Małgorzata Czuryk*

Special rules of remuneration for individuals performing cybersecurity tasks

Abstract

Effective support for measures to protect ICT systems against cyberthreats is possible through the use of appropriate incentive schemes to motivate people hired by entities concerned with matters of cybersecurity. One such incentive involves an ICT benefit, paid from the Cybersecurity Fund managed by the minister competent for computerisation.

Key words: cybersecurity, remuneration, ICT benefits

* Assoc. Prof. Małgorzata Czuryk, PhD, Faculty of Law and Administration University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

Remuneration (pay) for the performance of cybersecurity tasks may be increased to include an ICT benefit on the account of high qualifications. This benefit, paid as a salary bonus (in the case of employees) or as a cash benefit (in the case of public officers and professional soldiers), may be granted to individuals charged with ensuring cybersecurity at entities defined by legislators. The performance of these tasks alone does not create any entitlement to special treatment in terms of remuneration. For an ICT benefit to be paid, two requirements must be cumulatively met. These are: 1) the performance of cybersecurity tasks; 2) employment or service at specific entities. ICT benefits are paid from the Cybersecurity Fund.

Polish legislators define cybersecurity as the resilience of information systems against actions which compromise the confidentiality, integrity, availability, and authenticity of processed data, or the related services provided by such information systems[1]. EU legislators use a similar definition of cybersecurity (security of network and information systems), understanding it as the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems[2].

The aim of the Cybersecurity Fund, from which ICT benefits and related costs are paid and covered, is to support measures to protect ICT systems

1 Art. 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2020, item 1369, as amended), further referred to as the NCSA.

2 Art. 4(2) of the Directive of the European Parliament and Council (EU) (2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2016, L 194, p. 1). For more on cybersecurity see: K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, ibidem 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *Activities of local government units in the scope of telecommunication*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, ibidem 2020, no. 2; I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, ibidem.

against cyberthreats[3]. An ICT system is a system of cooperating IT equipment and software designed to ensure the processing, storage, transmission and receipt of data via ICT networks using an ICT end device that is suitable for a given type of network[4].

Pursuant to Art. 2(2) of the ASRR, the Cybersecurity Fund is a state earmarked fund, which is established under an act. Its revenues come from public funds, and its costs are incurred for pre-defined state tasks. A state earmarked fund does not have a legal personality. It is a separate bank account managed by the minister defined in the act under which the fund is created, or by another authority named in that act[5]. The State Treasury is liable for the fund's obligations, and one other consequence of its lack of legal personality is that its legal subjectivity is restricted to the budget sphere[6].

The Cybersecurity Fund is managed by the minister competent for computerisation. The computerisation division includes matters related to: 1) the computerisation of public administration and entities performing public tasks; 2) ICT systems and networks of public administration; 3) supporting investment in computerisation; 4) the fulfilment of the Republic of Poland's international computerisation and ICT-related obligations; 5) involvement in shaping the EU's computerisation policies; 6) the development of an information society and counteracting digital exclusion; 7) the development of services provided by electronic means; 8) the shaping of security policy in relation to personal data protection; 9) telecommunications; 10) cyberspace security in the civilian dimension; 11) the national PESEL register (Universal Electronic System for the Registration of Population), the ID Cards Register, the Civil Status Registry and the Central Register of Issued and Cancelled Passport Documents; 12) the vehicle, driver, and car park card holders registers; 13) supervision over the provision of trust services; 14) electronic identification[7].

3 Art. 2(1) of the Act of 2 December 2021 on the Special Rules of Remuneration for Individuals Performing Cybersecurity Tasks (Journal of Laws 2021, item 2333, as amended), further referred to as the ASRR.

4 Art. 3(3) of the Act of 17 February 2005 on the Computerisation of Entities Performing Public Tasks (consolidated text, Journal of Laws 2021, item 2070, as amended).

5 Art. 2(29) of the Public Finance Act of 27 August 2009 (consolidated text, Journal of Laws 2021, item 305, as amended).

6 W. Bożek, P. Mańczyk, [in:] *Ustawa o finansach publicznych. Komentarz*, ed. Z. Ofiarski, Warszawa 2020, Art. 29.

7 Art. 12a of the Act of 4 September 1997 on government administration departments (consolidated text, Journal of Laws 2021, item 1893, as amended).

