Chapter III

Legal Bases for the Operation of E-government in Poland

MIROSŁAW KARPIUK & JAROSŁAW KOSTRUBIEC

Abstract The processing of cases by the public administration electronically is now a standard, not the future, although there is still a lot to do in this regard. Today it is difficult to imagine a public administration detached from the digital sphere. Modern administration is an e-government using new technologies to carry out the tasks assigned by the legislature. Particular attention should be paid to the process of informatization of the activities of bodies performing public tasks, including the need to adapt the ICT systems used to carry out such tasks, which should be highly resistant to interference. An important element in the functioning of such administration is also the exchange of information by electronic means, including electronic documents, between public entities and other actors, including citizens for whom e-government operates. In addition to the informatization of public administration activities, attention should also be paid to its digital accessibility, support for the development of telecommunications services and networks, including in the area of local government, the tasks of the Minister responsible for informatization, administrative e-proceedings, or cybersecurity issues. All these elements determine the status of e-government as a tool for meeting social needs.

Keywords: • e-government • information systems • informatization • cybersecurity

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, Ph.D., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl. Jarosław Kostrubiec, Ph.D., Dr. Habil. Associate Professor, Maria CurieSkłodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, ORCID: 0000-0003-1379-9846, e-mail: jaroslaw.kostrubiec@mail.umcs.pl.

https://doi.org/10.4335/2026.1.3 ISBN 978-961-7124-29-3 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

In the age of information society and digital government, public administration has faced new challenges to adapt not only to the requirements of a modern governance, but also to the needs of the information society, including communication with office personnel via the Internet. Remote handling of cases should not be an exception but rather, on the contrary, the standard of operation of the public administration enabling stakeholders to contact quickly, without having to appear in the office in person.

An efficient and open public administration is where the state's organisational and management system is characterised by a high quality of public services, internal computerisation and professionalism. The degree of openness of the public administration is also evidenced by the digital competences of the society (Karpiuk, Chałubińska-Jentkiewicz, 2015a: 102). The digital society forces the administration to switch from a conventional model to an electronic model, where most public services are provided electronically. However, the digitally excluded must be still taken into account, as they must also have access to the services provided by the public administration.

The solutions being implemented for the functioning of modern e-government ensure the provision of e-services through different ICT platforms. The emerging opportunities for the development of this sphere of public life inevitably face various problems and barriers (Romaniuk, 2022: 464). Electronic exchange of services in the global economy is becoming increasingly important, but giving rise to previously unknown risks. This phenomenon is linked to the ever-increasing exchange of information and the emergence of goods and services that can be purchased through ICT networks (Karpiuk, Chałubińska-Jentkiewicz, 2015b: 121).

Owing to information systems, the e-government has new capabilities to be employed to perform public tasks, but it is still important to ensure that appropriate safeguards are applied when using these systems so that disruptions do not compromise the continuity and quality of these tasks.

In an era when information systems form the foundation of many areas of public life, or are an instrument supporting public activities, they both need to respond to the dynamics of change and be properly protected (Karpiuk, 2023: 50). The development of new technologies indeed contributes to streamlining the provision of public services, but also makes cyber threats more and more dangerous. Therefore, information systems used by public administrations must be more resilient to cyberattacks restricting access to services provided through them.

2 Informatization of the activity of public administration

Informatization is not only a dynamic, but also continuous and indispensable process. It is nowadays impossible to govern correctly without a properly developed IT infrastructure, which is very important for the operation of public administration. Widespread informatization covers the public sector, which must operate effectively, efficiently, quickly and fairly, reaching the widest possible range of beneficiaries. It is a process that allows an improvement of the implementation of public tasks, or a wider access to information, while reducing the costs of public administration operation (Chałubińska-Jentkiewicz, Karpiuk, 2015: 425).

As stated in Article 13 of the Act of 17 February 2005 on informatization of the activities of entities performing public tasks (consolidated text Journal of Laws of 2023, item 57 as amended), – hereinafter referred to as the Informatization Act, the public entity uses for the performance of the public tasks ICT systems which meet the minimum requirements provided for these systems, including ensuring their interoperability, while ICT systems used for scientific and educational purposes do not have to meet these requirements. The ICT system is defined in Article 3(3) of the Informatization Act as a set of interoperating IT hardware and software ensuring the processing, storage, transmission and reception of data by telecommunications networks using a terminal equipment appropriate for a given type of telecommunications network, thus, as follows from Article 2(43) of the Act of 16 July 2004. Telecommunications Law (consolidated text Journal of Laws of 2022, item 1648 as amended), - telecommunication equipment to be connected directly or indirectly to network terminations. The minimum requirements for ICT systems, according to Article 3 (9) of the Informatization Act, are a set of organizational and technical requirements, the fulfilment of which by the ICT system used for the performance of public tasks enables the exchange of data with other ICT systems used for the performance of public tasks and ensures access to the information resources made available by these systems. Interoperability, on the other hand, is, as defined in Article 3(18) of the Informatization Act, the ability of various entities and ICT systems and public registers used by them to cooperate in order to achieve mutually beneficial and agreed objectives, taking into account the sharing of information and knowledge by the business processes supported by them and implemented using data exchange through the ICT systems used by those entities.

Interoperability – according to § 4 of the Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and exchange of information in electronic form and minimum requirements for ICT systems (consolidated text Journal of Laws of 2017, item 2247) – is achieved by: 1) unification, understood as the use of compatible norms, standards and procedures by various entities performing public tasks, or 2) interchangeability, understood as the possibility of substituting a product, process or service without simultaneous interference with the exchange of information between entities performing

public tasks or between these entities and their customers, while meeting all the functional and non-functional requirements of the interoperating systems, or 3) compatibility, understood as the suitability of products, processes or services intended for joint use, under specific conditions ensuring the fulfilment of the relevant requirements and in the absence of undesired effects. The application of the above rules depends on the circumstances arising from the risk assessment and the characteristics of the ICT system being designed, its extent and the solutions available on the IT supplies and services market. It should be emphasised, however, that the way in which interoperability is achieved by the entity performing public tasks must not breach the principle of technological neutrality.

