Ius Novum
2/2017

NEW EUROPEAN UNION LAW ON PROTECTING EUROPEAN UNION CLASSIFIED INFORMATION

STANISŁAW HOC*

The issue of protecting the European Union classified information has been discussed in the literature[1] and institutions responsible for the protection of classified information based on the Act of 5 August 2010 on protecting classified information,[2] the development of which was accelerated due to the fact that the Republic of Poland was soon to hold the Presidency of the Council of the European Union. It is worth emphasising that the statute meets very high legislative standards.

The regulation that was binding in the EU, i.e. the Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations,[3] was subsequently repealed and replaced by the Council Decision 2011/292/EU of 31 March 2011 on

* prof. dr hab., Wydział Prawa i Administracji Uniwersytetu Opolskiego

1 S. Hoc, *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia* [Protecting classified information and other secret data under statutory protection: Selected issues], Wydawnictwo Uniwersytetu Opolskiego, Opole 2006, pp. 161–168; S. Hoc, *Ochrona informacji niejawnych pochodzących od organów Unii Europejskiej, NATO oraz innych państw* [Protection of classified information of the European Union, NATO and other states], [in:] M. Gajos (ed.), *Ochrona informacji niejawnych i biznesowych*, Materiały II Kongresu [Protection of classified and business information: 2nd Congress material], Katowice 2006, pp. 33–46; S. Hoc, *Ochrona informacji niejawnych Unii Europejskiej* [Protection of European Union classified information], Przegląd Prawa Publicznego No. 10, 2011, pp. 43–54; S. Hoc, *Ochrona informacji niejawnych wymienianych w interesie Unii Europejskiej* [Protection of classified information exchanged in the interest of the European Union], Przegląd Prawa Publicznego No. 7–8, 2013, pp. 43–54; S. Zalewski, *Przepisy odnoszące się do informacji niejawnych w UE i NATO oraz ich implementacja do prawa polskiego* [Regulations regarding classified information in the EU and NATO, and their implementation in Polish law], [in:] G. Szpor (ed.), *Jawność i jej ograniczenia* [Openness and its limitation], Volume VI: A. Gryszczyńska (ed.), *Struktura tajemnic* [Structure of secrets], C.H. Beck, Warsaw 2014, pp. 77–143.

2 Journal of Laws [Dz.U.] of 2016, item 1167; see, S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz* [Act on protecting classified information: Commentary], LexisNexis, Warsaw 2010; I. Stankowska, *Ustawa o ochronie informacji niejawnych. Komentarz* [Act on protecting classified information: Commentary], LexisNexis, Warsaw 2014.

3 Official Journal of the European Union of 11.4.2001, L 101/1 with subsequent amendments.

the security rules for protecting EU classified information,[4] which entered into force on the day of its publication, i.e. 27 May 2011. Currently applicable are: the Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information[5] and the Commission Decision (EU, Euratom) 2015/443/EU of 13 March 2015 on security in the Commission[6] and Commission Decision (EU, Euratom) 2015/444 on protecting EU classified information[7].

It is worth emphasising that the Agreement between the Member States of the European Union, meeting within the Council, regarding the Protection of Classified Information Exchanged in the Interests of the European Union of 25 May 2011[8] is a legal document introducing a coherent and complex policy of protecting classified information that is in force beside, not instead of, the regulations on the security of the Council.

The preamble to the Decision 2013/488/EU indicates that in order to develop the Council activities in all areas which require handling classified information, it is appropriate to establish a comprehensive security system for protecting classified information covering the Council, its General Secretariat and the Member States. The Decision should apply where the Council, its preparatory bodies and the General Secretariat of the Council (GSC) handle the EU classified information (EUCI). It is emphasised that in accordance with national laws and regulations and to the extent required for the functioning of the Council, the Member States should respect this Decision where their competent authorities, personnel or contractors handle EUCI, so that each may be assured that an equivalent level of protection is afforded to EUCI. It is emphasised that the Council, the Commission and the European External Action Service (EEAS) are committed to applying equivalent security standards for protecting EUCI. The Council underlines the importance of associating, where appropriate, the European Parliament and other Union institutions, bodies or agencies to observe the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States. The Council has been obliged to determine the appropriate framework of sharing EUCI held by the Council with other Union institutions, bodies or agencies, as appropriate, in accordance with the Decision 2013/488/EU and inter-institutional arrangements in force.