Pursuant to Art. 3 of the ASRR, in order to seek Cybersecurity Fund support, a request must be made by the relevant entity to the minister competent for computerisation. The request must include: 1) a detailed description of cybersecurity tasks, including the number of people performing individual tasks; 2) a statement by the manager of the requesting entity that the requirements are met; 3) a statement of the maximum amount of the projected costs associated with the provision of the ICT benefit; 4) the date on which the ICT benefit funds are expected to be received. Such requests are made once a year, and they must be submitted by 31 August of the year preceding the payment of the ICT benefit. Requests submitted past this date are not accepted. If the request is found to be formally deficient, the minister competent for computerisation requires that the requesting entity resolves any deficiencies within seven days. Failing this requirement, the request is not subject to consideration. If the request contains an obvious typing error, the minister competent for computerisation corrects such an error on an ex-officio basis, and notifies the requesting entity of such a correction, or requires the requesting entity to correct the error within seven days. Upon failing this requirement, the request is not subject to consideration.

Pursuant to Art. 4 of the ASRR, the minister competent for computerisation provides formally compliant requests to the Cybersecurity Matters Board for assessment[8]. Following the request approval of the Cybersecurity Matters Board, the minister provides money from the Cybersecurity Fund for the payment of the ICT benefit for a given calendar year within the time limit stated in the request. The benefit is granted subject to a positive assessment by the Cybersecurity Matters Board. In other words, the assessment issued by the Cybersecurity Matters Board is binding for the minister competent for computerisation. Cybersecurity Fund money may not be paid for an ICT benefit in the event of a negative assessment.

As stipulated by Art. 5 of the ASRR, a salary bonus, or a cash benefit in the case of public officers and professional soldiers (ICT benefit), may be granted to individuals who perform their tasks: 1) in the following authorities,

8 In accordance with Art. 64 of the NCSA, the Cybersecurity Matters Board operates under the Council of Ministers as an assessment and advisory body concerned with cybersecurity and cybersecurity operations carried out by CSIRT MON, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams and authorities competent for cybersecurity. The Board formulates its stance (assessment) through a voting procedure, M. Nowikowska [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 321.

bodies and entities: a) CSIRT teams; b) cybersecurity authorities; c) sectoral cybersecurity teams; d) in the capacity of the Government's Cybersecurity Plenipotentiary; 2) related to ensuring cybersecurity at: a) the Internal Security Agency; b) the Foreign Intelligence Agency; c) the Central Anticorruption Bureau; d) organisational units subordinate to the President of the Council of Ministers or ministers; e) the Chancellery of the President of the Council of Ministers and at agencies supporting ministers; f) the Chancellery of the President of the Republic of Poland; g) the Chancellery of the Sejm; h) the Chancellery of the Senate; i) the Police; j) the Prosecutor's Office; k) the Military Counterintelligence Service; l) the Military Intelligence Service; m) the Border Guard; n) and the State Protection Service. The catalogue of entities whose employees or functionaries may receive an ICT benefit is restricted. Accordingly, the benefit may not be granted to individuals who perform cybersecurity tasks but who are not employed or on duty at these entities, even if their tasks are highly important in terms of state security. This solution is ill-considered to some extent, since it fails to include a range of individuals who work outside the entities listed in Art. 5 of the ASRR but whose tasks are important in terms of countering cyberthreats.

As stipulated by Art. 7 of the ASRR, the amount of remuneration including bonuses, or the amount of salary including bonuses, along with the ICT benefit, may not exceed twenty-one times the base amount for members of the civil service corps. The ICT benefit is granted annually for the period of cybersecurity task performance. Should the entity obliged to pay the ICT benefit not receive the funds for this purpose, the benefit may not be paid. ICT benefits are granted and cancelled by the manager of the entity at which individuals performing cybersecurity tasks are employed or on duty as public officers or professional soldiers. Individuals performing cybersecurity tasks forfeit their right to ICT benefits after: 1) receiving a penalty for a breach of order or a disciplinary penalty; 2) being unjustifiably absent from work for at least two days; 3) showing up at work intoxicated or under the influence of alcohol or other psychoactive substances; 4) being caught drinking alcohol or using psychoactive substances at work or on duty; 5) leaving a place of work or duty without justification.

The ICT benefit is not taken into consideration when determining the amount of annual remuneration. Annual remuneration is set at 8.5% of the amount of remuneration received by the employee in the calendar year for which that remuneration is due, taking into account remuneration and other work employment-relationship benefits taken as a basis to calculate the cash equivalent for vacation leave, as well as remuneration for vacation leave

and remuneration for redundant time due to employees who have resumed working after being reinstated[9].

