a is added after para. 17 as follows:
'17a. The district court, the Prosecutor General, the district prosecutor and the Border Guard shall keep registers of the rulings, written statements of consent, requests and orders related to operational controls. Registers shall be kept in electronic format, in compliance with legislation on the protection of confidential information.'

j) para. 19 is replaced by:
'19. The ruling of the court referred to in:
1) para. 1, 4, 9 and 10- may be appealed against by the Border Guard authority that filed a request for that ruling;
2) para. 4 and 16c- may be appealed against by the relevant prosecutor, as referred to in para. 1.

The provisions of the Code of Criminal Proceedings shall apply accordingly in the appeal.';

2) art. 10b is replaced by:
'Art. 10b. 1. In order to prevent and detect crimes, the Border Control can obtain any other related data that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:
1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[10]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data'
3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.

2. The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge. It shall be disclosed:

1) to the officer indicated in the request from the Commander-in-Chief of the Border Guard or the Commander of the Border Guard unit or any other person duly authorised by them;
2) upon oral request from the officer holding a written authorisation from the persons referred to in point 1;
3) through the telecommunications network, to the officer holding a written authorisation from the persons referred to in point 1.

3. In the event described in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of the telecommunications company, the postal operator or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists

[10] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.

in the agreement made between the Commander-in-Chief of the Border Guard and that entity.

4. The disclosure of the information to the Border Guard, as referred to in para. 1, can take place through a telecommunications network, if:

1) the telecommunications networks used ensure that:
   a) the person who obtained the information, the type of information and the time in which the information was obtained can be determined,
   b) technical and organisational safeguards are in place to restrict access to unauthorised persons;

2) it is justified due to the specific character or scope of the tasks carried out by the organisational units of the Border Guard or of the actions taken by them.

5. The Commander-in-Chief of the Border Guard and the Commander of the Border Guard units shall keep registers of requests to obtain telecommunications, postal or internet data, containing information identifying the organisational unit of the Border Guard and the officer who obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers are kept in electronic format, in compliance with legislation on the protection of confidential information.

6. The data referred to in para. 1 which is relevant for criminal proceedings shall be passed on by the Commander-in-Chief of the Border Guard or the Commander of the Border Guard unit to the relevant prosecutor with territorial or material jurisdiction. The prosecutor shall decide on the scope and method of use of the data.

7. The data referred to in para. 1 that is not relevant for criminal proceedings should be immediately, collectively and officially destroyed.'

3) art. 10ba and art. 10bb are added after art. 10b as follows:

'Art. 10ba. 1. Controls on Border Guard when extracting telecommunications, postal or internet data are carried out by the district court with jurisdiction over the Border Guard authority that gained access to the data.

2. The Border Guard referred to in para. 1 shall pass on a report to the district court referred to in para. 1, on a six-monthly basis in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data that was obtained;
2) the legal classification of the acts for which the telecommunications, postal and internet data was requested.

3. Within the framework of the controls referred to in para. 1, the district court can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the Border Guard.

4. The district court shall inform the Border Guard of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of 10bb para. 1, is not subject to the controls referred to in para. 1.

Art. 10bb. 1. In order to prevent or detect crimes, the Boarder Guard can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place,

the company or name and the organisational structure of that user can be extracted,

4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 10b para. 2-7 apply when granting access to and processing the data referred to in para. 1.'.

Art. 3. In the Act of 28 September 1991 on Fiscal Controls (Journal of Laws 2015, item 553 as amended[11]) is amended as follows:

1) in art. 36b:

a) para. 1 is replaced by:

'1. In order to prevent or detect fraud or the crimes referred to in art. 2 para. 1 point 14b and art. 36c para. 1 point 3, fiscal intelligence services can obtain any other related data that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[12]), hereinafter 'telecommunications data',

2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data'

3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.'

b) the introduction to the enumeration in para. 2 is replaced by:

'The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge:'

c) para. 3 is replaced by:

'3. In the event outlined in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of the telecommunications company, the postal operator or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists in the agreement made between the Inspector General of Fiscal Control and that entity.',

d) para. 4 and 5 are repealed.

e) the introduction to the enumeration in para. 6 is be replaced by:

[11] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 788, 1269, 1357, 1649 and 2281.

[12] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.

‘The disclosure of the information to the fiscal intelligence services, as referred to in para. 1, can take place through a telecommunications network, if:’,

f) para. 7 is replaced by:
‘7. The disclosure of information referred to in para. 1 shall take place at the expense of the telecommunications company, postal operator or supplier of services provided by electronic means.’,

g) para. 8 is added as follows:
8. ‘ The Inspector General of Fiscal Control shall keep registers of requests to obtain telecommunications, postal or internet data, containing information identifying the organisational unit of the fiscal intelligence services and the employee that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers are kept in electronic format, in compliance with legislation on the protection of confidential information.’,

2) art. 36ba and art. 36bb are added after art. 36b as follows:
‘Art. 36ba. 1. Controls on the fiscal intelligence services when obtaining telecommunications, postal or internet data are carried out by the Warsaw District Court, hereinafter the ‘Court’.
2. The Inspector General of Fiscal Control shall send a report to the Court covering the following:
1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data obtained;
2) the legal classification of the acts for which the telecommunications, postal or internet data was requested or any information concerning data that was obtained to safeguard human lives or health or to support the search and rescue missions.
3. Within the framework of the controls referred to in para. 1, the Court can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the fiscal intelligence services.
4. The Court shall inform the Inspector General of Fiscal Control of the results of the controls within 30 days of their completion.
5. The data obtained on the basis of 36bb para. 1, is not subject to the controls referred to in para. 1

Art. 36bb. 1. In order to prevent or detect fraud or the crimes referred to in art. 2 para. 1 point 14b and art. 36c para. 1 point 3, the fiscal intelligence services can extract the following data:
1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 36b para. 2, 3, 6 and 7 apply when granting access to and processing the data referred to in para. 1.’;

3) in art. 36c:

a) para. 1:
- point 5 is replaced by:

'5) prosecuted under international agreements ratified with prior consent granted by the Act and set out under Polish criminal law',

- The common part. is replaced by:

'- if other resources are ineffective or unhelpful, the Court, upon written request of the Inspector General of Fiscal Control, made after receiving the written request of the Prosecutor General, may, by way of a ruling, order an operational control.',

b) para. 4 is replaced by:

'4. The operational controls are performed confidentially and consist of:
1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;
2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
5) gaining access to and checking the contents of mail.',

c) para. 7 is replaced by:

'In justified cases, when new circumstances, relevant for preventing or detecting crime or fraud or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the Court, upon written request from the Inspector General of Fiscal Control made after receiving written consent from the Prosecutor General may, also after the date of expiry of the periods referred to in para. 6, issue further rulings on prolonging operational controls for consecutive periods whose total duration cannot exceed 12 months.',

d) para. 7a is added after para. 7 as follows:

'7a. The Inspector General of Fiscal Control can authorise the head of the organisational unit referred in to art. 36d para. 4 point 1, to submit any request referred to in para. 1, 6 or 7 or to order an operational control to take place as described in para. 2.'

e) para. 10 is replaced by:

'10. The telecommunications company, postal operator and supplier of services provided by electronic means is obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by fiscal intelligence services.',

f) para. 10a is added after para. 10 as follows:

'10a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[13]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by the fiscal intelligence services as appropriate for their infrastructure.',

g) para. 13a is added after para. 13 as follows:

' 13a. The Court, the Prosecutor General and the Inspector General of Fiscal Control shall keep registers of the rulings, written statements of consent, requests and orders related to operational controls. The registers shall be kept in

[13] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

electronic format, in compliance with the provisions on the protection of confidential information.',

h) para. 14 is replaced by:

'14. The ruling of the Court referred to in:

1) para. 1, 2, 6 and 7- may be appealed against by the Inspector General of Fiscal Control that filed a request for that ruling;
2) para. 2 art. 36d para. 1c- may be appealed against by the Prosecutor General.

The provisions of the Code of Criminal Proceedings shall apply accordingly in the appeal.',

4) in art. 36d:

a) the introduction to the enumeration in para. 1 is replaced by:
'Any data referred to in art. 36b para. 1 obtained when carrying out fiscal intelligence actions as well as any materials, including materials collected during the operational controls or when secretly monitoring the manufacture, transportation, preservation or sale of objects arising from a crime, which:',

b) para. 1f-1i are added after para. 1e as follows:
'1f. In the event that the materials obtained during the operational controls:

1) contain the information referred to in art. 178 of the Code of Criminal Proceedings, the Inspector General of Fiscal Control shall order their immediate, collective and official destruction;
2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code, or any confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings, the Inspector General of Fiscal Control shall pass on those materials to the Prosecutor General.

1g. In the event referred to para.1f point 2, the Prosecutor General, upon receiving the materials, shall immediately submit them to the Court, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 1f point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code.

1h. Immediately after the prosecutor files the request, the Court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 1g point 2 in criminal proceedings or proceedings for fraud, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings or proceedings for fraud.

1i. The Prosecutor General is entitled to appeal against the ruling of the Court on whether to authorise the use of the materials referred to in para. 1g point 2 in criminal proceedings or proceedings for fraud. The provisions of the Code of Criminal Proceedings apply in that appeal.',

c) art. 3 is replaced by:
'3. The materials obtained in the actions carried out on the basis of art. 36aa para. 1, art. 36b para. 1, art. 36c para. 1 and 2 or art. 36ca para. 1, which do not contain evidence allowing for the opening of criminal proceedings or proceedings for fraud, as well as any materials obtained as a result of the operational controls referred to in para. 1h, whose destruction was ordered by the Court, shall be immediately, collectively and officially destroyed.',

d) para. 5 is replaced by:
'5. The Inspector General of Fiscal Control shall immediately inform the Prosecutor General if an order is given out or enforced in relation to the destruction of the materials referred to in para. 3, collected on the basis of art. 36b. para. 1, art. 36c para. 1 and 2 and art. 36ca para. 1, as well as any materials obtained as a result of the operational controls referred to in para. 1h whose destruction was ordered by the Court.'

Art. 4. Art. 6a is added after art. 6 of the Act of 21 August 1997 on the Military Court System (Journal of Laws 2015, item 1198 and 1890) as follows:

'Art. 6a. The presidents of the district court-martials with jurisdiction over the authority requesting the disclosure of information shall, on a yearly basis, pass on any information concerning the processing of telecommunications, postal or internet data to the Ministry of Justice, broken down by the amount and type of data disclosed, as well as the results of any operational controls carried out by 31 March of the year following the one in which they were carried out and the reasons for carrying out the tasks referred to in art. 175b § 2 of the Act of 27 July 2001 on the Common Court System (Journal of Laws 2015, item 133 as amended[14]).'.

