Teka Komisji Prawniczej PAN Oddział w Lublinie
vol. XVIII, 2025, no. 2, pp. 511–521
https://doi.org/10.32084/tkp.10218

PROCESSING OF CLASSIFIED INFORMATION IN THE INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS OF PUBLIC UNIVERSITIES*

Dr. habil. Maciej Rzewuski, University Professor

University of Warmia and Mazury in Olsztyn, Poland
e-mail: maciej.rzewuski@uwm.edu.pl; https://orcid.org/0000-0001-5637-9257

Abstract. The processing of classified information in public universities is a subject that has not attracted considerable interest in the literature. Meanwhile, the role of classified information in administrative, personnel or disciplinary proceedings cannot be overstated. These materials enable proper functioning of the university in administrative and often also civil law transactions. However, improper handling of classified information in these proceedings can have deleterious consequences. For this reason, the knowledge regarding the gathering and use of classified information in practice should be systematically expanded, particularly among university employees who increasingly process such data.

Keywords: classified information; confidential materials; confidentiality clause; processing of classified information; information and communication technology (ICT) system; public university.

INTRODUCTION

The processing of classified information is a complex and multifaceted issue. The volume of classified materials and documents continues to increase in nearly all spheres of social and public life. Classified documents are also handled by public universities, which gather, use, and release classified information for the needs of administrative proceedings.

There is no doubt that access to classified information should be restricted to safeguard its sensitive nature. These postulates are not easy to introduce in practice. The issue is further complicated by the widespread implementation of information and communication technology (ICT) systems in the

* This research paper has been supported by Erasmus + Capacity building in Higher Education project 101179358 – Res-Uni – ERASMUS-EDU-2024-CBHE "Research Universities (Res – Uni)".

ISSN 1899-7694
e-ISSN 2719-7379

public administration. These systems are introduced to expedite university proceedings. However, ICT systems create new challenges for public universities regarding the protection and handling of confidential materials.

The aim of this article was to evaluate the legal regulations applicable to the processing of classified information in the ICT systems of public universities. Given the broad scope of the subject, the analysis was confined to the Polish and German legal systems. The analysis is preceded by several general remarks to highlight the nature and character of classified information in the practice of functioning of public universities.

1. POLISH LEGAL SOLUTIONS

1.1. Definition of Classified Information

The Act of 5 August 2010 on the Protection of Classified Information is the key legal act that establishes the rules for protecting classified information in Poland.[1] Article 1(1) of the above Act sets out the requirements for protecting classified information whose unauthorized disclosure could be damaging or detrimental to the interests of the Republic of Poland, including the rules for the handling and processing of such information, regardless of its form and manner of expression. These provisions outline the rules for assigning a classification level to information, protecting classified information, processing classified information, a security clearance procedure conducted to establish whether the person concerned provides sufficient assurance of secrecy, a procedure aiming to determine whether an entrepreneur is deemed reliable in safeguarding classified information, a procedure for controlling the security status of classified information, protection of classified information in ICT systems, and the application of physical security measures to classified information [Zapart 2020, 114].[2]

According to Article 1(2) PCI Act, the provisions of the act apply to the following individuals and entities: 1) public authorities, in particular the Sejm (the lower house of the Polish Parliament) and the Senate (the upper house of the Polish Parliament), the President of the Republic of Poland, central administration authorities, territorial government authorities, including organizations and departments subordinate to or supervised by these authorities, courts and tribunals, state audit and legal protection bodies; 2) organizations subordinate to or supervised by the Minister of National Defense; 3) National Bank of Poland; 4) state-owned legal entities and entities other than the previously mentioned state organizational units; 5) organizations

[1] Journal of Laws of 2024, item 632 [hereinafter: PCI Act].

[2] Decision of the Voivodeship Administrative Court in Warsaw of 27 April 2020, ref. no. II SA/Wa 2543/19, Lex no. 3058988.

subordinate to or supervised by public authorities; and 6) entrepreneurs intending to apply for or applying for contracts involving access to classified information, entrepreneurs performing such contracts or carrying out tasks that involve access to classified information pursuant to legal provisions.