Legislators have defined specific cybersecurity tasks and have divided them into groups. They also specified the required professional experience along with the condition to have expert knowledge on cybersecurity to perform necessary tasks in individual groups, and stated the brackets for ICT benefit amounts in conjunction with the group division of cybersecurity tasks. Specific cybersecurity tasks defined by legislators include: 1) cyberthreat intelligence and threat hunting; 2) malware analysis; 3) security and vulnerability testing, hardware and software testing; 4) information system security assessment, including penetration testing and security audits; 5) conducting expert cybersecurity analyses and identifying new vulnerabilities; 6) developing specialised technical tools to support cybersecurity tasks; 7) managing an organisational unit or sub-unit designated to perform cybersecurity tasks; 8) engaging in preventative measures to increase cybersecurity; 9) engaging in advanced measures to actively protect IT systems; 10) advanced incident handling; 11) post-breach analysis; 12) the testing and assessment of the security of ICT solutions; 13) the designing, construction and maintenance of incident monitoring and detection systems and functional support for the security operational centre (SOC), the Computer Security Incident Response Team (CSIRT); 14) data correlation, analyses and situational mapping; 15) monitoring cyberthreats and incidents at the national level; 16) analyses of major incidents, connections between incidents and formulating conclusions; 17) registering and handling major incident notifications; 18) responding to and classifying incidents; 19) analysis and management as part of the response to identified hardware and software vulnerabilities; 20) coordinating support for reported incidents; 21) handling notifications and analysing the content of cases involving the distribution, dissemination or transmission of child pornography using ICT technology; 22) specialised tasks within SOC or NOC, including: security monitoring (log analysis and correlation), the identification and preliminary handling of incidents; 23) cybersecurity risk estimation; 24) the development and deployment of business continuity and reconstruction plans, and of the information security management system; 25) supervision over cybersecurity risk estimation; 26) preparing cybersecurity

9 Art. 4(1) of the Act of 12 December 1997 on Additional Annual Remuneration for Employees of Public-Budget Units (consolidated text, Journal of Laws 2018, item 1872, as amended).

recommendations, standards and good practices, especially to increase the security of information systems at the disposal of entities within the national cybersecurity system; 27) the ongoing maintenance and development of internal significant information systems; 28) searching for known hardware and software vulnerabilities in supervised ICT systems; 29) preliminary incident handling; 30) securing digital traces; 31) identifying cyberthreats; 32) identifying and handling investigations involving the operators of essential services; 33) supervision over entities within the national cybersecurity system; 34) supervision over entities providing cybersecurity services; 35) conducting cybersecurity awareness campaigns, in particular the organisation of exercises and training courses; 36) conducting analyses of the functioning of the national cybersecurity system, including legal, organisational, standard and certification-related solutions in the area of cybersecurity, including drafts of normative acts; 37) conducting analyses to determine whether sector or sub-sector entities meet the requirements for being operators of essential services; 38) conducting inspections on entities within the national cybersecurity system, including cybersecurity service providers; 39) domestic and international cooperation in the area of cybersecurity[10].

It should be noted that the ICT benefit provides an incentive not only to work (or to serve on duty) more efficiently in entities performing cybersecurity tasks, but also to prevent cybersecurity experts from leaving for the private sector due to the better financial opportunities it may offer.

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2.

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

10 Regulation of the Council of Minister of 19 January 2022 on the Amount of the ICT Benefit for Individuals Performing Cybersecurity Tasks (Journal of Laws 2022, item 131).

Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Ustawa o finansach publicznych. Komentarz, ed. Z. Ofiarski, Warszawa 2020.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Szczególne zasady wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa

Streszczenie

Skuteczne wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami jest możliwe przy zastosowaniu odpowiednich mechanizmów motywujących osoby zatrudnione lub pełniące służbę w podmiotach zajmujących się sprawami cyberbezpieczeństwa. Jednym z takich motywatorów jest świadczenie telekomunikacyjne, wypłacane z Funduszu Cyberbezpieczeństwa, którego dysponentem jest minister właściwy do spraw informatyzacji.

Słowa kluczowe: cyberbezpieczeństwo, wynagrodzenie, świadczenie teleinformatyczne