Art. 5. The act of 27 July 2001 on the Common Court System (Journal of Laws 2015, item 133 as amended[15]) is amended as follows:

1) in art. 16 § 4a point 2, a full stop is replaced by a semicolon and point 3 is added as follows:
'3) for the control of telecommunications, postal and internet data- for matters relating to controls on Police, the National Security Agency, the Border Guard, the Central Anticorruption Bureau, the Customs Office and the fiscal intelligence services when obtaining telecommunications, postal and internet data.',

2) The title of division IVa should read as follows:
'Processing of personal, telecommunications, postal and internet data';

3) art. 175b is added after art. 175a as follows:
'Art. 175b. § 1. The presidents of the district courts with jurisdiction over the authority requesting the disclosure of information shall, on a yearly basis, pass on any information concerning the processing of telecommunications, postal or internet data to the Ministry of Justice, broken down by the number of cases in which data was disclosed for a particular type of data, as well as the results of any operational controls carried out by 31 March of the year following the one in which they were carried out.

[14] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 509, 694, 1066, 1224, 1309, 1311, 1418, 1595 and 1781 and in the Journal of Laws 2016 as item 147.
[15] Amendments to the consolidated text of the Act were published in the Journal of Laws as items 509, 694, 1066, 1224, 1309, 1311, 1418, 1595 and 1781.

§2. The Ministry of Justice shall present any aggregate information concerning the processing of telecommunications, postal and internet data to the Chamber of Deputies and the Senate on a yearly basis as well as the results of any controls carried out by 30 June of the year following the one in which they were carried out.'.

Art. 6. The Act of 24 August 2001 on the Military Police and Military Law Enforcement Units (Journal of Laws 2016, item 96) is amended as follows:

1) Art. 30 is replaced by

'Art. 30. 1. In order to prevent and detect crimes, including fraud committed by the persons referred to in art. 3 para. 2 point 1, 3, 4, 5 and 6, safeguard human lives or health or support any search and rescue missions, the Military Police can obtain any other related data that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[16]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data'
3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.

2. The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge. It shall be disclosed as follows:

1) To the Military Police officer indicated in the request from the Commander-in-Chief of the Military Police or the commander of the Military Police unit or any other person duly authorised by them;
2) upon oral request from the Military Police officer holding a written authorisation from the persons referred to in point 1;
3) through the telecommunications network, to the Military Police officer holding a written authorisation from the persons referred to in point 1.

3. In the event outlined in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of the telecommunications company, the postal operator or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists in the agreement made between the Commander-in-Chief of the Military Police and that entity.

4. Disclosure of the information referred to in para. 1, to the Military Police can take place through a telecommunications network, if:

1) the telecommunications networks used ensure that:
   a) the person who obtained the information, the type of information obtained and the time in which the information was obtained can be determined.
   b) technical and organisational safeguards are in place to restrict access to unauthorised persons;

[16] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.

2) it is justified due to the specific character or scope of the tasks carried out by the organisational units of the Military Police or of the actions undertaken by them.

5. The Commander-in-Chief of the Military Police and the Commander of the Military Police unit shall keep registers of requests to obtain telecommunications, postal or internet data, containing information identifying the Military Police organisational unit and the Military Police that obtained that data, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with the legislation on the protection of confidential information.

6. The information referred to in para. 1 which is relevant for criminal proceedings shall be passed on by the Commander-in-Chief of the Military Police or the Commander of Military Police unit to the relevant prosecutor with territorial or material jurisdiction. The prosecutor shall decide on the on the scope and method of use of the data. .

7. The information referred to in para. 1 that is not relevant for criminal proceedings should be immediately, collectively and officially destroyed.',

2) art.30b and 30c are added after art.30a as follows:

'Art. 30b. 1. Controls on the Military Police when obtaining telecommunications, postal or internet data are carried out by the district court-martial with jurisdiction over the Military Police authority that gained access to the data.

2. The Military Police authority referred to in para. 1 shall send a report to the district court referred to in para. 1, on a six monthly, in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data obtained;
2) the legal classification of the acts for which the telecommunications, postal and internet data was requested or any information concerning data that was obtained to safeguard human lives or health or to support the search and rescue missions.

3. Within the framework of the controls referred to in para. 1, the district court-martial can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the Military Police.

4. The district court-martial shall inform the Military Police authority of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of para. 1, is not subject to the controls referred to in art. 30c para. 1.

Art. 30cb. 1. In order to prevent or detect crimes, including fraud, committed by the persons referred to in art. 3 para. 2 points 1 , 3, 4 , 5 and 6,to safeguard human lives or health or to support search and rescue missions, Military Police can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 30 para. 2-7 apply when granting access to and processing the data referred to in para. 1.';

3) in art. 31:

a) para. 1 is replaced by;

'1. In preliminary investigations carried out by Military Police within the bounds of the tasks outlined in art. 4 para.1 and in relation to the people referred to in art. 3 para. 2 points 1, 3, 5 and 6 to obtain and record evidence and to prevent, detect and determine perpetrators prosecuted on public indictment for any intentional crimes:

1) against peace and humanity
2) against the Republic of Poland, excluding the crimes outlined in art. 127-132 of the Penal Code,
3) against human life, as outlined in art. 48-150 of the Penal Code,
4) outlined in art. 140, art. 156 § 1 and 3, art. 163 § 1 and 3, art. 164 § 1, art. 165 § 1 and 3, art. 166, art. 167, art. 171 § 1, art. 173 § 1 and 3, art. 189, art. 189a, art. 200, art. 200a, art. 202 § 3 and 4, art. 211a, art. 223, art. 228 § 1 and 3–5, art. 229 § 1 and 3–5, art. 230 § 1, art. 230a § 1, art. 231 § 1 and 2, art. 232, art. 245, art. 246, art. 252 § 1–3, art. 258, art. 263 § 1 and 2, art. 265, art. 269, art. 280–282, art. 285 § 1, art. 286 § 1 and 2, art. 299 § 1–6, art. 305, art. 310 § 1, 2 and 4, art. 339 § 2, art. 345 § 2 and 3 and art. 358 § 2 of the Penal Code,
5) related to fraud, if the value of the object of the offence or the decrease in public law liabilities exceeds fifty times the minimum average of remuneration for the work outlined on the basis of specific legislation,
6) outlined in art. 8 of the Act of 6 June 1997 on the implementation of the Penal Code (Journal of Laws no. 88, item 554 as amended[17]),
7) outlined in art. 43 and art. 44 of the Act of 1 July 2005 on the procurement, preservation and transplantation of cells, tissue and organs (Journal of Laws 2015, item 793, 1893 and 1991),
8) outlined in art. 53 para. 1, art. 55 para. 1, art. 56 para. 1, art. 58 para. 1, art. 59 para. 1 and art. 62 para. 1 of the Act of 29 July 2005 on counteracting drug addiction (Journal of Laws 2012, item 124 as amended[18]),
9) prosecuted under international agreements ratified with prior consent granted by the Act and set out in Polish criminal law

- if other resources are ineffective or unhelpful, the district court-martial, upon written request of the Commander-in-Chief of the Military Police, made after receiving the written consent of the Prosecutor General or upon written request from the Commander of the Military Police unit, made after receiving the consent of the Commander-in-Chief of the Military Police and the written consent of the competent district military prosecutor, may, by way of ruling, order an operational control.',

b) para. 7 shall be replaced by:

'7. The operational controls are performed confidentially and consist of:

1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;

[17] Amendments to the Act were published in the Journal of Laws 1997 no. 160 as item 1083, in the Journal of Laws 1998 no. 113 as item 715, in the Journal of Laws 2009 no. 141 as item 1149 and no. 206 as item 1589 and in the Journal of Laws 2010 no. 98 as item 626.

[18] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 28, 875, 1893, 1916 and 2014.

2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
5) gaining access to and checking the contents of mail.',

c) para. 10 is replaced by:
'10. In justified cases, when new circumstances, relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the district court-martial with territorial jurisdiction over the requesting Military Police authority, upon written request from the Commander-in-Chief of the Military Police or the Commander of the Military Police unit made after receiving written consent from the Commander-in-Chief of the Military Police and the competent military prosecutor may, also after the date of expiry of the periods referred to in para. 9,issue further rulings on prolonging operational controls for consecutive periods whose total duration cannot exceed 12 months.',

d) para. 10a is added after para. 10 as follows:
'10a. the Commander-in-Chief of the Military Police or Commander of the Military Police unit can authorise their deputy to make the requests referred to in para. 1, 4 point 1, para. 9 and 10 or to order the operational controls in accordance with para. 4 point 1.',

e) para. 13 is replaced by:
'13. Telecommunications companies, postal operators and suppliers of services provided by electronic means are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by Military Police.',

f) 13a is added after para. 13 as follows:
'13a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[19]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by Military Police as appropriate their infrastructure.',

g) para.16f-15j are added after para. 16e as follows:
'16f. In the event that the materials referred to in para. 16:
1) contain information referred to in art. 178 of the Code of Criminal Proceedings, the Commander-in-Chief of the Military Police or the Commander of the Military Police unit shall order their immediate, collective and official destruction;
2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about crimes referred to in art. 240 § 1 of the Penal Code, or any confidential information related to the profession or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings, the Commander-in-Chief of the Military Police or the

[19] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

Commander of the Military Police unit shall pass on those materials to the prosecutor.

16g. In the event referred to in para.16f point 2, the military prosecutor, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 15f point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code.

16h. Immediately after the prosecutor files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 16g point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings.

16i. The prosecutor is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 16g point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings apply in that appeal.

16j. Military Police authorities are obliged to enforce the order of the court to destroy the materials referred to in para. 16h and to carry out the immediate, collective and official destruction of the materials which are prohibited in criminal proceedings. The Military Police authorities shall immediately inform the prosecutor when the materials referred to in para. 16g have been destroyed.',

h) para. 17a is added after para. 17 as follows:

'17a. The district court-martial, the Prosecutor General, the district military prosecutor and the Military Police authorities shall keep registers of the ruling, written statements of consent, requests and orders related to operational controls as well as a central register of operational controls. The registers are kept in electronic format, in compliance with the legislation on the protection of confidential information.',

i) para. 19 is replaced by:

'19. The ruling of the court referred to in:

1) para. 1, 4, 9 and 10- may be appealed against by the Military Police authority that filed a request for that ruling;
2) para. 4 and 16c- may be appealed against by the relevant prosecutor, as referred to in para. 1.