The Decision 2013/488/EU is composed of 19 articles discussed below.

Article 1 applies to the purpose, scope and definitions. The Decision lays down the basic principles and minimum standards of security for protecting EUCI. The basic principles and minimum standards apply to the Council and the General Secretariat of the Council and are respected by the Member States in accordance with their respective national laws and regulations, so that each may be assured that an equivalent level of protection is afforded to EUCI. For the purposes of

---

4 Official Journal of the European Union of 27.5.2011, L 141/1.

5 Official Journal of the European of Union 15.10.2013, L 274/1.

6 Official Journal of the European Union of 17.3.2015, L72/41.

7 Official Journal of the European Union of 17.3.2015, L72/53.

8 Official Journal of the European Union 8.7.2011, C 202/13 and Journal of Laws [Dz.U.] of 2015, item 2159.

the Decision 2013/488/EU, the definitions set out in Appendix A shall apply. It contains 51 terms, inter alia accreditation, document, TEMPEST, classified contract, originator, material, etc.

Article 2 concerns the definition of EUCI, security classifications and markings. The European Union Classified Information means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or one or more of the Member States. EUCI is classified at one of the following levels:

1) TRÈS SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of its Member States;
2) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of its Member States;
3) CONFIDENTIAL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of its Member States;
4) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of its Member States.

Classified information bears the above security classification marking, however, it may bear additional markings to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

Article 3 concerns classification management. The competent authorities ensure that EUCI is appropriately classified, clearly identified as classified information and retains its classification level for only as long as necessary. EUCI shall not be downgraded or declassified nor shall any of the markings be modified or removed without the prior written consent of the originator. The Council shall approve a security policy on creating EUCI, which shall include a practical classification grade.

Article 4 applies to the protection of classified information. It states that the EU classified information shall be protected in accordance with the Decision 2013/488/EU, and the holder of any item of EUCI shall be responsible for protecting it in accordance with this Decision. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Union, the Council and the General Secretariat of the Council shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B to the Decision. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 5 refers to security risk management. Risk to EUCI is managed as a process. This process is aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in the Decision 2013/488/EU and at applying those measures in line with the concept of defence in depth as

defined in Appendix A to the Decision. The effectiveness of such measures is continuously evaluated. It must be underlined that security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious or criminal activities, including espionage, sabotage and terrorism. Contingency plans take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability. On the other hand, preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI are included in business continuity plans.

Article 6 applies to implementation of the Decision 2013/488/EU. Where necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing this Decision. The Security Committee may agree at its level security guidelines to supplement or support the Decision 2013/488/EU and any security policies approved by the Council.

Article 7 concerns personnel security. Personnel security is the application of measures to ensure that access to EUCI is granted only to individuals who have:

1) a need-to-know,
2) been security cleared to the relevant level, where appropriate, and
3) been briefed on their responsibilities.

Personnel security clearance procedures are designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI. All individuals in the General Secretariat of the Council whose duties require them to have access to or handle EUCI classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level before being granted access to such EUCI. Such individuals must be authorised by the GSC Appointing Authority to access EUCI up to a specified level and up to a specified date. Member States' personnel whose duties may require access to EUCI classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security cleared to the relevant level or otherwise duly authorised by virtue of their functions, in accordance with national laws and regulations. Before being granted access to such EUCI and at regular intervals thereafter, all individuals shall be briefed on and acknowledge their responsibilities to protect EUCI in accordance with the Decision 2013/488/EU.

Article 8 applies to physical security, i.e. the application of physical and technical protective measures to prevent unauthorised access to EUCI. Physical security measures are designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process. Physical security measures are put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems. Areas in which EUCI classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored are established as Secured Areas in accordance with Annex II to the Decision

and approved by the competent security authority. Only approved equipment or devices are used for protecting EUCI at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above.