A number of administrative entities maintain public registers, defined in Article 3(5) of the Informatization Act as registers, records, lists, inventories or other forms of records, serving the performance of public tasks, maintained by a public entity. The public entity is obliged to: 1) maintain the register in a manner that ensures that the minimum requirements for ICT systems are met, where the register operates using ICT systems; 2) maintain the register in accordance with the minimum requirements for public registers and the exchange of information in electronic form; 3) enable information to be provided to this register and information from this register to be made available electronically, where the register operates using ICT systems. This obligation stems from Article 14 of the Informatization Act. Keeping records of various aspects of the public administration's operation facilitates considerably the performance of its tasks and enables direct access to the database it holds, which also applies to sharing the information contained therein.

According to Article 15 of the Informatization Act, an entity maintaining a public register shall provide a public entity or a non-public entity carrying out public tasks with free access to the data collected in the register, to the extent necessary for the performance of those tasks. These data should be made available by electronic means and used for the performance of public tasks. A means of electronic communication is understood in Article 2(5) of the Act of 18 July 2002 on the provision of services by electronic means (consolidated text Journal of laws of 2020, item 344 as amended) as technical solutions, including ICT equipment and software tools interoperating with them, enabling individual distance communication using data transmission between ICT systems, including in particular e-mail.

The request for access to the data collected in the register – as is apparent from § 2 of the Ordinance of the Council of Ministers of 27 September 2005 (consolidated text Journal of laws of 2018, item 29) – contains: 1. the name of the entity requesting access to the data collected in the register and the address of its office; 2. the name of the requested entity; 3. the identification of the register in which the data to be made available are collected; 4. specification of the public task and the legal basis for its performance by the entity requesting access to the data stored in the register, the performance of which requires that the data be made available; 5. specification of the extent of the data requested

and the manner in which it is made available; 6. specification of the period during which the data are made available; 7. a declaration of the entity applying for access to the data collected in the register that the data will be used exclusively for the performance of a public task; 8. a statement of compliance by the entity requesting access to the data stored in the register with the technical and organisational security conditions necessary for access to that data; 9. the personal signature or qualified electronic signature of the representative of the entity requesting access to the data collected in the register.

When providing information from the register for its further use for purposes other than the performance of a public task, the entity maintaining a public register (as an entity obliged to provide or transmit public sector information for multiple use) shall not restrict the use of that information by other users. This principle of non-discrimination follows from Article 9(1) of the Act of 11 August 2021 on open data and further use of public sector information (Journal of Laws of 2021, item 1641 as amended). The President of the Council of Ministers may entrust the entities obliged to share or transmit public sector information for further use with tasks in the field of public sector informatization, digital innovation and development of information society and countering digital exclusion, as provided for in Article 10c (1) of the Act of 8 August 1996 on the Council of Ministers (consolidated text Journal of Laws of 2021, item 178 as amended). This is intended to promote the development of the digital society as well as to shape digital awareness in citizens, including sensitizing them to cyber threats, including promoting knowledge about the safe use of ICT systems (Karpiuk, 2022a: 18).

When organizing data processing in the electronic system , the public entity – pursuant to Art. 16(1) of the Informatization Act – is obliged to ensure that data can also be transmitted in electronic form by exchanging electronic documents related to handling of cases falling within its scope of activity, using IT data carriers or electronic means of communication.

The public entity shall inform on its pages of the Public Information Bulletin about: 1) the address of the electronic registry inbox provided in the form of a URI; 2) the maximum size of the electronic document with its attachments, expressed in megabytes, which can be served by means of the electronic registry inbox, not less than 5 megabytes; 3) the scope of electronic documents created using templates placed by these entities in the central repository or the repository of electronic document templates; 4) the types of electronic data carriers on which an electronic document can be served; 5) the types of electronic data carriers on which an official confirmation of receipt can be stored; 6) other legal requirements for the service of electronic documents. The legislature introduces this information obligation in § 3 of the Ordinance of the President of the Council of Ministers of 14 September 2011 on the drawing up and service of electronic documents and the provision of forms, templates and copies of electronic documents (consolidated text Journal of Laws of 2018, item180).

An important aspect of improving the quality of e-government is auditing. The scope of these audits is defined in Article 25 of the Informatization Act and Justice as follows: 1) the audit of the implementation of cross-sectoral IT projects is carried out by the President of the Council of Ministers; 2) the audit of the implementation of sectoral IT projects is carried out by the minister in charge of the central government administration department for which a sectoral IT project has been established; 3) the audit of the operation of ICT systems used for the performance of public tasks or the following duties: meeting the requirement of equal treatment of IT solutions of the ICT system used for data exchange; publication in the Public Information Bulletin or otherwise making available the list of electronic documents structures, data formats, communication and encryption protocols, as well as well as acceptance tests – shall be carried out: a) in local government units and their associations, as well as legal entities and other local government organisational entities created or run by these local government units – the competent provincial governor (*wojewoda*), b) in public entities subordinated or supervised by the central government administration – the administration body of central government supervising the public entity, c) in other public entities - the minister responsible for informatization. The audit is carried out in terms of compliance with minimum requirements for electronic systems or minimum requirements for public registers and electronic information exchange. In the case of local government and entities established by them, the audit may only concern electronic systems and public registers which are used for the performance of central-government tasks entrusted to the local government. If an assessment of another electronic system or public register is necessary to obtain a full assessment of the electronic system or public register used for the performance of central-government tasks entrusted to the local government, that particular system or register may also be subject to the audit. Audits on the regularity of the spending by local government units and their associations, as well as legal persons and other local government organisational units established or operated by these local government units of funds provided in the form of a special purpose grant – from the point of view of legality, cost-effectiveness, purpose and reliability of public spending – are carried out by the competent chamber of audit. Regional chambers of audit are the state financial supervision and audit bodies. This status is determined in Article 1(1) of the Act of 7 October 1992 on Regional Chambers of Audit (consolidated text Journal of Laws of 2022, item 1668 as amended).