The provisions of the Code of Criminal Proceedings shall apply accordingly in the appeal.',

Art. 7. The Act of 24 May 2002 on the National Security Agency and the Intelligence Agency (Journal of Laws 2015, item 1929 and 2023) is amended as follows:

1) art. 19 para. 2 is replaced by:
‘2. The agency heads can authorise their subordinate officials to take care of matters on their behalf within a specified scope, excluding the matters referred to in art. 29- 31 and art. 27, with the exception of the Deputy Head of the National Security Agency within the scope specified in art. 27 para. 9a.’;

2) In art. 27:
a) para. 1 is replaced by:
‘1. The court, upon written request from the Head of the National Security Agency, made after receiving the written consent of the Prosecutor General, may, by way of a ruling, order an operational control- if other resources are ineffective or unhelpful- in the preliminary investigations carried out by the National Security Agency in order to determine, prevent and detect the crimes referred to in:
1) art. 5 para. 1 point 2 letters a, c, d, e,
2) chapters XXXXV-XXXVII of the Penal Code and chapters 6 and 7 of the Fiscal Penal Code, if they undermine the state economically.

- and to obtain and record criminal and prosecute the perpetrators.’,

b) para. 6 is replaced by:
‘6. The operational controls are performed confidentially and consist of:
6) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;
7) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
8) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
9) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
10) gaining access to and checking the contents of mail.’,

c) para. 9 is replaced by:
’9. In justified cases, when new circumstances, relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the court referred to in para. 2, upon written request from the Head of the National Security Agency, made after receiving written consent from the Prosecutor General may, also after the date of expiry of the periods referred to in para. 8, issue further rulings on prolonging operational controls for consecutive periods whose total duration cannot exceed 12 months.’,

d) para. 9a is added after para. 9 as follows:
‘9a. The Head of the National Security Agency can authorise their deputy to make the requests referred to in para. 1, 3, 8 and 9 or to order an operational control in accordance with para. 3.’,

e) para. 11a is replaced by:
‘11a. The ruling of the court referred to in:
1) para. 1, 3, 8 and 9- may be appealed against by the Head of the National Security Agency;
2) para. 3 and 15c- may be appealed against by Prosecutor General.

The provisions of the Code of Criminal Proceedings shall apply accordingly in the appeal.’,

f) para. 12 is replaced by:

'12. Telecommunications companies, postal operators and suppliers of services provided by electronic means are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by National Security Agency.',

g) para. 12a is added after para. 12 as follows:

'12a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[20]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by the National Security Agency as appropriate for their infrastructure.',

h) 15h-15l are added after 15g as follows:

'15h. In the event that the materials referred to in para. 15:

1) contain information referred to in art. 178 of the Code of Criminal Proceedings, the Head of the National Security Agency shall order their immediate, collective and official destruction;
2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code, or any confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings, the Head of the National Security Agency shall pass on those materials to the prosecutor.

15i. In the event referred to in para.15h point 2, the Prosecutor General, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 15h point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code.

15j. Immediately after the Prosecutor General files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 15i point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings.

15k. The Prosecutor General is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 15i point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings apply in that appeal.

15l. The Head of the National Security Agency is obliged to enforce the order of the court to destroy the materials referred to in para. 15j and to carry out the

[20] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

immediate, collective and official destruction of the materials which are prohibited in criminal proceedings. The Head of the National Security Agency shall immediately inform the Prosecutor General when the materials have been destroyed.',

i) para. 16b-16d are added after para. 16a as follows:

'16b. The court, the Prosecutor General and the and the Head of the National Security Agency shall keep registers of the rulings, written statements of consent, requests and orders related to operational controls.

16c. The Head of the National Security Agency shall keep separate registers of requests made to the Court to retain materials collected during the operational controls which are relevant to national security, of orders to destroy materials collected during the operation controls and of notifications made by the Prosecutor General regarding any orders on the destruction of materials collected during the operational controls issued by the Head of the National Security Agency and later enforced.

16d. The registers referred to in art. 16b and16c, shall be kept in electronic format, in compliance with the provisions on the protection of confidential information.',

3) in art. 28:

a) para. 1 is replaced by:

'1. The National Security Agency can obtain any other related data that is necessary for carrying out their duties but that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[21]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data'
3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.

b) The introduction to the enumeration in art. 2 is replaced by:
'The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge. It shall be disclosed:,'

c) para. 3 is replaced by:

'3. In the event described in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of employees of the telecommunications company, the postal operator or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists in the agreement made between the Head of the National Security Agency and that entity.',

d) para. 5-7 are added as follows:

'5. The Head of the National Security Agency shall keep a register of requests to obtain telecommunications, postal or internet data, containing information identifying the organisational unit of the National Security Agency and the

[21] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.

National Security Agency official that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with legislation on the protection of confidential information.

6. The data referred to in para. 1 which is relevant for criminal proceedings shall be passed on to the Prosecutor General by the Head of the National Security. The Prosecutor General shall make a decision on the scope and method of use of the data.',

7. The data referred to in para. 1 which is not relevant for criminal proceedings or for national security, shall be immediately, collectively and officially destroyed.',

4) art. 28a and 28b are added after art. 28 as follows:

'Art. 28a. 1. Controls on the National Security Agency when obtaining telecommunications, postal or internet data are carried out by the Warsaw District Court.

2. The Head of the National Security Agency referred to in para. 1 shall send a report to the court referred to in para. 1, on a six-monthly basis, in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data obtained;
2) the legal classification of the acts for which the telecommunications, postal and internet data was requested.

3. Within the framework of the controls referred to in para. 1, the court can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the National Security Agency.

4. The court, referred to in para. 4, shall inform the Head of the National Security Agency of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of 28cb para. 1, is not subject to the controls referred to in para. 1.

Art. 28b. 1. In order to carry out the duties referred to in art. 5 para. 1, the National Security Agency can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 28 para. 2-7 apply when granting access to and processing the data referred to in para. 1.';

Art. 8. Art. 18. para. 6 of the Act of 18 July 2002 on the provision of services by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844) is replaced by:

'6. The service provider shall disclose the information referred to in para. 1-5, to the competent national authorities free of charge, under specific legislation, for the purposes of the proceedings.',

Art. 9. The Telecommunications Act of 16 July 2004 (Journal of Laws 2015, item 243 as amended[22]) is amended as follows:

1) In art. 179, 4d is added after 4c as follows:
'4d. Telecommunications companies that are micro or small enterprises, as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity, subject to para. 4c, are not required to provide the technical conditions to ensure access to and record data through an interface.',
2) art. 180g. is repealed
3) in art. 209, point 28 is repealed from para. 1

Art. 10. The Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws 2014, item 253 as amended[23]) is amended as follows:

1) art. 20 para. 2 is replaced by:
'2. The Heads of the Military Counterintelligence Service and the Military Intelligence Service can authorise their subordinate professional soldiers or officers to take care of matters on their behalf within a specified scope, on the understanding that the Head of the Military Counterintelligence Service cannot authorise others to take care of the matters referred to in art. 29 para.3, art.33 and para.1 and art. 34 para. 1 and art. 31, with the exception of the Deputy Head of the Military Counterintelligence Service within the scope specified in art. 31 para. 7a.',

2) in art. 31:
a) para.1 is replaced by:
'1. In the preliminary investigations undertaken by the Military Counterintelligence Service in order to carry out the tasks outlined in art. 5 para. 1 point 1, 5, 7 and 8 and in para. 2, if other resources are ineffective or unhelpful, the court, upon written request from the Head of the Military Counterintelligence Service, made after receiving the written consent of the Prosecutor General, may issue a ruling ordering an operational control.',

b) para. 4 is replaced by:
'4. The operational controls are performed confidentially and consist of:
1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;
2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;

[22] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281.
[23] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 502 and 1055 and in the Journal of Laws 2015 as items 1066 and 1224.

4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
5) gaining access to and checking the contents of mail.',

c) para. 7 is replaced by:
'7. In justified cases, when new circumstances, relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the court referred to in para. 2, upon written request from the Head of the Military Counterintelligence Service made after receiving written consent from the Prosecutor General may, also after the date of expiry of the periods referred to in para. 6, issue further rulings on prolonging operational controls for consecutive periods whose total duration cannot exceed 12 months.',

d) para. 7a is added after para. 7 as follows:
'7a. The Head of the Military Counterintelligence Service can authorise their deputy to make the requests referred to in para. 1, 3, 6 and 7 or to order the operational controls in accordance with para. 3.',

e) para. 10 is replaced by:
'10. The ruling of the court referred to in:
1) para. 1, 3, 6 and 7- may be appealed against by the Head of the Military Counterintelligence Service;
2) para. 3 and 14c- may be appealed against by the Prosecutor General.

The provisions of Code of Criminal Proceedings of 6 June 1995 shall apply accordingly in the appeal.',

f) para. 11 is replaced by:
'11. Telecommunications companies, postal operators and suppliers of services provided by electronic means are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Military Counterintelligence Service.',

g) para. 11a is added after para. 11 as follows:
'11a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[24]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Military Counterintelligence Service as appropriate their infrastructure.',

h) 14f-14j are added after para. 14e as follows:
'14f. In the event that the materials referred to in para. 14:
1) contain information referred to in art. 178 of the Code of Criminal Proceedings, the Head of the Military Counterintelligence Service shall order their immediate, collective and official destruction;
2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings of 6 June 1997, excluding information about the crimes referred to in art. 240 § 1 of Penal Code of 6 June 1997, or any confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings of 6 June 1997, the Military

[24] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

Counterintelligence Service shall pass on those materials to the Prosecutor General.

14g. In the event referred to in para.14f point 2, the Prosecutor General, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 14f point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings of 6 June 1997 and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings of 6 June 1997, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code of 6 June 1997.

14h. Immediately after the Prosecutor General files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 14g point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials which are prohibited in criminal proceedings.

14i. The Prosecutor General is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 14g point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings of 6 June 1997 apply in that appeal.

14j. The Head of the Military Counterintelligence Service is obliged to enforce the order of the court to destroy the materials referred to in para. 14h and to carry out the immediate, collective and official destruction of the materials which are prohibited in criminal proceedings. The Head of the Military Counterintelligence Service shall immediately inform the Prosecutor General when the materials have been destroyed.',

i) para. 15b is added after para. 15 as follows:

'15b. The court, the Prosecutor General and the Head of the Military Counterintelligence Service shall keep registers of the rulings, written statements of consent, requests and orders related to operational controls in electronic format and in compliance with the legislation on the protection of confidential information.'.