Article 9 concerns the management of classified information. The management of classified information is the application of administrative measures for controlling EUCI throughout its life cycle to supplement the measures provided for in Articles 7, 8 and 10, and thereby help deter and detect deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI. Information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and receipt. The competent authorities in the GSC and in the Member States shall establish a registry system for this purpose. Information classified as TRÈS SECRET UE/EU TOP SECRET shall be registered in designated registries. Services and premises where EUCI is handled or stored are subject to regular inspection by the competent security authority. EUCI shall be conveyed between services and premises outside physically protected areas as follows: by electronic means protected by cryptographic products or on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products, or, in all other cases, as prescribed by the competent security authority in accordance with the relevant protective measures laid down in Annex III to the Decision.

Article 10 applies to the protection of EUCI handled in communication and information systems. It is detailed and contains nine paragraphs. Information assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Effective information assurance shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. Information assurance is based on a risk management process. A Communication and Information System (CIS) means any system enabling the handling of information in electronic form. The CIS shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources. The Decision 2013/488/EC applies to a CIS handling EUCI. The CIS shall handle EUCI in accordance with the concept of information assurance. All CIS shall undergo an accreditation process. Accreditation aims at obtaining assurance that all appropriate security measures have been implemented and that a sufficient level of protection of EUCI and of a CIS has been achieved in accordance with the Decision. The accreditation statement shall determine the maximum classification level of the information that may be handled in a CIS as well as the corresponding terms and conditions. Security measures (referred to as TEMPEST security measures) shall be implemented to protect CIS handling information classified as CONFIDENTIEL UE/EU CONFIDENTIAL and above against compromise of such information through unintentional electromagnetic emanations. Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information. Article 10(6) lays down how cryptographic product shall be approved.

During the transmission of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or specific technical configurations as specified in Annex IV to the Decision. The competent authorities of the GSC and of the Member States respectively shall establish the following information assurance functions: an Information Assurance Authority (IAA), a TEMPEST Authority (TA), a Crypto Approval Authority (CAA), and a Crypto Distribution Authority (CDA). For each system, the competent authorities of the GSC and of the Member States, respectively, shall establish: a Security Accreditation Authority (SAA), and an IA Operational Authority.

Article 11 applies to industrial security, i.e. the application of measures to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the life cycle of classified contracts. Such contracts shall not involve access to information classified as TRÈS SECRET UE/EU TOP SECRET. The GSC may entrust by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities registered in a Member State or in a third State which has concluded an agreement or an administrative arrangement in accordance with point (a) or (b) of Article 13(2). The GSC, as contracting authority, shall ensure that the minimum standards on industrial security set out in the Decision, and referred to in the contract, are complied with when awarding classified contracts to industrial or other entities. The National Security Authority (NSA), the Designated Security Authority (DSA) or any other competent authority of each Member State shall ensure, to the extent possible under national laws and regulations, that contractors and subcontractors registered in their territory take all appropriate measures to protect EUCI in pre-contract negotiations and when performing a classified contract. The NSA, DSA or any other competent security authority of each Member State shall ensure, in accordance with national laws and regulations, that contractors or subcontractors registered in the respective Member State participating in classified contracts or sub-contracts which require access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either in the performance of such contracts or during the pre-contractual stage, hold a Facility Security Clearance (FSC) at the relevant classification level. The contractor or subcontractor personnel who, for the performance of a classified contract, require access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be granted a Personnel Security Clearance (PSC) by the respective NSA, DSA or any other competent security authority in accordance with national laws and regulations and the minimum standards laid down in Annex I to the Decision.

Article 12 applies to sharing EUCI. The Council shall determine the conditions under which it may share EUCI held by it with other Union institutions, bodies, offices or agencies. An appropriate framework may be put in place to that effect, including by entering into inter-institutional agreements or other arrangements where necessary for that purpose. Any such framework shall ensure that EUCI is given protection appropriate to its classification level and according to basic

principles and minimum standards, which shall be equivalent to those laid down in the Decision.