In the light of Article 1(1) PCI Act, classified information is defined as information whose unauthorized disclosure could be damaging or detrimental to the interests of the Republic of Poland. According to Polish legal scholars, this legal definition has two principal components. The first component is the material element, which requires only that the information has a distinguishing feature whose unauthorized disclosure would or might harm the Republic of Poland or its interests, including during the processing of such information and regardless of its form and manner of expression [Szewc 2007, 115-16; Ziółkowska and Fleszer 2024; Szałowski 2017, 12].[3] The second component is the formal element implying that information does not have to be marked with any of the confidentiality classification categories (levels of sensitivity) provided for by Article 5 of the PCI Act to be deemed as legally protected classified information [Piskorz-Ryń and Wyporska-Frankiewicz 2016, 38-39; Ziółkowska and Fleszer 2024]. In Polish judicature, it is accepted that classified information is protected regardless of whether it was assigned a level of confidentially classification by the respective authority. This type of information is deemed classified on account of the potentially harmful consequences of its content or manner of acquisition, rather than by virtue of a formal confidentiality marking.[4]

1.2. Processing of Classified Information in the Information and Communication Technology Systems of Public Universities

Pursuant to Article 2(5) PCI Act, the processing of classified information is defined as all operations that involve and are based on classified information, in particular the generation, modification, copying, classification, gathering, storage, transfer, and release of such information [Stankowska 2014; Hoc 2010; Szewc 2007, 22]. According to Article 48(1-5) PCI Act, ICT systems intended for processing classified information are subject to security accreditation at least every five years. Security accreditation for an ICT system that processes classified information marked as "confidential" or assigned a higher category is granted by the Internal Security Agency (ABW) or the Military Counterintelligence Service (SKW). An accreditation certificate is issued based on ICT system security documentation approved by the ABW or SKW and the results of a security audit.

[3] Decision of the Supreme Administrative Court of 24 April 2018, ref. no. I OSK 1422/16, Lex no. 2592324.

[4] Decisions of the Supreme Administrative Court of 6 September 2016 (ref. no. I OSK 210/15, Lex no. 2143005) and 6 July 2017 (ref. no. I OSK 932/16, Lex no. 2375583).

A security accreditation certificate issued for an ICT system should contain the following data: name of the issuing agency, date of issue, name of the applicant, name of the organization applying for security accreditation of its ICT system, legal basis, factual and legal reasoning, certificate's validity, as well as the full name, function, and signature of the person authorized to issue the certificate (Article 48(7) PCI Act). The security accreditation certificate for an ICT system intended for processing classified information designated as "restricted" is issued by the head of an organization by approving the ICT system security documentation. If an ICT system is operated by more than one organization, accreditation is granted by the head of the organization managing the system (Article 48(9-10) PCI Act).

Software is an integral part of ICT system, and it must be accredited to prevent unauthorized access to and interference with sensitive data stored in computers and electronic systems [Barczak-Oplustil, Behan, Małecki, et al. 2023, 5; Mikowski 2016, 200]. According to the literature, security measures are implemented both before and during data processing in an ICT system or network, in the following stages: 1) planning – designing the intended purpose of an ICT system, the maximum confidentiality marking of classified information processed in an ICT system, security mode of operation of an ICT system, estimated number of users, and the system installation site; 2) design – preliminary assessment of the risk to the security of classified information with the aim of determining security requirements, selecting the most appropriate security solutions based on the results of the preliminary risk assessment, developing an accreditation plan detailing the scope and schedule of accreditation tasks in agreement with the accreditation authority, determining the required type and number of cryptographic devices and tools, as well as the manner of their use, in agreement with the supplier of cryptographic keys, and identifying special security requirements that are then specified in a protocol; 3) implementation – acquisition and implementation of security devices or tools for an ICT system, conducting system security tests, assessing the residual risk to classified information after the implementation of security devices or tools, development of a safe operation protocol, identification of additional security requirements, and acquisition of security accreditation for an ICT system; 4) operation – an ICT system's compliance with security documentation is monitored; ICT security risks are managed on a regular basis; security tests are conducted periodically to validate the effectiveness of security solutions and resolve the identified problems; the ICT system and security documentation are regularly updated, and any modifications that could affect ICT system security have to be approved by the accreditation authority; 5) decommissioning – the decommissioning of an ICT system must be reported in writing to the ABW or SKW; the accreditation certificate issued for an ICT system intended

for processing classified information marked as "confidential" or assigned a higher category is returned to the ABW or SKW; classified information is removed from the ICT system, in particular by transferring classified information to another ICT system, archiving data, or destroying data carriers [Ziółkowska 2024a].