3) in art. 32

a) para. 1 is replaced by;

'1. The Military Counterintelligence Service can obtain any other related data that is necessary for carrying out their duties but that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[25]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015 item 1830), hereinafter 'postal data'

[25] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198 and in the Journal of Laws 2015 as items 1069, 1893 and 2281 and in the Journal of Laws 2016 as item 147.

3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.',

b) The introduction to the enumeration in art. 2 is replaced by:
'The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge.',

c) para. 3-5 is replaced by:
'3. The telecommunications company, postal operator or provider of electronic services shall immediately inform the Head of the Military Counterintelligence Service when information is disclosed in accordance with para. 2 point 2.
4. The telecommunications company, postal operator and provider of electronic services are obliged to disclose the information outlined in para. 1 to the officers indicated in the request.
5. In the event described in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of the telecommunications company, the postal operator or the supplier of electronic services or with their involvement if necessary and if such a possibility exists in the agreement made between the Head of the Military Counterintelligence Service and that entity.',

d) the introduction to the enumeration in para. 6 is replaced by:
'Disclosure of the information referred to in para. 1, to the Military Counterintelligence Service can take place through a telecommunications network, if:',

e) para. 7-9 are added as follows:
'7. The Head of the Military Counterintelligence Service shall keep a register of requests to obtain telecommunications, postal or internet data, containing information identifying the organisational unit and official from the Military Counterintelligence Service that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with the legislation on the protection of confidential information.
8. The data referred to in para. 1 which is relevant for criminal proceedings shall be passed on by the Head of the Military Counterintelligence Service to the Prosecutor General. The Prosecutor General shall decide on the scope and method of use of the data.
9. The data referred to in para. 1 which is not relevant for criminal proceedings should be immediately, collectively and officially destroyed.'

4) Art. 32a and 32b are added after art.32 as follows:
'Art. 32a. 1. Controls on the Military Counterintelligence Service when obtaining telecommunications, postal or internet data are carried out by the Warsaw District Court.
2. The Head of the Military Counterintelligence Service shall send a report to the court referred to in para. 1, on a six-monthly basis, in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data obtained;
2) the legal classification of the acts for which the telecommunications, postal or internet data was requested.

3. Within the framework of the controls referred to in para. 1, the court can familiarise itself with the materials that justify the disclosure of telecommunications, postal or internet data to the Military Counterintelligence Service.
4. The court referred to in para. 1 shall inform the Head of the Military Counterintelligence Service of the results of the controls within 30 days of their completion.
5. The data obtained on the basis of 32b para. 1, is not subject to the controls referred to in para.1.

Art. 32b. 1. In order to carry out the duties referred to in art. 5, the Military Counterintelligence Service can extract the following data:
1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 32 para. 2-9 apply when granting access to and processing the data referred to in para. 1.';

Art. 11. The Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws 2014, item 1411 as amended[26]) is amended as follows:
1) art. 10 para. 2 is amended as follows:
'2. The Head of the Central Anti-Corruption Bureau can authorise their subordinate officials to take care of matters on their behalf within a specified scope, excluding the matters referred to in art. 19, art. 23 and art. 17, with the exception of the deputy Head of the Central Anti-Corruption Bureau within the scope specified in art. 17 para. 9a.',
2) in art. 17:
a) art. 1 point 1 is replaced by:
'1) outlined in art. 228-231, art. 250a, art. 258, art.286, art.296-297, art.299, art.305, art.310 § 1, 2 and 4 of the Penal Code of 6 June 1997,',

b) art. 5 is replaced by:
'5. The operational controls are performed confidentially and consist of:
1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks;

[26] Amendments to the consolidated text were published in the Journal of Laws 2014 as item 1822 and in the Journal of Laws 2015 as items 1066, 1217, 1224, 1268 and 2023.

2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places;
3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication;
4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems;
5) gaining access to and checking the contents of mail.',

c) para. 9 is replaced by
'9. In justified cases, when new circumstances, relevant for preventing or detecting crime or for determining perpetrators and obtaining criminal evidence, arise during the operational controls, the court referred to in para. 2, upon written request from the Head of the Central Anti-Corruption Bureau made after receiving written consent from the Prosecutor General may, also after the date of expiry of the periods referred to in para. 8, issue further rulings on prolonging operational controls for consecutive periods whose total duration cannot exceed 12 months.',

d) para. 9a is added after 9 as follows:
'9a. The Head of the Central Anti-Corruption Bureau can authorise their deputy to make the requests referred to in para. 1, 3, 8 and 9 or to order the operational controls in accordance with para. 3.',

e) para. 12 is replaced by:
'12. Telecommunications companies, postal operators and suppliers of electronic services are obliged to ensure, at their own expense, that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Central Anti-Corruption Bureau.',

f) para. 12a is added after para. 12 as follows:
'12a. Suppliers of services provided by electronic means that are either micro or small enterprises as set out in the provisions of the Act of 2 June 2004 on freedom of economic activity (Journal of Laws 2015, item 584 as amended[27]) shall ensure that the technical and organisational conditions are in place to facilitate the operational controls carried out by the Central Anti-Corruption Bureau as appropriate for their infrastructure.',

g) 15f-15j are added after para. 15e as follows:
'15f. In the event that the materials referred to in para. 15:
1) contain information referred to in art. 178 of Code of Criminal Proceedings of 6 June 1997, the Head of the Central Anti-Corruption Bureau shall order their immediate, collective and official destruction;
2) may contain any of the information referred to in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings of 6 June 1997, excluding information about the crimes referred to in art. 240 § 1 of the Penal Code of 6 June 1997, or any confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings of 6 June 1997, the Head of the Central Anti-Corruption Bureau shall pass on those materials to the Prosecutor General.

[27] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 699, 875, 978, 1197, 1268, 1272, 1618, 1649, 1688, 1712, 1844 and 1893 and in the Journal of Laws 2016 as item 65.

15g. In the event referred to in para.15f point 2, the Prosecutor General, upon receiving the materials, shall immediately submit them to the court which ordered the operational controls or gave its consent for them as indicated in para. 3, together with a request for:

1) a statement indicating which of the materials submitted contain the information referred to in para. 15f point 2;
2) a statement authorising the use of any materials, in criminal proceedings, containing confidential information related to the professions or duties referred to in art. 180 § 2 of the Code of Criminal Proceedings of 6 June 1997 and which are not subject to the prohibitions laid down in art. 178a and art. 180 § 3 of the Code of Criminal Proceedings of 6 June 1997, excluding any information about the crimes referred to in art. 240 § 1 of the Penal Code of 6 June 1997.

15h. Immediately after the Prosecutor General files the request, the court shall issue a ruling on whether to authorise the use of any of the materials referred to in para. 15g point 2 in criminal proceedings, wherever it is in the interest of the justice system, and where the facts cannot be established on the basis of any other evidence. The court shall also order the immediate destruction of the materials whose use is prohibited in criminal proceedings.

15i. The Prosecutor General is entitled to appeal against the ruling of the court on whether to authorise the use of the materials referred to in para. 15g point 2 in criminal proceedings. The provisions of the Code of Criminal Proceedings of June 1997apply in that appeal.

15j. The Head of the Central Anti-Corruption Bureau is obliged to enforce the order of the court to destroy the materials referred to in para. 15h and to carry out the immediate, collective and official destruction of the materials which are prohibited in criminal proceedings. The Head of the Central Anti-Corruption Bureau shall immediately inform the Prosecutor General when the materials have been destroyed.',

h) para. 17 is replaced by:

'17. The ruling of the court referred to in:

1) para. 1, 3, 8 and 9- may be appealed against by the Head of the Central Anti-Corruption Bureau;
2) para. 3 and 15c- may be appealed against by the Prosecutor General.

The provisions of the Code of Criminal Proceedings of 6 June 1997 shall apply accordingly in the appeal.',

i) para. 17a is added after para. 17:

'17a. The court, the Prosecutor General and the Head of the Central Anti-Corruption Bureau shall keep registers of the rulings, written statements of written consent, requests and orders related to operational controls. The registers shall be kept in electronic format, in compliance with legislation on the protection of confidential information.'

3) In art. 18:

a) para. 1 is replaced by:

'1. The Head of the Central Anti-Corruption Bureau can obtain any other related data that is necessary for carrying out the duties referred in art. 2 but that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:

1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[28]), hereinafter 'telecommunications data',
2) art. 82 para. 1 point 1 of the Postal Act of 23 November 2012 (Journal of Laws, item 1529 and Journal of Laws 2015, item 1830), hereinafter 'postal data'
3) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

- and may process it without the knowledge or consent of the person concerned.',

b) the introduction to the enumeration in para. 2 is replaced by:
'The telecommunications company, postal operator or supplier of services provided by electronic means shall disclose the information referred to in para. 1 free of charge:',

c) para. 3 is replaced by:
'3. In the event referred to in para. 2 point 3, the disclosure of information, as referred to in para. 1, shall be carried out without the involvement of the telecommunications company, the postal operator or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists in the agreement made between the of the Central Anti-Corruption Bureau and that entity.',

d) para. 5-7 are added as follows:
'5. The Head of the Central Anti-Corruption Bureau shall keep a register of requests to obtain telecommunications, postal or internet data, containing information identifying the organisational unit and official from the Central Anti-Corruption Bureau that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with the legislation on the protection of confidential information.
6. The data referred to in para. 1 which is not relevant for criminal proceedings shall be passed on to the Prosecutor General by the Head of the Central Anti-Corruption Bureau. The Prosecutor General shall make a decision on the scope and method of use of the data.'
7. The data referred to in para. 1 which is not relevant for criminal proceedings or for national security, shall be immediately, collectively and officially destroyed.',

4) art. 18a and art. 18b are added after 18 as follows:
'Art. 18a. 1. Controls on the Central Anti-Corruption Bureau when obtaining telecommunications, postal or internet data are carried out by the Warsaw District Court.
2. The Head of the Central Anti-Corruption Bureau shall send a report to the court referred to in para. 1, on a six-monthly basis, in compliance with legislation on the protection of confidential information. The report shall cover the following:
1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of information obtained;
2) the legal classification of the acts for which the telecommunications, postal and internet data was requested or any information concerning data that was obtained to safeguard human lives or health or to support the search and rescue missions.