The conduct of an audit – as follows from Article 3 of the Act of 15 July 2011 on audit in the central government administration (consolidated text Journal of Laws of 2020, item 224 as amended), – aims to evaluate the activities of the audited entity based on established facts and with the use of adopted criteria of audit. Where irregularities are found, the purpose of the audit is also to establish their extent, causes and consequences and the persons responsible, and to make recommendations with a view to remedying the irregularity.

3 Digital accessibility of public administration

Public entities are required to guarantee digital accessibility, and therefore the operation of websites or mobile applications, by ensuring their functionality, compatibility, visibility and comprehensibility. This obligation results from Article 5 of the Act of 4 April 2019 on the digital accessibility of websites and mobile applications of public entities (consolidated text Journal of Laws of 2023, item 82 as amended) hereafter ADA. The website is defined in Article 4(10) ADA as a set of logically arranged elements, linked together by navigation and links, presented using a web browser under a single web address; and the mobile application, is defined in Article 4(1) ADA as a publicly accessible software with a touch interface designed for use on portable electronic devices, excluding applications intended for use on portable personal computers. According to the legislature, functionality is the property of a website or mobile application enabling the user to use all the features offered by it (Article 4 (4) ADA), compatibility is the property enabling this website or application to interoperate with as many computer programmes as possible, including tools and software supporting disabled persons (Article 4 (6) ADA), visibility – the property of a website or mobile application enabling it to be received by the user through hearing, sight or touch (Article 4 (9) ADA), and comprehensibility is a property enabling the user of these webpages and applications to understand the content and the manner of their presentation (Article 4(11) ADA)

The Minister responsible for informatization, as part of supervision exercised over the application of ADA regulations by public entities, submits inquiries to these entities in digital accessibility matters, in particular about the number and method of settling complaints about ensuring the availability of the digital website, mobile application or elements of the website or mobile application. The minister may also impose fines, by way of an administrative decision, on public entities in matters relating to digital accessibility. The extent of this supervision is defined in Article 13 ADA.

Based on the information contained in the declarations of availability, the minister responsible for computerization draws up a list of mobile applications of public entities and the same minister, in cooperation with the Research and Academic Computer Network - National Research Institute (NASK), draws up a list of addresses of websites of public entities. The competence of the minister responsible for informatization in this regard is provided for in Article 14 ADA. As stated in § 2 of the Ordinance of the Council of Ministers of 7 June 2017 on granting the Research and Academic Computer Network the status of a national research institute (Journal of Laws of 2017, item 1193), the NASK's areas of activity include: 1) conducting research and development work in the fields of: a) telecommunication, b) ICT, c) cyber security, d) the operation of the Polish register of internet domains, f) information society; 2) adapting the results of research and development works to the needs of practice;3) implementation of R&D results in services provided for *inter alia*, security and law enforcement purposes, national security and the

security of critical infrastructure units. NASK runs the Computer Security Incident Response Team operating at the national level (CSIRT NASK).

4 Electronic delivery

The structure of the Act of 18 November 2020 on e-delivery (consolidated text Journal of Laws of 2022, item 569 as amended), – hereinafter AED, is based on two basic principles: the primacy of electronic delivery over ¬traditional delivery and the principle of universality of electronic delivery. The essence of the principle of the primacy of electronic delivery is the organisation of exchange¬ of correspondence essentially by means of a¬ public service of registered electronic delivery to an e-mail address. This electronic service is complemented by a hybrid¬ public service combining the characteristics of electronic delivery with the traditional handing a letter to the addressee in person. The hybrid public service is addressed to digitally excluded persons and those who, for reasons other than digital exclusion, are not yet ready to abandon the traditional method of delivery (Skóra, 2022: 474-475). As provided for in Article 5 AED, a public entity shall deliver correspondence requiring confirmation of its sending or receipt by means of a public hybrid service where: 1) it is not possible to send correspondence to an e-mail address or 2) the public entity is aware that a natural person having an e-mail address has been imprisoned.

Article 6 AED provides for the exemption of the application of the provisions on the address for electronic delivery and the use of the public hybrid service. According to that provision, those exemptions apply where: 1) the entity requests the delivery of a document originally drawn up in a hardcopy form 2) the correspondence may not be delivered to an e-mail address or through a hybrid public service because of: a) the inability to draw up and transmit a document in electronic form resulting from separate rules, b) the inability to use a hybrid public service resulting from special provisions, c) the need to deliver a non-transformable document recorded in a non-electronic form or a tangible object, d) an important public interest, in particular national security, defence or public order, e) technical and organisational constraints arising from the amount of correspondence and other reasons of technical nature; 3) special provisions provide for the possibility of delivery also by means other than a public electronic registered delivery service or hybrid public service, in particular by its employees, and the sender, in specific circumstances, considers another method of delivery to be more efficient.

The legislature, in Article 8 AED, obliges the public entity to have an address for electronic delivery entered in the electronic address database, linked to a public electronic registered delivery service The address for electronic delivery defined in Article 2(1) AED, is an electronic address (designation of the ICT system enabling communication by means of electronic communication, in particular electronic mail, Article 2(1) of the Act of 18 July 2002 on the provision of services by electronic means, consolidated text Journal of Laws of 2020, item 344 as amended), - of the entity using a public electronic

registered delivery service or hybrid public service or a qualified registered electronic delivery service, enabling the unambiguous identification of the sender or addressee of the data sent using these services.