Therefore, an ICT system security accreditation certificate protects classified information not only against malware, but also against any incidents that could potentially result in unauthorized access to confidential materials [Gwardzińska 2011, 31].

According to the Polish legislator, electromagnetic protection measures for safeguarding classified information marked as "confidential" or assigned a higher category have to be audited and evaluated by the ABW or SKW as part of the security accreditation process. Cryptographic devices and tools for the protection of classified information are also audited and evaluated as part of the security accreditation process (Article 50 PCI Act). The main aim of electromagnetic protection measures is to safeguard classified information and prevent unauthorized access to such data. These goals are achieved by assessing the security risks to classified information and selecting the most appropriate electromagnetic protection measures. For this purpose, protocols are implemented for creating and storing backup copies, handling classified information in crisis situations and during ICT system failures, and monitoring the operational status of ICT systems. Alternative connections, devices, and power sources are used to ensure uninterrupted access to ICT system resources [Ziółkowska 2024b].

According to the Polish legislator, to ensure effective electromagnetic protection, ICT systems processing classified information must be located within a Hardware Electromagnetic Protection Zone (HEPZ). This procedure is initiated by submitting a request with the ICT Security Department of the ABW or SKW. Hardware zones 0, 1, and 2 must be also created to specify the categories of hardware required to ensure electromagnetic protection. The ABW or SKW issues a certificate for every HEPZ. The certificate states the number of the HEPZ and the category of hardware required in a specific zone [Kij 2017]. The ABW issues certificates[5] for the following types of devices and tools: 1) electromagnetic protection measures, including shielded enclosures and HEPZ – an electromagnetic protection certificate is issued for a specific protection device or HEPZ; 2) cryptographic devices or tools: a cryptographic protection certificate designated with the letter 'T' is issued for a specific type or model of a cryptographic

[5] Decision No. 35 of the Head of the Internal Security Agency of 3 August 2021 on the certification of devices, tools, and measures for the protection of classified information (Official Journal of the Internal Security Agency, item 8).

device or tool that is intended for protecting classified information marked as "confidential" or assigned a higher category; a cryptographic protection certificate designated with the letter 'Z' confirms that a cryptographic device or tool with a valid 'T' certificate complies with the applicable requirements for protecting classified information; a cryptographic protection certificate is issued for a cryptographic device or tool that is intended for protecting information marked as "restricted"; 3) devices or tools used for safeguarding ICT systems – an ICT security certificate is issued for a device or tool designed for safeguarding an ICT system [Ziółkowska 2024b].

All devices, tools, and measures that are intended for protecting classified information and covered by a HEPZ certificate are subject to legal protection until they are destroyed or decommissioned.

2. GERMAN LEGAL SOLUTIONS

2.1. Definition of Classified Information

The General Administrative Regulation on the Material Protection of Classified Information of 13 March 2023[6] (Classified Information Directive, VSA) is the principal normative act setting out the rules for the handling of classified information in the Federal Republic of Germany. Pursuant to para. 1(1) VSA, the Classified Information Directive is addressed to federal authorities and federal public law institutions that have access to classified information, as well as to their employees who have access to classified information or perform duties that may entail such access. The German authorities are required to apply exclusively the Classified Information Directive in their dealings with the Bundestag and Bundesrat [Mickiewicz 2024, 175].