Article 13 refers to the exchange of classified information with third States and international organisations. Where the Council determines that there is a need to exchange EUCI with a third State or an international organisation, an appropriate framework shall be put in place to that effect. The Union shall conclude agreements with third States or international organisations on security procedures for exchanging and protecting classified information (called "security of information agreements"), or the Secretary-General may enter into administrative arrangements on behalf of the GSC in accordance with paragraph 17 of Annex VI where the classification level of EUCI to be released is as a general rule no higher than RESTREINT UE/EU RESTRICTED. The decision to release EUCI originating in the Council to a third State or an international organisation shall be taken by the Council on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired is not the Council, the GSC shall first seek the originator's written consent to release. If the originator cannot be established, the Council shall assume the former's responsibility. Assessment visits shall be arranged to ascertain the effectiveness of the security measures in place in a third State or an international organisation for protecting EUCI provided or exchanged.

Article 14 refers to breaches of security and compromise of EUCI. A breach of security occurs as a result of an act or omission by an individual, which is contrary to the security rules laid down in the Decision. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons. Any breach or suspected breach of security shall be reported immediately to the competent security authority. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, the NSA or other competent authority shall take all appropriate measures in accordance with the relevant laws and regulations to:

1) inform the originator,
2) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts,
3) assess the potential damage caused to the interests of the Union or of the Member States,
4) take appropriate measures to prevent a recurrence, and
5) notify the appropriate authorities of the action taken.

Any individual who is responsible for a breach of the security rules laid down in the Decision may be liable to disciplinary action in accordance with the applicable rules and regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary or legal action in accordance with the applicable laws, rules and regulations. In case of the commission of crime of the EU classified information disclosure, law enforcement bodies in Belgium (EU headquarters) or a Member State concerned (e.g. Poland) shall initiate prosecution.

Article 15 lays down the principles of responsibility for implementation. The Council shall take all necessary measures to ensure overall consistency in the application of the Decision 2013/488/EU. The Secretary-General shall take all necessary measures to ensure that, when handling or storing EUCI or any other classified information, the Decision is applied in premises used by the Council and within the GSC, by GSC officials and other servants, by personnel seconded to the GSC and by GSC contractors. Member States shall take all appropriate measures, in accordance with their respective national laws and regulations, to ensure that when EUCI is handled or stored the Decision is respected.

Article 16 lays down the organisation of security in the Council. As part of its role in ensuring overall consistency in the application of the Decision, the Council approves:

1) security of information agreements,
2) decisions consenting to the release of EUCI to third States and international organisations,
3) an annual assessment visit programme proposed by the Secretary-General and recommended by the Security Committee,
4) security policies.

The Secretary-General is the GSC's Security Authority. In that capacity, the Secretary-General:

1) implements the Council's security policy and keeps it under review,
2) coordinates with Member States' NSAs on all security matters relating to the protection of classified information relevant for the Council's activities,
3) grants the EU officials and other GSC servants Personnel Security Clearance (PSC),
4) as appropriate, orders investigations into any actual or suspected compromise or loss of classified information held by or originating in the Council and requests the relevant security authorities to assist in such investigations,
5) undertakes periodic inspections of the security arrangements for protecting classified information on GSC premises,
6) undertakes periodic visits to assess the security arrangements for protecting EUCI in Union bodies, agencies, Europol and Eurojust as well as in the course of crisis management operations and assurance measures used by EU special representatives (EUSRs) and their teams,
7) undertakes jointly and in agreement with the NSA concerned periodic assessment of the security arrangements for protecting UECI in Member States' services and premises,
8) coordinates security measures as necessary with the competent authorities of the Member States responsible for protecting classified information and, as appropriate, third States or international organisations, including on the nature of threats to the security of EUCI and the means of protection against them,
9) enters into the administrative arrangements.

The Security Office of the GSC is at the disposal of the Secretary-General to assist in those responsibilities.