[28] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198, in the Journal of Laws 2015 as items 1069, 1893 and 2281 and in the Journal of Laws 2016 as item 147.

3. Within the framework of the controls referred to in para. 1, the court can familiarise itself with the materials that justify the disclosure of telecommunications, postal and internet data to the Central Anti-Corruption Bureau.

4. The court referred to in para. 1 shall inform the Head of the Central Anti-Corruption Bureau of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of 18b para. 1, is not subject to the controls referred to in para. 1.

Art. 18b. 1. In order carry out the duties referred to in art. 2, the Central Anti-Corruption Bureau can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.',

2. Art. 18 para. 2-7 apply when granting access to and processing the data referred to in para. 1.';

Art. 12. The Act of 27 August 2009 on the Customs Office (Journal of Laws 2015, item 990 as amended[29]) is amended as follows:

1) in art. 75d:
   a) para. 1 is replaced by:
   '1. In order to prevent and detect fraud, as referred to in Chapter 9 of the Fiscal Penal Code, the Customs Office can obtain any other related data that is not included in the contents of telecommunications, mail or any other communications transmitted via an electronically supplied service, as outlined in:
   1) art. 180c and art. 180d of the Telecommunications Act of 16 July 2004 (Journal of Laws 2014, item 243 as amended[30]), hereinafter 'telecommunications data',
   2) art. 18 para. 1-5 of the Act of 18 July 2002 on the provision of services supplied by electronic means (Journal of Laws 2013, item 1422 and Journal of Laws 2015, item 1844), hereinafter 'internet data'

   - and may process it without the knowledge or consent of the person concerned.',

   b) The introduction to the enumeration in para. 2 is replaced by:
   'The telecommunications company or supplier of services provided by electronic means shall disclose the telecommunications or internet information free of charge:',

[29] Amendments to the consolidated text of the Act were published in the Journal of Laws 2015 as items 1045, 1217, 1268, 1269, 1479, 1642, 1830, 1890 and 2023.
[30] Amendments to the consolidated text of the Act were published in the Journal of Laws 2014 as items 827 and 1198, in the Journal of Laws 2015 as items 1069, 1893 and 2281 and in the Journal of Laws 2016 as item 147.

c) para. 3 is replaced by:

‘3. In the event described in para. 2 point 3, the disclosure of telecommunications and internet data shall be carried out without the involvement of the telecommunications company or the supplier of services provided by electronic means or with their involvement if necessary and if such a possibility exists in the agreement made between the Head of the Customs Office and that entity.’,

d) the introduction to the enumeration in para. 4 is replaced by:

‘The disclosure of the information to the Head of the Customs Office, as referred to in para. 1, can take place through a telecommunications network, if:’,

e) para. 5 is replaced by:

‘5. The telecommunications or internet data referred to in para. 1 which is relevant for criminal proceedings or fiscal criminal proceedings shall be passed on by the Head of the Customs Office or the Director of the Customs Chamber to the relevant prosecutor with jurisdiction over that authority. The prosecutor shall decide on the scope and method of use of the data.’

f) para. 6 and 7 are added as follows:

‘6. The telecommunications and internet data referred to in para. 1 which is not relevant for criminal proceedings shall be immediately, collectively and officially destroyed.’

7. The Head of the Customs Office and the Director of the Customs Chamber shall keep registers of requests to obtain telecommunications or internet data, containing information identifying the organisational unit and the official from the Customs Office that obtained that data, the type of data obtained, the reason for obtaining it and the time in which it was obtained. The registers shall be kept in electronic format, in compliance with the legislation on the protection of confidential information.’,

2) art. 75da and art. 75db are added after art. 75d as follows:

‘Art. 75da. 1. Controls on the Customs Office when obtaining telecommunications or internet data are carried out by the district court with jurisdiction over the Customs Office authority that gained access to the data.

2. The Customs Office authority referred to in para. 1 shall send a report to the district court referred to in para. 1, on a six-monthly basis, in compliance with legislation on the protection of confidential information. The report shall cover the following:

1) the number of times that the telecommunications, postal or internet data was obtained in the reporting period and the type of data obtained;
2) the legal classification of the acts for which the telecommunications and internet data was requested.

3. Within the framework of the controls referred to in para. 1, the district court can familiarise itself with the materials that justify the disclosure of telecommunications and internet data to the Customs Office.

4. The court shall inform the Head of the Customs Office of the results of the controls within 30 days of their completion.

5. The data obtained on the basis of 75bd para. 1, is not subject to the controls referred to in para.1.

Art. 75db. 1. In order to prevent or detect fraud as referred to in Chapter 9 of the Fiscal Penal Code, the Customs Office can extract the following data:

1) data from the list referred to in art. 179 para. 9 of the Telecommunications Act of 16 July 2004.
2) data referred to in art. 161 of the Telecommunications Act of 16 July 2004,
3) in the event that a user is not a natural person, the network termination number, the location or place in which the economic activity is taking place, the company or name and the organisational structure of that user can be extracted,
4) in the event there is a fixed public telecommunications network, the name of the town or road where the network ends, as made available to the user, can be extracted.

- and can process the data without the knowledge and consent of the person concerned.

2. Art. 75d para. 2-7 apply when granting access to and processing the data referred to in para. 1.';

Art. 13. Previous legislation shall apply to any operational controls that were carried out before the date on which the present act comes into force and were not completed by that date.

Art. 14. 1. If a request to order an operational control, as referred to in art. 19 para. 19 of the Police Act of the 6 April 1990, art. 9e para. 10 of the Act of 12 October 1990 on the Border Guard, art. 36c para. 7 of the Act of 28 September 1991 on Fiscal Controls and art. 31 para. 10 of the Act of 24 August 2001 on the Military Police and Military Law Enforcement Units, as set out in previous legislation, was filed before the date on which the present act comes into force, the controls shall be ordered in accordance with the provisions of the present Act.

2. If, after the completion of the operational controls, referred to in art. 13, the deadline expires, an operational control can be ordered, on the basis of art.19 para. 9 of the Police Act, art. 9e para. 10 of the Act of 12 October 1990 on the Border Guard, art. 36c para. 7 of Act of 28 September 1991 on Fiscal Controls and art. 31 para. 10 of the Act of 24 September 2001 on the Military Police and Military Law Enforcement Units, as amended by the present Act.

Art. 15. Previous legislation applies to proceedings concerning the disclosure of data, as referred to in art. 180c and art. 180d of the Telecommunications Act of the 16 July 2004. Previous legislation also applies to any data that identifies the entity that is using the postal services, the circumstances surrounding the provision of postal services or the use of any services the provision of which was initiated but not concluded before the date of enforcement of this Act. Previous legislation also applies to any data already collected.

Art. 16. Previous legislation applies to the operational controls carried out on the basis of art. 21 para. 1 of the Act of 24 May 2002 on the National Security Agency and the Intelligence Agency, as previously set out, in order to carry out the tasks outlined in art. 5 para. 1 point 2 letter b of the present Act, which remains unconcluded until the date on which it enters into force.

Art. 17. The Act enters into force on 7 February 2016.

President of the Republic of Poland: *A. Duda*

LAW ON POLICE[31]
of 6 April 1990

(Consolidated Text)Article 15 1.
Policemen, upon performing the actions mentioned in Article 14, are entitled to:
4a) observe and record using technical means the image of the rooms for arrested persons or persons detained until sober, police facilities for kids, transition rooms, and temporary transition rooms;
Article 19 1. (1)
In case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators and to obtain and record evidence of the perpetrators prosecuted on indictment, of intentional crime:
1) against life, as defined in Articles 148-150 of the Criminal Code;
2) defined in Article 134, Article 135(1), Article 136(1), Article 156(1) and (3), Article 163(1) and (3), Article 164(1), Article 165(1) and (3), Article 166, Article 167, Article 173(1) and (3), Article 189, Article 189a, Article 211a, Article 223, Article 228(1) and (3-5), Article 229(1) and (3-5), Article 230(1), Article 230a(1), Article 231(2), Article 232, Article 245, Article 246, Article 252(1-3), Article 258, Article 269, Article 280-282, Article 285(1), Article 286(1), Article 296(1-3), Article 296a(1), (2) and (4), Article 299(1-6) and Article 310(1), (2) and (4) of the Criminal Code;
2a) defined in Article 46(1), (2) and (4), Article 47 and Article 48(1) and (2) of the Act of 25 June 2010 on sports (Polish Journal of Laws Dz.U. of 2014 item 715);
3) against economic turnover defined in Articles 297-306 of the Criminal Code, resulting in property loss or directed against property, if the damage is in excess of the multiple of fifty minimum wages, defined in separate provisions;
3a) against sexual liberty and decency, if the victim is a minor, or if the pornographic content mentioned in Article 202 of the Criminal Code present a minor;
4) fiscal crimes, if the value of the subject of offence or reduction of public private amount due is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions;
4a) fiscal crimes mentioned in Article 107(1) of the Fiscal Criminal Code;
5) illegal manufacture, possession or turnover in arms, ammunition, explosives, intoxicants, psychotropic substances and their precursors, as well as nuclear and radioactive materials;
6) defined in Article 8 of the Act of 6 June 1997 – Provisions implementing the Criminal Code (Polish Journal of Laws No. 88, item 554, as amended),
7) defined in Articles 43-46 of the Act of 1 July 2005 on collection, storage, and transportation of cells, tissues, and organs (Polish Journal of Laws No. 169, item 1411, as amended),
8) (2) prosecuted under international agreements ratified pursuant to a prior consent expressed in a statute, specified in the Polish criminal act;

when other means appeared ineffective or there is significant probability of the means being ineffective or useless, the district court, upon a written request of the Police Commander in Chief, or the Commander of the Central Bureau of Police Investigations submitted after a prior written consent of the general Public Prosecutor or a written request of the Voivodship Police Commander, submitted after prior written consent of the regional prosecutor with territorial competence for the applying Police station, may, by way of resolution, order operational control.

1a. The written request mentioned in (1) shall be submitted along with the materials that justify the need for operational control.

2. The provision referred to in (1) shall be issued by the district court with territorial competence on account of the seat of the Police authority submitting the request.

3. In cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police

[31] English text provided by the Polish authorities

Commander may order, upon a written consent of the competent prosecutor referred to in (1), operational control, submitting also a request for resolution in that matter to the district court with territorial competence. Should consent not be granted within 5 days from the day of ordering operational control, the managing authority shall withhold the operational control and perform destruction of materials collected during the control in the presence of a committee to be evidenced by a report.