In para. 2(1) VSA, classified information is defined as facts, items, or findings, in any form of expression (such as documents, drawings, charts, maps, photocopies, photographic materials, electronic files, data carriers, electrical signals, devices, instruments, technical installations, and the spoken word) that are deemed confidential in the public interest, in particular to safeguard the security of the Federal Republic of Germany and its federal states. Trade secrets, business secrets, invention-related secrets, tax-related and other personal secrets and other matters pertaining to personal life may

[6] *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung)*, adopted pursuant to Article 86 sentence 1 of the Basic Law in conjunction with § 35(1) of the Security Clearance Act of 20 April 1994 (Federal Law Gazette I, p. 867), in conjunction with § 1(2) of the Competence Adjustment Act of 16 August 2002 (Federal Law Gazette I, p. 3165), and the Organizational Decree issued by the Federal Chancellor of 8 December 2021 [hereinafter: VSA].

also be regarded as confidential in the public interest. The wording of the cited regulation clearly indicates that in the German legal system, classified information is a broad concept that extends to various spheres of public life, including the exercise of justice and the functioning of the justice system.

In Germany, access to classified information is also regulated by the Act on the Preconditions and Procedure for Federal Security Clearances and the Protection of Classified Information of 20 April 1994 (Security Clearance Act, SÜG).[7] Pursuant to para. 1(1) SÜG, the Act regulates the prerequisites and conditions for a security vetting procedure involving a person who will be granted (initial security clearance) or has already been granted access to sensitive information (repeat security clearance) by the respective authority, as well as the protection of classified information. Any person whose duties will involve access to sensitive data (participant in the procedure) must first undergo a security clearance. Such proceedings require the participant's consent, unless otherwise provided by law. A person whose duties involve access to sensitive data must be at least 16 years of age (para. 2(1) SÜG).

2.2. Processing of Classified Information in the Information and Communication Technology Systems of Public Universities

Pursuant to the general provisions of the VSA concerning the use of ICT systems, institutions and authorized entities must ensure that ICT systems intended for processing classified information remain secure during their entire life-cycle – from the moment an ICT system is implemented to process classified information until the moment such information is removed from the repository of classified data (para 49(1)). These systems are applied to process classified information marked as "confidential" or assigned a higher category. The processing of such information should be preceded by a risk analysis based on the standards developed by the Federal Office for Information Security (BSI) (para. 49(2)) [Mickiewicz 2024, 179-80].

According to the German legislator, classified information may be processed only in ICT systems that have been approved for such use. For such approval to be granted, an ICT system must comply with the data security standards implemented by the BSI, and its compliance must be formally documented. The implemented data security measures are regularly audited by the BSI for compliance with the requirements of the Federal Ministry of the Interior and Community based on the risks specified in § 4a of the Act on the Federal Office for Information Security[8] (para. 50 (1-2) VSA).

---

[7] *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz)*, Federal Law Gazette I, p. 867 [hereinafter: SÜG].

[8] *Gesetz über das Bundesamt für Sicherheit in derInformationstechnik (BSI-Gesetz –BSIG)*, https://www.gesetze-im-internet.de/bundesrecht/bsig_2009/gesamt.pdf [accessed: 12.08.2025].

The following security requirements must be also met for authorization to be granted: a) access is granted solely on a need-to-know basis – *Kenntnis nur, wenn nötig* (para. 3(1-2) and para. 58(1.2) VSA); b) the rules concerning the classification and marking of classified information must be observed (para. 15(1), para. 17 (1), para. 18 (2), para. 19 and para. 20(2) VSA); c) classified information must be administered and documented (para. 21 VSA); d) the rules concerning the (temporary) storage of classified information must be observed (para. 23 VSA); e) the security of ICT networks for processing confidential information must be guaranteed during their entire life-cycle (para. 49(1) VSA); f) classified information must be removed from databases and destroyed (para. 30 and para. 56 VSA); g) the guidelines on the transmission of classified information via communication channels must be observed (para. 55 VSA); h) the rules concerning supranational and international organizations and bilateral agreements on information security must be observed (para. 34 and 35 VSA); i) security accreditation must be accomplished (para. 36 VSA).