For the purposes of implementing Article 15(3), regarding Member States' responsibility to ensure that the Decision is respected, Member States should:

1) designate a National Security Authority (NSA) responsible for security arrangements for protecting EUCI in order that:
   a) EUCI held by any national department, body or agency, public or private, at home or abroad, is protected in accordance with the Decision 2013/488/EU,
   b) security arrangements for protecting EUCI are periodically inspected or assessed,
   c) all individuals employed within a national administration or by a contractor who may be granted access to information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above are appropriately security cleared or are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations,
   d) security programmes are set up as necessary in order to minimise the risk of EUCI being compromised or lost,
   e) security matters related to protecting EUCI are coordinated with other competent national authorities, including those referred to in the Decision 2013/488/EU,
   f) responses are given to appropriate security clearance requests in particular from any Union bodies, agencies, entities;
2) ensure that their competent authorities provide information and advice to their governments, and through them to the Council, on the nature of threats to the security of EUCI and the means of protection against them.

Article 17 lays down the tasks of the Security Committee, which examines and assesses any security matter within the scope of the Decision 2013/488/EU and gives recommendations to the Council as appropriate. The Security Committee is composed of representatives of the Member States' NSAs and is attended by a representative of the Commission and of the EEAS. It is chaired by the Secretary-General or by his designated delegate. The Committee meets as instructed by the Council, or at the request of the Secretary-General or of an NSA. Representatives of the Union bodies, agencies and entities that apply this Decision or the principles thereof may be invited to attend when questions concerning them are discussed.

The Security Committee organises its activities in such a way that it can give recommendations on specific areas of security. It establishes an expert sub-area for IA issues and other expert sub-areas as necessary. It also draws up terms of reference for such expert sub-areas and receives reports from them on their activities including, as appropriate, any recommendations for the Council.

In accordance with Article 19, the Decision 2013/488/EU entered into force on the date of its publication in the Official Journal of the European Union, i.e. on 15 October 2013.

The Decision is supplemented with annexes and appendices, which are its integral parts. Those concern the following areas.

Annex I: Personnel security is composed of 43 paragraphs. It lays down criteria for determining whether an individual, taking into account his loyalty, trustworthiness

and reliability, may be authorised to have access to EUCI, and the investigative and administrative procedures to be followed to that effect.

Annex II: Physical security consists of 31 paragraphs. It lays down minimum requirements for the physical protection of premises, buildings, offices, rooms and other areas where EUCI is handled and stored, including areas housing a CIS.

Annex III: Management of classified information consists of 63 paragraphs. It lays down the administrative measures for controlling EUCI throughout its life cycle in order to help deter and detect deliberate or accidental compromise or loss of such information.

Annex IV: Protection of EUCI handled in a CIS consists of 52 paragraphs. Provisions set out in this annex form a baseline for the security of any CIS handling EUCI. Detailed requirements for implementing these provisions are defined in IA security policies and security guidelines.

Annex V: Industrial security consists of 36 paragraphs. It lays down general security provisions applicable to industrial or other entities in pre-contract negotiations and throughout the life cycle of classified contracts let by the GSC.

Annex VI: Exchange of classified information with third States and international organisations consists of 39 paragraphs.

Appendix A contains definitions applying to the terms used for the purpose of the Decision. Appendix B contains equivalent classification of classified information in the 28 EU Member States. Appendix C contains a list of National Security Authorities (NSAs). It is worth mentioning that only in two EU Member States, there are two NSAs designated: in Denmark this is the Danish Security Intelligence Service and the Danish Defence Intelligence Service, and in the Netherlands Ministerie van Binnenlandes Zaken en Koninkrijksrelaties and Ministerie van Defensie Beveiligingsautoriteit. Appendix D contains a list of 30 abbreviations.

In Poland, the Head of the Internal Security Agency (ISA) is designated to perform the role of National Security Authority. In the military, the Head of the Military Counterintelligence Service (MCS) performs the function on his behalf. It should be noted that, in accordance with Article 32(4) of the Act on protecting classified information, in case of a motion to initiate a security clearance procedure in order to grant an international organisation security clearance to a person holding a (national) security clearance issued by ISA, MCS, the Intelligence Agency (IA) or the Military Intelligence Service (MIS), a questionnaire completion is not required and an international organisation security clearance is issued only up to the date designated in the national security clearance.