An entity required to provide the public service of registered electronic delivery under Article 38 AED is the designated operator (the postal operator responsible for providing the universal service — Article 3(13) of the Act of 23 November 2012 Postal law, consolidated text Journal of Laws of 2022, item 896 as amended). The public electronic registered delivery service shall be provided: 1) in accordance with the standard covering: a) the technical requirements for the transmission of electronic documents as part of the public electronic registered delivery service, b) the manner of identification of the sender and the addressee of the data as part of the public electronic registered delivery service, c) the structure of dispatch confirmation and receipt confirmation as part of the public electronic registered delivery service, d) the form and method of issuing the dispatch confirmation, issuing the receipt confirmation, recording of the dispatch confirmation and receipt confirmation as part of the public electronic registered delivery service, e) the scope and structure of data related to communication between addresses for electronic delivery, f) the requirements of the functioning of the registered e-delivery inbox - Article 26a of the Act of 5 September 2016 on trust services and electronic identification, consolidated text Journal of Laws of 2021, item 1797 as amended; 2) at reasonable prices. The designated operator, when providing the public electronic registered delivery service, shall ensure: 1) the identification of the sender before the dispatch of the data; 2) the identification of the addressee before the delivery of the data; 3) securing the data dispatch and receipt by an advanced electronic seal in such a way that no undetectable alteration of the data is possible; 4) notifying the sender and the addressee of any change of data necessary for the purpose of sending or receiving the data; 5) the indication, by means of a qualified electronic timestamp, of the date and time of sending, receiving and any change of the data. Electronic registered delivery service means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations, Article 3 (36) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, p. 73)

A designated operator is required to provide the public hybrid service pursuant to Article 45 AED. The public hybrid service shall be provided: 1) in a uniform manner under comparable conditions; 2) ensuring that post offices of the designated operator are deployed throughout the country; 3) in compliance with standard letter delivery times; 4) at affordable prices; 5) at a frequency ensuring the delivery of letters at least on each working day and not less than 5 days per week, excluding public holidays; 6) in such a way as to ensure that the sender receives an electronic document confirming receipt of

registered mail (mail accepted against receipt and delivered against receipt – Article 3 (23) of the Act of 23 November 2012 Postal law, consolidated text Journal of Laws of 2022, item 896 as amended). When providing a public hybrid service, the designated operator must ensure the operation of: 1) the infrastructure necessary for printing and enveloping the correspondence sent in an electronic form; 2) the postal network necessary for the sorting, shipment and delivery of mail. According to § 2 of the Ordinance of the Minister of State Assets of 9 August 2021 on the implementation of the public hybrid service domestically (Journal of laws of 2021, item 1503 as amended), the standard time of delivery of letters is up to 6 days from the date of posting the electronic document containing the contents of the correspondence transformed into a letter until the date of delivery, notification of attempt to deliver the letter, or refusal to accept the letter containing the correspondence.
The designated operator providing a public hybrid service is required, pursuant to Article 46(1) AED, to convert an electronic document sent by a public entity from an e-delivery address into a letter in order to deliver the correspondence to the addressee. The conversion takes place in an automated manner, ensuring the protection of postal secrecy at each stage of the service.

Reference should be made to the position of the Regional Administrative Court in Warsaw in its judgment of 23 April 2021, VII SA/WA 2392/20 (LEX No 3178567), according to which wrong proceeding by an administrative body regarding the adopted form of a document served by means of electronic communication must not harm the party who received such a document, including depriving that party of the right to appeal against the decision received in this way. The rules on delivery are, above all, a guarantee for the party to the proceedings and not for the body, and cannot be interpreted to the detriment of the party.

5 E-government and cybersecurity

The ICT systems used by the public administration must be adequately protected, preferably free from interference, but at least protected against interference that undermines their normal functioning and limits the quality of the provision of public services through such systems. Therefore, an adequate level of cybersecurity must be maintained in this area of public administration activity.

Cybersecurity is defined – by Article 2(4) of the Act of 5 July 2018 on the national cybersecurity system (consolidated text Journal of Laws of 2022, item 1863 as amended) hereafter ANCS – as the resilience of information systems to activities affecting the confidentiality, integrity, availability and authenticity of data processed or related services offered by these systems. Cybersecurity is a specific sector of security that includes the protection of information systems against threats (Czuryk, 2019: 42; Karpiuk, 2021a: 46-47; Karpiuk, 2021b: 234). It covers the threat prevention and

forecasting, as well as remedying the effects arising as a result of these threats (Karpiuk, 2021c: 612).

Ensuring security in cyberspace is one of the basic tasks of public authorities. Threats of an IT nature have increasingly serious consequences and cyber attacks can be used not only as a means of economic pressure but also political one (Kaczmarek, 2019: 145).

The Polish legislature determines the organisation of the national cybersecurity system, as well as the tasks and responsibilities of the entities which form part of the system. According to Article 3 ANCS, the aim of the national cybersecurity system is to ensure security in cyberspace at national level, including the undisturbed provision of essential services and digital services, by achieving an adequate level of security of information systems for the provision of these services and ensuring incident response. This is achieved, also in the case of e-government and its electronic services, through information systems (ICT systems together with electronic data processed therein). The national cybersecurity system consists of public entities of different legal and territorial status, as well as non-public entities. However, public entities, especially those specialised in cybersecurity, are essential to that system (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 4).