4. (revoked)

5. Should the need arise to order operational control in relation to a suspect or person charged, the request of the Police authority, referred to in (1), to order operational control should be accompanied by information about the proceedings against that person.

6. [3] Operational control is 3performed secretly and consists in:

1) obtaining and recording the contents of the conversations conducted via technical measures, including telecommunications networks;
2) obtaining and recording image or sound of persons from rooms, means of transport, or places other than public places;
3) obtaining and recording the contents of correspondence, including correspondence conducted via electronic communication measures;
4) obtaining and recording data included on IT data carriers, telecommunications terminal devices, IT and ICT systems;
5) obtaining access to and inspecting the contents of parcels.

6a. [4] Operational control does not encompass the activities mentioned in (6)(2), comprising in obtaining and recording image in the rooms mentioned in Article 15(1)(4a).

6b. [5] No consent of a court is required to conduct the activities mentioned in (6a).

7. The request of the Police authority, referred to in (1), to operational control ordered by the regional court, should include in particular:

1) case number and cryptonym, if any, of the case;
2) description of the offence, stating, if possible, its legal qualification;
3) circumstances justifying the need to perform operational control, including stated or possible ineffectiveness or uselessness of other measures;
4) data of a person or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control;
5) objective, time and type of operational control referred to in (6).

8. Operational control shall be ordered for a period not exceeding 3 months. The District court may, upon written request of the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander, following a written consent of the competent prosecutor, for a period not exceeding 3 subsequent months, issue a resolution on single extension of operational control, if the reasons for ordering the control have not been established.

9. [6] In justified cases, when new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime appear, the regional court may, upon a written consent of the Police Commander in Chief, filed following a written consent of the Public Prosecutor General, , also after the lapse of the periods mentioned in (8), issue subsequent extensions of operational control, whose total length may not exceed 12 months.

9a. [7] The Police Commander in Chief, Commander of the Central Bureau of Police Investigations, Voivodship Police Commander may authorize their deputies to file requests mentioned in (1), (3), (8), and (9) or to manage operational control pursuant to (3).

10. The provisions of (1a) and (7) apply to the requests mentioned in (3), (8), and (9). The court, prior to issuing the resolution referred to in (3), (4), (8), and (9) may wish to see the materials justifying the request, which were collected during operational control ordered for that case.

11. Requests referred to in (1), (3-5), (8), and (9) shall be examined by the regional court in a panel of one judge, and the at the same time court proceedings relating to examination of the requests should be performed under conditions foreseen for submission, storage and provision of secret information and adequate application of the regulations issued pursuant to Article 181(2) of the Polish Code of Criminal Procedure. The court sitting may be attended only

by a prosecutor and a representative of the Police authority requesting the order of operational control.

12. [8] The telecommunications undertakings, the postal operator, and the service provider rendering electronic services shall ensure, at their own expense, technical and organisational conditions facilitating the operational control carried out by the Police.

12a. [9] The service provider rendering electronic services who is a micro or a small enterprise in line with the provisions of the Act of 2 July 2004 on the freedom of business activity (Polish Journal of Laws of 2015 item 584, as amended) provides for the technical and organisational terms and conditions enabling the Police to carry out the operational control in line with the infrastructure at their disposal.

13. Operational control should be completed immediately when the causes of its institution no longer exist, at the latest, however, upon the expiry date.

14. The Police authority referred to in (1) shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control.

15. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander shall provide the competent prosecutor mentioned in (1) with any and all materials collected during operational control. Provisions of Article 393(1) first sentence of the Polish Code of Criminal Procedure shall apply accordingly to proceedings before a court in respect to these materials.

15a. Using the evidence obtained in the course of operational control is admissible only in a criminal procedure as regards an offence or a fiscal offence, with respect to which imposing such operational control by any authorized authority is allowed.

15b. The prosecutor mentioned in (1) decides on the scope and manner of using such materials. Articles 238(3-5) and Article 239 of the Polish Code of Criminal Procedure apply accordingly.

15c. If, as a consequence of operational control, a proof of committing an offence or a fiscal offence was obtained, with respect to which operational control may be imposed, committed by a person that was the object of the operational control other than covered by the operational control, or committed by another person, the court that ordered the operational control or consented to it in line with the mode specified in (3), on request of the prosecutor mentioned in (1), decides on whether it is admissible to use it in a criminal procedure.

15d. The request mentioned in (15c) shall be directed by the prosecutor to the court no later than within a month as of receiving the materials collected in the course of the operational control, no later than within 2 months since the end of such control.

15e. The court issues the decision mentioned in (15c) within 14 days since the day the prosecutor files the request.

15f. [10]If the materials mentioned in (15)

1) contain information mentioned in Article 178 of the Polish Code of Criminal Procedure, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or Voivodship Police Commander orders to immediately destroy them officially and to document it;
2) may contain information mentioned in Article 178a and Article 180(3) of the Polish Code of Criminal Procedure, except for the information on offences mentioned in Article 240(1) of the Polish Code of Criminal Procedure, or information comprising privileged information related to practising a profession or holding a function mentioned in Article 180(2) of the Polish Code of Criminal Procedure, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or Voivodship Police Commander provides these materials to the prosecutor.

15g. [11] In the case mentioned in (15f)(2), the prosecutor, immediately after receiving the materials, directs them to the court that ordered the operational control or consented to it under the mode specified in (3), along with a request to:

1) state which materials provided contain information mentioned in (15f)(2);

2) allow using in the criminal procedure of the materials containing information that are privileged information related to practising a profession or holding a function mentioned in Article 180(2) of the Polish Code of Criminal Procedure, not subject to any prohibitions, specified in Article 178a and Article 180(3) of the Polish Code of Criminal Procedure, except for the information on the offences mentioned in Article 240(1) of the Criminal Code.

15h. (12) Immediately after the prosecutor files the request, the court issues a decision to allow the materials mentioned in (15g)(2) in the criminal proceedings, if it is necessary from the viewpoint of the justice system, and the given circumstance may not be established pursuant to different evidence, as well as orders to immediately destroy materials, whose use in the criminal procedure is inadmissible.

15i. (13) The prosecutor is entitled to challenge the admissibility of the materials mentioned in (15g)(2) for use in a criminal proceedings. The provisions of the Polish Code of Criminal Procedure apply accordingly.

15j. (14) The Police authority is obliged to comply with the court order to destroy the materials mentioned in (15h). The materials whose use in the criminal proceedings is inadmissible shall then be destroyed in the presence of a committee and the process evidenced in a report. The Police authority shall immediately inform the prosecutor mentioned in 15g about destroying the materials.

16. The person subject to operational control shall not be provided with materials collected during the control. The provision is not in violation of the rights under Article 321 of the Polish Code of Criminal Procedure.

16a. (15) The regional court, the prosecutor general, the regional prosecutor, and the Police authority keep registers of decisions, written consents, requests, and orders regarding operational control.

16b. (16) The Police Commander in Chief keeps a central register of requests and orders concerning operational control run by Police authorities within the scope as provided for the registers kept by them.

16c. (17) Within the organisational units of the Police that enforce the orders to impose operational control, data included in the operational control documentation may be registered separately, within the scope provided for the registers kept by the Police authorities, mentioned in (16a).

16d. (18) The registers mentioned in (16a-16c) are kept electronically, subject to the provisions on the protection of confidential information.

17. Materials collected during operational control, which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the operational control.

17a. The Police authority is obliged to immediately inform the prosecutor mentioned in (1) on the issue and enforcement of the order to destroy the materials mentioned in (17).

18. (revoked)

19. (revoked)

20. (19) The rulings of the court mentioned in:

1) (1), (3), (8), and (9) – may be appealed against by the Police authority that filed the request to issue such a ruling;

2) (3) and (15c) – may be appealed against by the competent prosecutor mentioned in (1).

The provisions of the Polish Code of Criminal Procedure apply accordingly.

21. (20)The Minister competent for internal affairs, upon consultation with the Minister of Justice and the Minister competent for communications, shall determine, by way of ordinance, mode of record of operational control and storage and submission of requests and orders, as well as storage, submission, processing and destruction of materials obtained during control, taking account of the necessity to ensure secret character of measures taken and materials obtained, and models of forms and registers used.

22. The Minister competent for internal affairs shall provide the lower (Sejm) and upper (Senat) chambers of the Parliament with information about the activity defined in (1-21),

including information and data referred to in Article 20(3). The above should be provided to the Sejm and the Senate by 30 June of the following year.

Article 19a 1.

In cases on crime defined in Article 19(1), criminal police activities aimed to check previously obtained reliable information about the crime and to establish perpetrators and obtain evidence of crime may consist in secret purchase, sale or takeover of objects relating to crime, subject to forfeiture, or the manufacture, possession, transportation or turnover of which is prohibited, as well as to takeover or awarding financial benefits.

2. Preliminary investigations referred to in (1) may also involve a proposal to purchase, sell or takeover objects from crime, that are subject to forfeiture or objects, manufacture, possession, transport or sale of which is illegal, as well as the acceptance or giving of financial benefit.

3. The Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander may institute, for a definite period of time, the activities determined in (1) and (2), following a written consent of the appropriate general prosecutor competent for the seat of the applying Police authority, who shall be kept to date about the results of the activities. The prosecutor may stop the activities at any time.

3a. Before issuing a written consent, the prosecutor familiarizes themselves with the materials that justify the actions mentioned in (1) and (2).

4. The activities mentioned in (1) and (2) shall be instituted for no longer than 3 months. The Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander may, having obtained a written consent of the prosecutor mentioned in (3), order a one-time extension of the activities for a period no longer than another 3 months, if the causes persist. The provision of (3a) applies accordingly.

5. Where, in the course of activities determined in (1) and (2), reasonably justified by new circumstances that are critical for the examination of credible information about a crime and the detection of perpetrators and securing evidence, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander may following a written consent of the competent prosecutor mentioned in (3) order the continuation of activities, even when the periods referred to in (4) have lapsed. The provision of (3a) applies accordingly.

6. 6. The activities referred to in (1) and (2) may be secretly recorded using image or sound recording devices.

7. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander shall provide the competent regional prosecutor mentioned in (3) with any and all materials collected during activities mentioned in (1) and (2). Provisions of Article 393(1) first sentence of the Polish Code of Criminal Procedure shall apply accordingly to proceedings before a court in respect to these materials.

8. Materials collected during the activities mentioned in (1) and (2), which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the activities.