In accordance with the NSA Guidelines, if it is necessary to confirm Polish citizens' capability to protect international classified information, the Head of ISA shall issue a relevant certificate in English. The Head of ISA may also confirm this capability in the way required by the given State or international organisation. Certificates are granted based on a valid appropriate security clearance (NATO, ESA or EU). Persons seconded to services and work abroad and members of permanent and working NATO or EU teams are granted security certificates, referred to as NATO Personnel Security Clearance Certificate or EU Personnel Security Clearance Certificate. Individuals who are assigned to participate in conferences, workshops

and visits to the EU or NATO institutions abroad are granted Certificates of Security Clearance for the period covering the implementation of the task not exceeding the security clearance validity date, provided the international partner requires it. In substantiated circumstances (e.g. an urgent visit abroad), the EU or NATO certificate may be granted based on the valid (national) security clearance certificate issued by ISA, MCS, IA or MIS, authorising an individual to access Polish classified information at a relevant level, and a clearance procedure initiated in accordance with Article 32(4) of the Act on protecting the EU or NATO classified information.

In order to obtain access to the EU or NATO classified information, beside the obligation to hold a security authorisation (or certificate), an individual has to be briefed on the protection of CI and sign a declaration of such training completion and acknowledging effects and consequences of intended and unintended disclosure or use of CI in the way breaching the regulations in force.

Summing up, the Decision 2013/488/EU utilises the experience gained from the application of former Decisions. It contains more synthetic provisions, although also casuistic ones, and can contribute to more efficient protection of EUCI. Due to the use of modern solutions in the regulations of the Act of 5 August 2010 on protecting classified information, there is no need for amendment.

What must be emphasised is a high level of national solutions' convergence with the Council and Commission Decisions as well as NATO standards concerning classified information, although some national solutions demonstrate certain specificity with regard to personnel and industrial security.

Regulation of criminal liability for the commission of crimes against the protection of information (Chapter XXXIII of the Criminal Code) as well as the issue of granting access to classified information in criminal and civil proceedings are subject to the State's assessment.

BIBLIOGRAPHY

Hoc S., *Ochrona informacji niejawnych i innych tajemnic ustawowo chronionych. Wybrane zagadnienia* [Protecting classified information and other secret data under statutory protection: Selected issues], Opole 2006.

Hoc S., *Ochrona informacji niejawnych pochodzących od organów Unii Europejskiej, NATO oraz innych państw* [Protection of classified information of the European Union, NATO and other states], [in:] M. Gajos (ed.), *Ochrona informacji niejawnych i biznesowych. Materiały II Kongresu* [Protection of classified and business information: 2nd Congress material], Katowice 2006.

Hoc S., *Ustawa o ochronie informacji niejawnych. Komentarz* [Act on protecting classified information: Commentary], LexisNexis, Warsaw 2010.

Hoc S., *Ochrona informacji niejawnych Unii Europejskiej* [Protection of European Union classified information], Przegląd Prawa Publicznego No. 10, 2011.

Hoc S., *Ochrona informacji niejawnych wymienianych w interesie Unii Europejskiej* [Protection of classified information exchanged in the interest of the European Union], Przegląd Prawa Publicznego No. 7–8, 2013.

Iwaszko B., *Ochrona informacji niejawnych w praktyce* [Protection of classified information in practice], Presscom, Wrocław 2012.

Ochrona informacji niejawnych: Poradnik praktyczny dla osób i instytucji przetwarzających informacje niejawne [Protection of classified information: Practical guidelines for personnel and agencies processing classified information], Wydawnictwo ABW, Warsaw 2011.

Stankowska I., *Ustawa o ochronie informacji niejawnych. Komentarz* [Act on protecting classified information: Commentary], LexisNexis, Warsaw 2014.