One of the authorities responsible for cybersecurity is the Minister of National Defence, who directs the section of national defence covering during peacetime the cybersecurity issues in the military dimension. The tasks of this central government administration body cover cybersecurity only in the military dimension. Cybersecurity issues in the civil dimension are covered by the section of informatization (Karpiuk, 2022b: 87). The Minister of National Defence is the governing body in the military sphere, including in matters of ensuring cybersecurity. It carries out tasks in this regard through subordinate and supervised organizational units (Bencsik, Karpiuk, 2023: 89). The body that is competent in the area of civil cybersecurity is the Minister responsible for informatization matters.

In the case of cybersecurity, an appropriate level of protection of information systems should be ensured, therefore, to guarantee that level, there may be restrictions on the freedoms and rights of individuals in cyberspace in specific cases. This is permissible provided that such protection is not otherwise assured (Czuryk, 2022a: 34). Security in cyberspace should be particularly protected, even in certain cases against individual freedoms and rights, if their exercise contradicts the need to ensure the cybersecurity of the state (Karpiuk, 2022d: 406).

Therefore, cybersecurity, as the resilience of information systems to disruptions, including with regard to data processed or services provided through them, must be adequately protected, accordingly to the threats. Such protection ensures the normal functioning of the public administration, which handles many matters electronically,

thereby greatly facilitating contact with the general public. In so doing, it shall make public services more efficient, swifter and more accessible to the citizen.

6 Supporting the development of telecommunication services and networks

Specific tasks in the area of supporting telecommunication services and networks have been assigned to local government as a structure that is closest to citizens. Pursuant to Article 3 of the Act of 7 May 2010 on the support for the development of telecommunications services and networks (consolidated text Journal of Laws of 2022, item 884 as amended) hereafter ASD, the local government body, in order to meet the collective needs of the local community, may: 1) build or operate telecommunications infrastructure and networks and acquire rights in telecommunications infrastructure and networks; 2) provide telecommunications networks or provide access to telecommunications infrastructure; 3) provide, using its telecommunications infrastructure and networks, services to specific entities (including telecommunications operators or end-users). Activities involving the construction of telecommunications infrastructure and networks may be undertaken if, in the area concerned: 1) there are no telecommunications infrastructure and networks; (2) existing telecommunications infrastructure and networks are not available or do not meet the needs of the local government unit.

Where that activity involves the provision by the local government unit of an internet access service through publicly available internet access points free of charge or for a fee lower than the market price, the information on the taking up of activities to support the development of telecommunications services and networks must also include the location of publicly available internet access points and an indication of the area where the service is provided through those points.

The local government unit may provide internet access services through publicly accessible internet access points free of charge or for a fee lower than the market price only in public places. According to § 1 of the Ordinance of the Minister of Informatization of 18 October 2018 on the minimum bit rate for Internet access services provided by local government units (Journal of Laws of 2018, item 2078) – the minimum bit rate for Internet access services provided by local government units via publicly available Internet access points free of charge or for a fee lower than the market price is 30 Mb/s.

The support for the development of telecommunications services and networks is provided in order to meet the collective needs of the local community. Public tasks serving to satisfy the needs of the local community, as stipulated in Article 166(1) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, No. 78, item 483, as amended), are performed by the local government unit as its own tasks. These tasks are the basic tasks of the local government. They are placed at the appropriate level of local government by the constitutional principle of subsidiarity (Winczorek, 2008:

331). These tasks are territorial in nature, defined by the boundaries and level of the local government where the local government unit concerned operates, and should concern its inhabitants (Banaszak, 2009: 752).

Pursuant to Article 3a ASD, the executive body of the local government unit concerned may award to entities not included in the public finance sector and not engaged in a commercial business a special-purpose grant from the budget of the local government unit for the financing or co-financing of investment costs related to meeting the needs of those entities for access to the high-speed telecommunications network at the location of the end-user. As provided for in Article 126 of the Act of 27 August 2009 on public finance (consolidated text Journal of laws of 2022, item 1634 as amended) these grants are funds, subject to special accounting rules, from the state budget, local government unit's budget and State's special funds allocated under the Act, separate legislation or international agreements, for financing or co-financing the fulfilment of public tasks. The rules governing the award of a specific-purpose grant, including in particular the criteria for selecting projects for financing or co-financing and the procedure for awarding that grant and the method of accounting for it, are to be determined by a resolution adopted by the legislative body of the local government unit. Therefore, the legislature leaves the local government authorities a discretion in this regard. In the judgment of 16 April 2019, III SA/Po 9519 (LEX no 2654279), the Regional Administrative Court in Poznań states that each grant is intended to finance or co-finance the performance of public tasks, i.e. tasks that exist at the date of granting the right to finance or co-finance them. It is only when the right to the grant has been awarded that a public task can be implemented. The grant is a redistributive expense, for future purposes, and derogations, if any, must clearly stem from statutory provisions.

The local government unit, when entrusting a telecommunications company with the performance of activities in the field of supporting the development of telecommunications services and networks, where it is not possible, due to economic conditions, in a given area for the telecommunications company to carry out financially viable telecommunications business, may, pursuant to Article 8 ASD :1) provide telecommunications infrastructure or networks to the telecommunications company for fees lower than the cost of production; 2) co-finance the costs incurred for the provision of telecommunications services to end-users or telecommunications companies for the purpose of providing such services.

The issues concerning the activities of local government units to stimulate demand for services related to Internet access are set out in Article 15 ASD. According to that provision, local government units may take measures to stimulate or aggregate user demand for broadband internet services, in particular education and training services, by equipping consumers with telecommunication terminal equipment or computer equipment, or by financing the cost of telecommunications services borne by consumers. The legislative body of the local government unit determines, by resolution, the

conditions and procedure for financing that activity, in particular by determining the conditions of eligibility of the beneficiaries of the aid. The above activities are carried out in a non-discriminatory manner, with transparency and proportionality, and are aimed at maintaining technological neutrality. Any project undertaken by local government to stimulate demand for services related to Internet access requires prior publication, with a description thereof, in the Public Information Bulletin on the website of the local government unit concerned and at the office premises of that unit.