8a. The Police authority is obliged to immediately inform the prosecutor mentioned in (3) on the issue and enforcement of the order to destroy the materials mentioned in (8).

9. Minister competent for internal affairs, upon consultation with the Minister of Justice, shall determine, by way of ordinance, mode of record of activates referred to in (1) and (2), as well as submission, processing and destruction of materials obtained in the course of the activities, giving due regard to the secrecy of these activities and materials, as well as models of forms and records to be used.

Article 19b 1.

To document crimes referred to in Article 19(1) or establish the identity of those involved in the crimes or take over the objects of crime, the Police Commander in Chief, Commander of the

Central Bureau of Police Investigations, or the Voivodship Police Commander may institute a secret surveillance of the manufacture, transport, storage and turnover in crime objects, provided this does not involve a threat to human life or health.

2. The regional prosecutor competent for the seat of the Police authority in charge of the activities shall be notified of such institution immediately. The prosecutor may order the abandonment of the activities at any time.

3. The Police authority mentioned in (1) shall keep the regional prosecutor informed about the results of the activities.

4. 4. In accordance with the order referred to in (1), public authorities and institutions and entrepreneurs shall allow further transport of a parcel containing crime objects in the original condition or, if removed or replaced, in whole or in part.

5. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander shall provide the competent prosecutor mentioned in (2) with any and all materials collected during activities mentioned in (1). Provisions of Article 393(1) first sentence of the Polish Code of Criminal Procedure shall apply accordingly to proceedings before a court in respect to these materials.

6. Minister competent for internal affairs, upon consultation with the Minister of Justice, shall determine, by way of ordinance, mode of record of activates referred to in (1), giving due regard to the secrecy of these activities and materials, as well as models of forms and records to be used.

Article 20 1.

The Police, within the limits provided for in Article 19, may obtain information, *inter alia* secretly, as well as store, check and process this information.

2. (revoked)

2a. The Police may collect, obtain, store, process, and use information for the purposes of implementing statutory tasks, including personal data, concerning the following persons, including without their knowledge and consent:

1) persons suspected of committing offences prosecuted by public indictment;
2) juvenile offenders who have committed crimes prohibited under the Act as offences prosecuted by public indictment;
3) persons of unknown identity or persons who try to conceal their identity;
4) persons posing a threat mentioned in the Act of 22 November 2013 on the procedure concerning the persons with mental disorders that pose a threat to the life, health, or to sexual liberty of other persons;
5) wanted persons;
6) missing persons;
7) [(21)] persons, to whom the assistance and protection measures were imposed, as provided for in the Act of 28 November 2014 on the protection and assistance of victims and witnesses (Polish Journal of Laws of 2015, item 21).

2aa. The Police, in order to implement statutory tasks, may collect, obtain, store, process, verify, and use information, including personal data, obtained or processed by authorities from other countries and by the International Criminal Police Organization – INTERPOL.

2ab. The Police may provide information, including personal data, in order to prevent or combat crime to authorities from other countries or to the International Criminal Police Organization – INTERPOL, mentioned in (2aa), in line with the terms and conditions specified in the Act of 16 September 2011 on sharing information with law enforcement authorities from the European Union (Polish Journal of Laws no. 230 item 1371, of 2013 item 1650, and of 2014 item 1199), in the Community Law, and in the provisions of international agreements.

2b. Information mentioned in (1), (2a), (2aa), and (2ab) concern persons mentioned in (2a) and may include:

1) (1) personal data referred to in Article 27(1) of the Act of 29 August 1997 on the protection of personal data, with the reservation that in the case of genetic code data, non-coding regions of the genome only;

2) fingerprints;
3) photos, drawings, and descriptions of appearance;
4) features, distinguishing marks, pseudonyms;
5) information about the following:

a) place of permanent or temporary residence;
b) education, profession, workplace and position, financial standing and the assets;
c) documents and items that the perpetrator uses;
d) the perpetrator's mode of operations, their background and contacts;
e) the perpetrator's attitude towards the aggrieved persons.

2c. Information mentioned in (2a) is not collected if they are of no detection, evidence, or identification value in the subject procedure.

3. Where necessary for effective prevention of crimes specified in Article 19(1), detection thereof, or establishment of perpetrators and collection of evidence, the Police may use information included in insurance contracts, in particular data which are processed by insurance companies and which concern the entities or individuals that signed insurance contracts, as well as privileged information processed by banks.

4. The information and data referred to in (3) and information related to passing these information and data shall be protected as provided for in the provisions on the protection of secret information, and shall be disclosed only to police officers involved in a particular case and their superiors authorised to execute supervision over preliminary investigation carried out by their subordinates. Moreover, records containing such information and data shall be made available only to courts and prosecutors, if such a necessity occurs due to criminal prosecution.

5. Information and data referred to in (3) shall be made available on the basis of an resolution issued at the written request of the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander by a regional court that has the territorial competence for this particular case owing to the location of the seat of the authority that has lodged the request.

6. The request mentioned in (5) shall specify:

1) case number and cryptonym, if any, of the case;
2) description of the offence, stating, if possible, its legal qualification;
3) the circumstances which justify the need to disclose the information and data;
4) the entity that the information and data relate to;
5) the entity obliged to disclose the information and data;
6) the type and the scope of the information and data.

7. Having examined the request, the court shall, by way of resolution, give the consent to disclosing the information and data of the entity concerned, defining their type and scope, the entity obliged to disclose them, and the police authority entitled to request them; or refuse to give the consent to disclosing the information and data. Article 19(11) shall apply accordingly.

8. The Police authority that has lodged the request to issue a resolution is entitled to appeal against the resolution referred to in (7).

9. The police authority authorised by the court shall provide the entity obliged to disclose the information and data with a written notification which shall communicate the type and scope of information and data to be disclosed, the entity that the information and data relate to, and the name of the police officer authorised to collect them.

10. Notwithstanding (11) and (12), the Police shall, within 90 days of the date the information and data referred to in (3) are collected, notify the entity referred to in (6)(4) about the court resolution giving consent to disclosing the information and data.

11. The court that has issued a resolution ordering to disclose information and data at the request of the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander lodged after obtaining the written consent of the General Public Prosecutor, may, by way of resolution, suspend, for a certain period with the possibility of prolongation, the obligation referred to in (10), if it has been reasonably demonstrated that notification of the entity referred to in (6)(4) may affect the results of preliminary investigation. Article 19(11) shall apply accordingly.

12. If preliminary proceedings are instituted within the period specified in (10) or (11), the prosecutor, or the Police, if so ordered by the prosecutor, shall notify the entity referred to in (6)(4) about the court resolution giving consent to disclosing the information and data prior to the termination of the preliminary proceedings or immediately after discontinuance thereof.

13. If the information and data referred to in (3) do not provide sufficient evidence to initiate preliminary proceedings, the authority that has requested the resolution shall notify this fact in writing to the entity that provided the information and data.

14. The State Treasury shall be liable for damages following from the violation of the provisions of (4) as provided for in the Civil Code.

15. In order to prevent or detect crimes or identify persons, the Police may obtain, store and process information, including personal data from records kept by public authorities pursuant to separate provisions, in particular from the National Criminal Register and the Electronic System of Population Records (PESEL), including collections of data that are used to process data that includes personal data, as a result of the investigative activities undertaken by these authorities. Administrators of data stored in these registers shall make them available free of charge.

16. Public authorities that keep registers referred to in (15)may, by way of decision, consent to disclose the information stored in these registers by means of telecommunications devices for the benefit of Police organisational units without the necessity to submit written requests, provided that:

1) these units have devices at their disposal that can record in the system who used the data, when, and for what purpose, as well as which data have been disclosed;
2) these units have technical and organisational measures for prevention of the use of the data contrary to the purpose for which data have been disclosed;
3) it is justified owing to the specificity or scope of the tasks or activities carried out.

16a. The personal data mentioned in (2a), (2aa), (2ab) and (15), except for personal data mentioned in Article 27(1) of the Act of 29 August 1997 on personal data protection. The Police may process:

1) for the purpose other than the purpose for which the data were collected, obtained, provided, disclosed, or gathered – if it is necessary to implement the statutory tasks of the Police;
2) for historic, statistical, or other research purposes – provided that the data is modified in a way that prevents assigning an identification number or specific physical features, physiological features, mental features, economic features, cultural features, or social features, to a specific or identifiable natural person, or provided that such assigning would require incommensurable costs, time, or actions.

17. 17. Personal data collected with the view to crime detection shall be stored as long as the Police will need them to perform its statutory tasks. Police authorities shall verify these data, disposing of redundant items, at least once every 10 years starting from the date the information is obtained.

17a. The personal data that is deemed irrelevant may be transformed in a way that prevents assigning individual personal or material information to a specific or identifiable natural person, or provided that such assigning would require incommensurable costs, time, or actions.

17b. The personal data mentioned in (17) shall be deleted, if the Police authority has received reliable information that:

1) the offence that served as the basis for adding the information to the data set was not committed, or there is insufficient data that justifies the suspicion sufficiently;
2) the event or circumstances, in connection with which the information was added to the data set, does not meet the conditions of a prohibited act;
3) the person concerned by the data was acquitted by means of a binding court judgement.

18. Personal data that disclose race or ethnicity, political views, religious or philosophical attitudes, religion, party or trade union membership, data about health, addictions or sexual relations of persons suspected of crimes prosecuted on indictment who have not been

convicted for these crimes, shall be destroyed immediately after adequate ruling enters into force.

19. The Minister competent for internal affairs shall determine, by way of ordinance, the methods for processing the personal data referred to in (2a), (2aa), and (2ab) in databases, specify which police forces are allowed to use the databases, and set out models of the documents to be used in data processing, with due regard given to the need to protect data from unauthorised access, and the conditions to refrain from collecting specific types of information, and in the case of information mentioned in (2aa) and (2ab), considering the necessity to comply with the requirements specified by the authorities of other countries or by the International Criminal Police Organization – INTERPOL, specified in (2aa) in connection with collecting or obtaining such information.

Article 20a 1.

On account of carrying out the tasks referred to in Article 1(2) the Police shall ensure protection for the forms and methods of task performance, information, its own facilities and the particulars of police officers.

2. In the course of preliminary investigation, police officers may use documents which prevent determination of their particulars and the measures applied when performing official duties.

3. In special cases, (2) may apply to persons referred to in Article 22(1).

3a. A person shall not be guilty of a crime, if they:

1) order the documents referred to in (2) and (3) to be drawn up or oversee drawing up of such documents;
2) draw up the documents referred to in (2) and (3);
3) assist in drawing up of the documents referred to in (2) and (3);
4) are a police officer or the person referred to in (3), if they use the documents referred to in (2) and (3).