The BSI issues detailed requirements in the classified information security module included in the basic protection of ICT systems. In individual cases, information security officers may introduce additional data security requirements to comply with the provisions of national and international regulations concerning the handling and processing of classified information marked as "confidential" or assigned a higher category. Before an ICT system is approved for use, the effectiveness of the implemented information security measures must be verified (for example, by external auditors), and the results must be documented (para. 50(3) VSA).

According to para. 53(1) VSA, all transmission devices, lines, and distributors that carry classified information in non-encrypted format must be protected against unauthorized access. Information technology systems that process classified information categorized as classified information for official use only must be protected within facilities and zones that are as a rule protected against unauthorized access (para. 53(2) VSA). Information technology systems that process classified information marked as "confidential" must be protected within facilities and zones that are as a rule protected against unauthorized access (para. 53(3) VSA). The effectiveness of the safeguards in areas situated outside the protected facilities and zones stipulated in para. 53(2-3) VSA must be additionally verified by information security officers.

The provisions of para. 45 VSA deal with the facilities and zones in which ICT systems for processing classified information are located. Classified information marked as "confidential" or assigned a higher category is administered and processed in these facilities and zones. These premises should be located in security zones or should be declared as security zones within the meaning

of para. 39(3) VSA,[9] and they should be adequately protected against unauthorized access. Information security officers select the appropriate security measures for facilities and zones where classified information categorized as classified information for official use only is processed by ICT systems.

The means of entry and access to work areas where classified information is processed, security zones, premises where classified information is stored, facilities protected against technical eavesdropping, ICT systems for processing classified information marked as "confidential" or assigned a higher category, and technical monitoring systems for classified information must be adequately protected against unauthorized access. As a rule, such means should be kept in personal custody during working hours and locked away in a secure data storage facility or a key container at the end of the workday. Where possible, key containers and safes should be monitored. The keys to secure data containers and storage rooms should remain in the personal custody of the respective user of such containers and rooms (para. 46(1-2) VSA). The location where the means of entry and access are kept shall be known only to authorized personnel. The means of entry and access must be changed in the following circumstances: 1) before first use, 2) when there is a change in authorized personnel, 3) after use in the absence of authorized personnel, 4) when there is suspicion that the means of entry and access have been compromised, 5) at least every twelve months (para. 46(3) VSA).

Backup means of entry and access should be provided for emergency situations. They should be stored in labeled and sealed envelopes, separately from the means of entry and access that are currently in use, in the appropriate containers for classified information (para. 46(5) VSA).

In Germany, the processing of classified information is closely linked with the use of cryptographic means. Cryptographic means (national or domestic) are defined as products and devices with the associated documentation, as well as the cryptographic keys for encryption, decryption, and transmission of information, which are designated as such by the BSI, or – within the jurisdiction of the Federal Ministry of Defense – by the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (para. 59(1) VSA). Classified cryptographic means shall be marked with the warning "KRYPTO" (cryptographic security) or "CRYPTO" (cryptosecurity). Cryptographic devices that have not been classified, the

[9] Pursuant to this provision, if necessitated by the scope and significance of classified information that is handled in a given location, the competent highest federal authority – acting in agreement with the Federal Ministry of the Interior and Community – must establish security zones within the agency or other public federal bodies (or parts thereof). These zones must be protected by personnel, organizational, and technical measures to prevent unauthorized access. Access is permitted only in locations with reliable access control. Security zones may comprise single rooms, multiple rooms, entire buildings, or groups of buildings.

associated cryptographic components and other associated modules performing security-sensitive functions shall be marked with the warning "CCI" (Controlled COMSEC Item). It should be noted that certification is required for all cryptographic means, and the certification process must comply with the rules applicable to the certification process of classified information marked as "confidential" or assigned a higher category (para. 59(2-3) VSA).