The legislature also introduced specific rules for the location of telecommunications projects. Pursuant to Article 46 ASD, the local spatial development plan may not establish prohibitions, and the solutions adopted therein may not prevent the location of public purpose projects in the field of public connectivity, if such a project is in compliance with special provisions. Public connectivity is defined in Article 4(18) of the Act of 21 August 1997 on real estate management (consolidated text Journal of Laws of 2021, item 1899, as amended) as telecommunications infrastructure serving to provide publicly available telecommunications services, therefore according to Article 2(31) of the Act of 16 July 2004. Telecommunications Law (consolidated text Journal of Laws of 2022, item 1648 as amended), – telecommunications services (services consisting primarily in the transmission of signals over a telecommunications network) available to the general public.

In the absence of a local spatial development plan, the location of a public connectivity project other than telecommunications infrastructure of little impact is determined by a decision on the location of a public-purpose project. The elements of the decision on the location of a public-purpose project are specified in Article 54 of the Act of 27 March 2003 on spatial planning and development (consolidated text Journal of Laws of 2022, item 503 as amended). According to this provision, the decision defines:1) the type of project; 2) the conditions and detailed rules for land planning and development resulting from special provisions, including in the area of : a) conditions and requirements for the protection and shaping the spatial order, b) protection of the environment and human health and cultural and historical heritage and works of contemporary culture, c) maintenance in terms of technical infrastructure and communication, d) requirements regarding protection of interests of third parties, e) protection of civil structures in mining areas; 3) lines demarcating the project site, delimited on the map on an appropriate scale. Such a decision must also meet the conditions laid down in Article 107 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text 2022 Journal of Laws, item 2000 as amended), hereinafter referred to as CAP, and thus contain the following elements: 1) identification of the public administration body; 2) date of issue; 3) identification of the party or parties; 4) reference to the legal basis of the decision; 5) ruling; 6) statement of factual and legal reasons; 7) instruction on whether and how the party may appeal against the decision and on the right to waive the appeal and the consequences of such waiver; 8) signature including the name and official position of the employee of the body authorized to issue the decision; 9) where the decision may be

appealed against by way of an action brought before common court, protest against decision or application to an administrative court – the instruction on the admissibility of filing the action, the protest against the decision or application and on the amount of the procedural fee if fixed, or on the basis of calculation of the fee if proportional, as well as the possibility for the party to apply for an exemption from procedural costs or granting legal aid. The factual reasons for the decision should in particular include an indication of the facts which the body has found to be proven, the evidence on which it relied and the reasons why other evidence has been found incredible and devoid of probative value, while the legal reasons should explain the legal basis for the decision, together with citing the relevant legal provisions. According to the position of the Regional Administrative Court in Gliwice expressed in the judgment of 12 April 2022, II SA/Gl 1500/21 (LEX nr 3338604), the minimum formal requirements of the decision are: the identification of the body which has issued it, the addressee of the decision, the content of the decision and the signature of the person who has issued it. The document does not have to be titled as a decision, but must contain a ruling.

The Regional Administrative Court in Poznań, in its judgment of 12 January 2022, II SA/Po 956/21 (LEX No. 3285590), stated that the decision on the location of a public purpose project was not enforceable due to its subject. Such a decision specifies only the type of project that can be carried out in a given area, the conditions and detailed rules for land planning and development resulting from separate regulations, as well as the lines demarcating the project area. Thus, such a decision does not have any substantive legal effects and does not give the investor the right to commence construction works related to the planned project.

7 Minister responsible for informatization and his responsibilities

The minister responsible for informatization is in charge of the section of informatization, and according to Article 12a of the Act of 4 September 1997 on central government administration sections (consolidated text Journal of Laws of 2022, item 2512, as amended), this section includes the matters of: 1) informatization of the public administration and entities performing public tasks; 2) ICT systems and networks of the public administration; 3) support for projects in the field of informatization; 4) implementation of the international obligations of the Republic of Poland in the field of informatization and telecommunication; 5) participation in shaping the European Union policy in the field of informatization; 6) development of the information society and counteracting digital exclusion; 7) development of services provided electronically; 8) shaping the national policy in the area of personal data protection; 9) telecommunications; 10) cyberspace security in the civil dimension; 11) the PESEL register, the Register of Personal Identity Cards, the Register of Civil Status and the Register of Passport Documents; 12) the register of vehicles, the register of drivers and the register of parking card holders; 13) supervision of the provision of trust services as defined in the

regulations on trust services; 14) electronic identification. The minister responsible for informatization supervises the President of the Office of Electronic Communications.

Under Article 19a of the Informatization Act, the minister responsible for informatization shall ensure the functioning of the Electronic Platform of Public Administration Services (ePUAP). H shall publish on that platform information on the addresses of electronic registry inboxes provided by public entities.

According to the position contained in the judgment of the Regional Administrative Court in Warsaw of 26 March 2021, VII SA/Wa 1959/20 (LEX No. 3173288), a precondition for granting an ePUAP functionality is not only the performance of public tasks, but having the status of a public entity. Pursuant to § 7 of the Ordinance of the Minister of Digital Affairs of 5 October 2016 on the scope and conditions of using the electronic platform of public administration services (consolidated text Journal of Laws of 2019, item 1969, as amended), a public entity shall apply to the minister responsible for informatization with a request to grant the functionality of a public entity on ePUAP. The application shall include the following elements: 1) identification of the public entity; 2) name and surname of the person authorized to represent the public entity together with the function or position; 3) details of the entity's administrator. The functionality of a public entity on ePUAP becomes available upon approval of the application by the minister.