3b. Government administration authorities and local government authorities shall, within the scope of their competence, assist the Police in issuing and securing the documents referred to in (2) and (3).

4. The Minister competent for internal affairs shall, by way of ordinance, lay down detailed rules and procedure for issuance, use and storage of the documents referred to in (2) and (3), with due regard given to the types of documents and the purpose for which they are disclosed, the authorities and persons authorised to issue, use and store the documents, the period for which they are made available, measures ensuring protection of the documents, and the rules for storing and recording these documents.

Article 20b

Disclosure of information about detailed form, principles and organisation of preliminary investigation, activities being carried out, as well as applied measures and methods of their implementation shall be allowed only in the case of justified suspicion that a crime prosecuted on indictment has been committed in relation to performance of these activities. In such a case, information shall be disclosed in accordance with the procedure laid down in Article 9 of the Act of 21 June 1996 on some powers of the personnel of the office servicing the Minister competent for internal affairs and the personnel of offices supervised by this minister (Polish Journal of Laws no. 106 item 491 as amended).

Article 20c [(22)] 1.

In order to prevent or detect crimes or in order to save human life and health, or in order to support rescue and find missions, the Police may obtain data that does not constitute a telecommunications message, a postal parcel, or a transmission within an electronic service, defined in:

1) Article 180c and Article 180d of the Act of 16 lipca 2004 - Telecommunications Law (Polish Journal of Laws of 2014 item 243 as amended), hereinafter referred to as “telecommunications data”;
2) Article 82(1)(1) of the Act of 23 November 2012 – Postal Law (Polish Journal of Laws item 1529 and of 2015 item 1830), hereinafter referred to as “postal data”;

3) Article 18(1-5) of the Act of 18 July 2002 – Act on electronic services (Polish Journal of Laws of 2013 item 1422 and of 2015 item 1844), hereinafter referred to as “on-line data”;

– and may process them without the knowledge and consent of the person concerned by such data.

2. A telecommunications undertaking, a postal operator, or a service provider rendering electronic services discloses, free of charge, data mentioned in (1):

1) to a police officer specified in the written request filed by the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander or person authorized by them;

2) at a verbal request of a police officer being in possession of a written authorization issued by the persons mentioned in (1);

3) via a telecommunications network to a police officer being in possession of a written authorization issued by the persons mentioned in (1).

3. In the case mentioned in (2)(3), disclosure of data mentioned in (1) takes place without participation of the employees of the telecommunications undertaking, postal operator, or service provider rendering electronic services, or with their minimal participation, if it is provided for in the agreement concluded by and between the Police Commander in Chief and that entity.

4. Disclosure of the data mentioned in (1) to the Police may take place via a telecommunications network, provided that:

1) the telecommunications networks used ensure:

a) that it is possible to ascertain the person that obtained the data, type of the data, and the time of obtaining the data;

b) technical and organisational safeguards that prevent unauthorized access to the data;

2) it is justified by the specifics or the scope of the tasks performed by the organisational units of the Police or the actions conducted by them.

5. The Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander keep registers of requests to obtain telecommunications, postal, and on-line data that identify the organisational unit of the Police and the police officer that obtained the data, their type, purpose, and time of obtaining. The registers are kept electronically, subject to the provisions on the protection of confidential information.

6. The data mentioned in (1) that are of significance for a criminal proceedings, shall be provided to the competent prosecutor by the Police Commander in Chief, Commander of the Central Bureau of Police Investigations, or the Voivodship Police Commander. The prosecutor decides on the scope and manner of using such data.

7. Data mentioned in (1) that are of no significance for the criminal proceedings, shall be destroyed in the presence of a committee and the process evidence in a report.

Article 20ca [(23)] 1.

The control over obtaining by the Police of telecommunications, postal, or on-line data shall be exerted by the regional court competent for the seat of the Police authority that received the data.

2. The Policy authority mentioned in (1) provides, subject to the provisions on the protection on confidential information, to the regional court mentioned in (1), semi-annually, a report that lists:

1) the number of cases of obtaining telecommunications, postal, or on-line data in the reporting period, quoting the type of the data;

2) legal qualifications, with connection with which the requests for the telecommunications, postal, or on-line data were filed, or the information on obtaining the data in order to save human health or life, or to support rescue and find missions.

3. In the course of the control mentioned in (1), the regional court may familiarize themselves with the materials that justify disclosure of the telecommunications, postal, or on-line data to the Police.

4. The district court shall inform the Police authority about the results of the inspection within 30 days since its end.

5. The inspection mentioned (1) does not extend to obtaining data pursuant to Article 20cb(1).

Article 20cb [24] 1.
In order to prevent or detect crimes, or in order to save human health or life, or to support rescue and find missions, the Police may obtain data:
1) from the list mentioned in Article 179(9) of the Act of 16 July 2004 – Telecommunications Law;
2) mentioned in Article 161 of the Act of 16 July 2004 – Telecommunications Law;
3) in the case of a user who is not a natural person, the number of the network termination, and the seat or place of conducting business activity, business name or name and organisational form of the user;
4) in the case of landline public telecommunications network – also the name of the city/town, and the street where the network terminal is located, access to which is granted to the user
– and may process them without the knowledge and consent of the person concerned by such data.

2. Article 20c(2-7) applies to disclosure and processing of data mentioned in (1).

Article 20d [25]
(revoked).

Article 20da 1. [26]
For the purposes of looking for missing persons, the Police may obtain telecommunications, postal, and on-line data, and may process it without the knowledge and consent of the person concerned by them; Article 20c(2-7) applies.

2. The materials collected in the course of the actions specified in (1) that do not contain information that is of significance for looking for missing persons shall be destroyed in the presence of a committee and the process evidence in a report.

EXTRACTS
FROM THE POLISH LEGISLATION
DEVELOPING THE NOTION OF METADATA

Telecommunications Law of 16 July 2004 (official translation):

Article 180c
1. The obligation mentioned in Article 180a(1) applies to the data needed to:
1) determine the network termination, telecommunications terminal device, end-user:
a) that initiates the connection;
b) to which the connection is directed;
2) specify:
a) date and hour of the connection, the length of the connection;
b) type of the connection;
c) location of the telecommunications terminal device.
2. The [competent ministers, including the Minister of Interior], considering the type of the telecommunications operations conducted […], data specified in 1), costs of obtaining and retaining data, and the need to avoid multiple retention and storage of the same data, shall specify by means of an ordinance:
1) a detailed list of data mentioned in 1);
2) types of [operators or providers] obliged to retain and store such data."

Article 180d
"[Telecom providers] are obliged to ensure access to, record, and disclose to eligible entities, including the Customs Service, the courts, and the prosecutor, at their own cost, the data processed by them as mentioned in Article 159(1)(1 and 3-5), Article 161, and Article 179(9) related to the telecommunications service rendered, on the terms and conditions and subject to the procedures specified in separate provisions."

Article 159. 1[32]
"The communications confidentiality within telecommunications networks, hereinafter called the "telecommunications confidentiality", shall encompass:
1) data concerning the user;
[…]
3) transmission data understood as data processed for the purpose of transferring messages within telecommunications networks or charging payments for telecommunications services, including location data, which should be understood as any data processed in a telecommunications network or within the framework of telecommunications services indicating geographic location of terminal equipment of a user of publicly available telecommunications services;
4) location data, understood as location data beyond the data necessary for message transmission or billing;
5) data relating to call attempts between specific telecommunications networks termination points, including data relating to unsuccessful call attempts meaning calls between telecommunications terminal equipment or network termination points which have been set up and not answered by an end user or aborted."

[32] *Translation from the web-site of the Polish Office of Electronic Communications:* *https://en.uke.gov.pl/files/?id_plik=41*

Article 161. 1
"Subject to 2), the contents or data subject to ICT privilege may be collected, recorded, stored, analysed, adjusted, deleted, or disclosed only if these actions, hereinafter referred to as "processing", only concern the service rendered to the user or are necessary in order to render the service. Processing for other purposes is only allowed pursuant to the statute.
2. Provider of publicly available ICT [(i.e. information and communication technology)] services is entitled to process the following data concerning a user who is a natural person:
1) first and last names;
2) first names of parents;
3) place and date of birth;
4) place of residence and address for correspondence, if different than the place of residence;
5) PESEL identification number [i.e. personal identification number] – for Polish nationals;
6) name, series and numbers of documents confirming identity; for foreigners who are not nationals of a Member State or of the Swiss Confederation – passport number or number of a residence card;
7) included in the documents to confirm the ability to complete the obligation towards the provider of publicly available ICT data under the ICT services contract.
3. Next to the data mentioned in 2), the provider of publicly available ICT services may, with the consent of a user who is a natural person, process other data of such user in connection with the service rendered, in particular the bank account number or the number of a bank card, an e-mail address, and contact phone numbers."

Article 179
"9. A telecommunications undertaking that provides publicly available ICT services is obliged to keep an electronic list of subscribers, users, or network termination, considering the data obtained upon the conclusion of the agreement."

Law on electronic services of 18 July 2002(official translation)

Article 18
"1 . The Service Provider may process the following personal data of the Client that is necessary to establish, shape the contents, amend, or terminate the legal relationship between them:
1) first and last name of the Client;
2) PESEL identification number or, if that number was not awarded, number of a passport, a personal identity document, or another document that confirms the holder's identity;
3) permanent registered address;
4) address for correspondence, if other than the address provided in 3);
5) data used to verify the electronic signature of the Client;
6) e-mail addresses of the Client.
[…]
4. The Service Provider may process, with the consent of the Client and for the purposes specified in Article 19(2)(2), other data concerning the Client that are not required in order to render the electronic service.
5. The Service Provider may process the following data that characterise the manner of using by the Client of the electronic service rendered (exploitation data):
1) designations identifying the Client granted based on the data mentioned in 1);
2) designations identifying the ends of the ICT network or IT system used by the Client;
3) information on commencing, concluding, and on the scope of using the electronic service;
4) information on the fact that the Client used electronic services."

Postal Law of 23 November 2012 (official translation)

Article 82.1

The postal operator […] shall be obliged to provide free of charge […] the technical and organisational abilities for the Police [and other law-enforcement and intelligence agencies] and the prosecution and the courts, the tasks specified in separate provisions that require:

1) obtaining data on the postal operator, postal services rendered, and information that enables identification of the entities that take advantage of such services.