According to para. 60 VSA, the BSI is assigned the role of the Civil National Distribution Authority (CNDA) with regard to the tasks associated with the central documentation, administration, and distribution of cryptographic means. In turn, the Bundeswehr Information Technology Center performs the duties of the Military National Distribution Authority. German authorities and institutions operating cryptographic means shall appoint at least one cryptographic means administrator and one representative authorized to administer cryptographic means. These persons must possess the required specialist knowledge to perform the assigned tasks (para. 61(1) VSA). The personnel who have been granted access to cryptographic means shall receive instructions from the information security officer, in accordance with the model presented in Annex VIII to the VSA, and must receive authorization to operate cryptographic means (para. 62 VSA).

CONCLUSIONS

The processing of classified information faces many practical challenges, which are further compounded by the pervasive implementation of ICT systems across nearly all areas of public life. The above applies increasingly to public universities. In practice, most changes are introduced with the aim of expediting administrative, personnel or disciplinary proceedings, but employees of public universities generally have limited knowledge about the processing of classified information that is presented and used in these proceedings, particularly if that information is processed using ICT systems. It is reasonable to conclude that the implementation of new ICT systems and instruments should always be accompanied by adequate personnel training and followed by periodic verification of the competencies required for processing classified information. Compliance with both requirements should satisfy national legislative postulates regarding expedited administrative proceedings at public universities, ensure the secure handling of classified materials, and protect classified information against unauthorized use.

REFERENCES

Barczak-Oplustil, Agnieszka, Adam Behan, Mikołaj Małecki, et al. 2023. "Pegasus w Polsce: niedopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych." *Czasopismo Prawa Karnego i Nauk Penalnych* 1:5-41.

Gwardzińska, Ewa. 2011. "Bezpieczeństwo teleinformatyczne informacji niejawnych." *Kwartalnik Nauk o Przedsiębiorstwie* 3:25-31.

Hoc, Stanisław. 2010. "Komentarz do art. 42." In *Ustawa o ochronie informacji niejawnych. Komentarz*. Warszawa: Wolters Kluwer.

Kij, Karol. 2017. "Obowiązek wyznaczenia Sprzętowej Strefy Ochrony Elektromagnetycznej (SSOE)." https://www.bezpieczneit.com/ochrona-elektromagnetyczna-wyznaczenie-sprzetowej-strefy-ochrony-elektromagnetycznej-ssoe/ [accessed: 03.08.2025].

Mickiewicz, Piotr. 2024. "Ewolucja niemieckiej polityki bezpieczeństwa cybernetycznego w latach 2011–2024." *Rocznik Integracji Europejskiej* 18:175-88.

Mikowski, Rafał. 2016. "Bezpieczeństwo fizyczne informacji niejawnych." Ze*szyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych* 9:199-213.

Piskorz-Ryń, Agnieszka, and Joanna Wyporska-Frankiewicz. 2016. "Dostęp do informacji publicznej a ochrona informacji niejawnych. Zagadnienia wybrane." *Zeszyty Naukowe Sądownictwa Administracyjnego* 4(67):35-59.

Stankowska, Iwona. 2014. "Komentarz do art. 42." In *Ustawa o ochronie informacji niejawnych. Komentarz*. Warszawa: Wolters Kluwer.

Szałowski, Ryszard. 2017. "Uwagi o ustawowej regulacji zakresu przedmiotowego informacji niejawnych." *Administracja. Teoria. Dydaktyka. Praktyka* 1:12-35.

Szewc, Tomasz. 2007. *Ochrona informacji niejawnych. Komentarz*. Warszawa: C.H. Beck.

Zapart, Robert. 2020. "Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji." *Polityka i Społeczeństwo* 18(3):124-43.

Ziółkowska, Agnieszka. 2024a. "Komentarz do art. 48." In *Ochrona informacji niejawnych. Komentarz*, edited by Agnieszka Ziółkowska. Warszawa: Wolters Kluwer.

Ziółkowska, Agnieszka. 2024b. "Komentarz do art. 50." In *Ochrona informacji niejawnych. Komentarz*, edited by Agnieszka Ziółkowska. Warszawa: Wolters Kluwer.

Ziółkowska, Agnieszka, and Dorota Fleszer. 2024. "Komentarz do art. 1." In *Ochrona informacji niejawnych. Komentarz*, edited by Agnieszka Ziółkowska. Warszawa: Wolters Kluwer.