Pursuant to Article 19b of the Informatization Act, the Minister responsible for informatization operates as part of the ePUAP a central repository of electronic document templates. Public administration bodies provide electronic document templates to the central repository and make them available in the Public Information Bulletin. International standards for preparing electronic documents by public administration bodies are used for the drafting of electronic documents, taking into account the need to sign them with a qualified electronic signature. The central repository for electronic document templates contains, stores and makes available document templates that take into account the necessary structural elements of electronic documents. The essential structural elements of electronic documents – as follows from § 2 (2) of the Ordinance of the Minister of Internal Affairs and Administration of 30 October 2006 on necessary structural elements of electronic documents (Journal of Laws of 2006, No. 206, item 1517 as amended)– are the following metadata: 1) identifier – a unique, in a given set of documents, tag of a document that enables its identification; 2) creator – the entity responsible for the content of the document, with specification of the creator's role in the process of document drafting or acceptance; 3) title – the name given to the document; 4) date – the date of the event related to document creation; 5) format – the name of the data format used to prepare the document; 6) access – identification of those to whom the document can be made available, under what rules, and to what extent; 7) type – determination of the basic document type (e.g. text, sound, image, video, collection) based on the list of types of the Dublin Core Metadata Initiative and its possible

specification in more detail (e.g. presentation, invoice, act, memo, ordinance, letter); 8) relation – determination of the direct link to another document and the type of this connection; 9) recipient – the entity to whom the document is addressed; 10) grouping – indication of affiliation to a set of documents; 11) classification – archival category of the document;12) language – code of natural language according to the ISO-639-2 standard or other language specification, if not present in the standard; 13) description – a summary, table of contents or short description of the content of the document; 14) rights – indication of the entity authorised to dispose of the document.

The Minister competent for informatization is responsible for the functioning of the electronic system, which:1) provides support for the public electronic identification system, in which the following are issued: a) trusted profile, b) personal profile; 2) enables public entities: a) to authenticate an individual using an electronic identification means, b) to ensure that an individual can sign an electronic document with a trusted signature. This responsibility is based on Article 20aa of the Informatization Act. The person applying for a trusted profile confirmed in the point confirming that profile submits an application in electronic form, using the electronic form provided in the system where the trusted profile is issued. The electronic form may be an element of the electronic service provided in ePUAP that enables the creation of an account in this electronic system – § 3 of the Ordinance of the Minister of Digital Affairs of 29 June 2020 on the trusted profile and trusted signature (Journal of Laws of 2020, item 1194 as amended).

The Minister responsible for informatization, pursuant to Article 20h of the Informatization Act, maintains a register of contact details of natural persons, designed to facilitate contact with natural persons in connection with the services and public tasks performed for these persons. The contact details are not used to contact natural persons with regard to their business activity. The register of contact details is kept in a way that : 1) allows natural persons to effectively enter, search, update and delete their contact details; 2) allows relevant entities: a) to effective enter, search, update and delete contact details in accordance with the request of the data subject, b) to search for contact details of natural persons for the purposes of provision by these entities of services and public tasks for these persons, or confirmation of the fact that no such data has been provided by the natural person searched for; 3) allows access to it 24 hours a day, 7 days a week, except for breaks for maintenance work carried out in the electronic system; 4) allows entering contact details into the register of contact data directly, in real time - § 3 of the Ordinance of the Minister of Digital Affairs of 19 December 2019 on the register of contact details (Journal of Laws of 2019, item 2467).

The Minister responsible for informatization is obliged by Article 20p of the Informatization Act to ensure the functioning of an organisational and technical solution for carrying out analyses supporting the development of key public policies using data made available by public entities, collected in public registers and ICT systems (an integrated analytical platform). In order to ensure the functioning of the integrated

analytical platform (pursuant to Article 20s of the Informatization Act), the Minister: 1) provides protection against unauthorised access to data; 2) prevents damage to the integrated analytical platform; 3) ensures the integrity of the data collected; 4) determines the rules on the security of the data processed, including personal data; 5) ensures accountability of the activities carried out under the integrated analytical platform; 6) determines the rules for reporting personal data breaches. Personal data processed under the integrated analytical platform shall be used in an adequate, appropriate and limited manner, only where necessary to achieve the specific analytical objectives. The use of data for purposes other than statutorily defined, in particular for making decisions or individual rulings, shall be prohibited. The integrated analytical platform is not intended for conducting current policy but for supporting public policies. The use of data within this platform must comply with the principle of proportionality. The use of such data must therefore not be excessive and must serve strategic analytical objectives pursued through key public policies.

The Minister competent for informatization – as follows from Article 12 AED. – shall create an address for electronic service linked to the public service of registered electronic delivery at the request of a public entity submitted to the Minister and, in the case of public entities entered in the National Court Register, automatically upon receiving via the electronic system, the data transmitted in connection with the request for entry. An application for the creation of an address for electronic deliveries linked to the public service of registered electronic delivery to a public entity contains the following data: 1) the name or business name of the entity under which the entity operates, and in the case of a court enforcement officer, his name and title; 2) the REGON identification number; 3) tax identification number (NIP), if assigned, or information on its cancellation or revocation; 4) KRS number, if assigned; 5) registered office and address; 6) address for correspondence; 7) the name of the administrator of the delivery box, his/her e-mail address and PESEL number, and if not assigned, then the unique identifier assigned by the Member State of the European Union for cross-border identification.