Topolewski S., Żarkowski P. (ed.), *Wpływ ochrony informacji niejawnych i danych osobowych na bezpieczeństwo państwa* [Influence of the protection of classified information and personal data on the security of the state], Wydawnictwo UPH, Siedlce 2016.

Wytyczne ABW w sprawie postępowania z informacjami niejawnymi międzynarodowymi [Internal Security Agency guidelines for processing international classified information], Wydawnictwo ABW, 31 December 2010.

Zalewski S., *Ochrona informacji niejawnych. Wybrane zagadnienia bezpieczeństwa osobowego* [Protection of classified information: Selected aspects of personal security], Wydawnictwo Naukowe NOVUM, Płock 2014.

Zalewski S., *Przepisy odnoszące się do informacji niejawnych w UE i NATO oraz ich implementacji do prawa polskiego* [Regulations regarding classified information in the EU and NATO, and their implementation in Polish law], [in:] G. Szpor (ed.), *Jawność i jej ograniczenia* [Openness and its limitation], Vol. VI: A. Gryszczyńska (ed.), *Struktura tajemnic* [Structure of secrets], C.H. Beck, Warsaw 2014.

Legal regulations and other sources of law

Act on protecting classified information of 5 August 2010, Journal of Laws [Dz.U.] of 2016, item 1167.

Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union of 25 May 2011, Official Journal of the European Union of 8.7.2011, C 202/13, and Journal of Laws [Dz.U.] of 2015, item 2159.

2001/264/EC Council Decision of 19 March 2001 adopting the Council's security regulations, Official Journal of the European Union of 11.4.2001, L 101/1 with subsequent amendments.

2011/292/EU Council Decision of 31 March 2011 on the security rules protecting EU classified information, Official Journal of the European Union of 27.5.2011, L 141/1.

2013/488/EU Council Decision of 23 September 2013 on the security rules for protecting EU classified information, Official Journal of the European Union of 15.10.2013, L 274/1.

Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission, Official Journal of the European Union of 17.3.2015, L 72/41.

Commission Decision (UE, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, Official Journal of the European Union of 17.3.2015, L72/53.

NEW EUROPEAN UNION LAW ON PROTECTING EUROPEAN UNION CLASSIFIED INFORMATION

Summary

The paper presents the EU binding regulations concerning the principles of the EU classified information protection laid down in the Council Decision 2013/488/EU. It refers, first of all, to the definition of classified information, protection, personnel, physical and industrial security, communication and information systems, exchange of classified information, cases of compromising or losing the EU classified information and organisation of security in the Council. Due to Poland's membership in the EU, the knowledge of the issues of the EU classified information protection is essential. It must be pointed out that the Head of the Internal Security Agency is designated to perform the tasks of a National Security Authority.

Key words: accreditation, Decision 2013/488/EU, classified information, security classification, National Security Authority

NOWE PRAWO O OCHRONIE INFORMACJI NIEJAWNYCH UNII EUROPEJSKIEJ

Streszczenie

Przedmiotem rozważań jest aktualna regulacja prawna Unii Europejskiej określająca zasady ochrony informacji niejawnych UE, która została zawarta w decyzji Rady 2013/488/UE. Odniesiono się przede wszystkim do definicji informacji niejawnych, ochrony, bezpieczeństwa: osobowego, fizycznego, przemysłowego, systemów teleinformatycznych, wymiany informacji niejawnych, przypadków naruszenia i narażenia na szwank bezpieczeństwa informacji niejawnych UE, a także organizacji bezpieczeństwa w Radzie. Ze względu na udział Rzeczpospolitej Polskiej w UE znajomość problematyki ochrony informacji niejawnych Unii ma ważne znaczenie praktyczne. Zwrócić przy tym należy uwagę na Krajową Władzę Bezpieczeństwa, której zadania wykonuje Szef Agencji Bezpieczeństwa Wewnętrznego.

Słowa kluczowe: akredytacja, decyzja 2013/488/UE, informacje niejawne, klauzule tajności, Krajowa Władza Bezpieczeństwa