The Minister maintains, as a public register, an electronic address database in which addresses for electronic delivery are collected, and ensures the maintenance and development of that database. Therefore, pursuant to Article 25 AED, the Minister: 1) provides protection against unauthorized access to the electronic address database; 2) ensures the integrity of data processed in the electronic address database; 3) ensures the availability of the electronic system, in which at least: a) the electronic address database is maintained, b) search services are made available in the electronic address database, c) collects information about qualified trust service providers providing qualified electronic delivery services and about their addresses for electronic delivery and their location - for data processors in the electronic address database, and prevents damage to this electronic system; 4) determines the rules of security of processed data, including personal data; 5) determines the rules for reporting personal data breaches; 6) ensures accountability of the

activities performed on the data in the electronic address database; 7) ensures the correctness of the data processed in the electronic address database.

According to Article 58 AED, the Minister competent for informatization ensures the functioning of the electronic system, in which at least: 1) the database of electronic addresses is maintained; 2) the search services are provided in the electronic address database; 3) information is collected about qualified trust service providers providing qualified electronic delivery services and about the addresses for electronic delivery maintained by them and their location; 4) the access point to the services of registered electronic delivery in cross-border traffic is made available. Together with the Minister responsible for the economy, they both ensure the functioning of the ICT systems: 1) allowing users to access the resources of delivery boxes located in the ICT system of the designated operator; 2) allowing users to access the public electronic registered delivery service and the public hybrid service; 3) through which data about the authentication of a natural person using an electronic identification means ensuring at least an average level of security are transmitted to the system of the designated operator; 4) through which other data necessary for the provision of the public electronic registered delivery service and the public hybrid service are transmitted to the system of the designated operator.

The Minister also disposes of the Broadband Fund. This fund, as provided for in Article 16a ASD, is a public special purpose fund. The Broadband Fund is intended to be spent for: 1) measures to support the development of high-speed telecommunications networks by financing or lending for the construction or conversion of such networks and the provision of telecommunication connections to the location of the end-user; 2) actions to stimulate end-user demand for broadband services by funding the purchase of telecommunication services, the purchase of multimedia devices and the organisation of training to develop digital competences or participate in that training; 3) the costs of maintaining and operating the System of Information on Access to Fixed-Line Broadband Internet Services (SIDUSIS), which is a public database operated by the Minister responsible for informatization, including information on address points; 4) the co-financing or financing of the operation of the Broadband Coordinator, which represents the municipality or district in telecommunications matters and the development and maintenance of broadband networks within the municipality or district; 5) costs related to the operation of the Broadband Fund. The resources of the Fund may constitute revenue of the Cybersecurity Fund. As is apparent from Article 2 of the Act of 2 December 2021 on special rules of remuneration for persons performing cybersecurity tasks (Journal of Laws of 2021, item 2333 as amended), the Cybersecurity Fund is to support measures to ensure the security of information systems against cyberthreats. Its resources are allocated for an IT allowance, therefore an extra pay added to the base pay and, in the case of professional officers and soldiers, for the monetary benefit granted to persons performing cybersecurity tasks. The allowance is an incentive not only for more efficient work or service in entities carrying out cybersecurity tasks (Czuryk, 2022b: 111).

8 Administrative e-procedure

According to Article 14 CAP, cases should be processed and settled in writing, recorded in a paper form or electronic form. Documents recorded in an electronic form shall bear a qualified electronic signature, a trusted signature or a personal signature, or shall bear a qualified electronic seal of the public administration body and identification of the person who put the seal in the body of the document. Cases may be handled with the use of letters generated automatically and bearing a qualified electronic seal of a public administration body. In the case of automatically generated letters, the provisions on the necessity to affix the signature of a public administration body employee to the letter do not apply. Cases may also be handled using online services provided by public administration bodies upon authentication of a party or other participant in the proceedings.

As rightly put by the Regional Administrative Court in Gorzów in the judgment of 12 April 2018, II SAB/Go 10/18 (LEX no. 2481265), it is the responsibility of the public administration body to configure electronic mail service, including anti-spam filters, and to organise the maintenance of the body's electronic mail service in such a way as to ensure trouble-free and immediate receipt of applications sent to the address indicated by it, in view of the legal admissibility of filing them also electronically. The consequences of difficulties, errors or irregularities in the design and operation by public administration bodies of official systems for communication with them cannot be passed on to the users of these systems. The risk that an application sent to it by electronic mail, addressed to the body's officially provided electronic address, will not be received or read by the body is borne by the body and not by the applicant.

The public administration body shall deliver letters to the electronic delivery address, unless the delivery is effected on an account in the information system of the body or at the premises of the body. This rule is introduced by Article 39 § 1 CAP. If it is not possible to service the letter in this way, the delivery shall be otherwise provided. The principle of official character of delivery adopted in the CAP is expressed by the body's duty of the authority to serve mail *ex officio* in the form provided for in the statutory provisions and to ensure the regularity of the operations constituting effective delivery. Under the legislation currently in force, the use of e-mail is not a legally permissible method of service unless electronic delivery is involved – as is apparent from the judgment of the Regional Administrative Court in Warsaw of 15 January 2020, VI SA/WA 1779/19 (LEX No 3019635).

As provided for in Article 63 CPA, applications in an electronic form shall be submitted to an address for electronic delivery or through an account in the information system of the public administration body concerned. Unless otherwise provided for in separate provisions, applications submitted to the e-mail address of the public administration body shall be left unprocessed. The application should contain at least an identification of the

person from whom it originates, address of that person, including where the application is submitted electronically, as well as the request and must comply with other requirements laid down in the special provisions. The e-mail address of a public administration body cannot be equated with an electronic registry inbox, as is apparent from the judgment of the Supreme Administrative Court of 28 March 2022, I OSK 1224/21 (LEX No 3341615).

9 Conclusions

Cyberspace is a place where activities are carried out in the public, private, social or economic spheres. It is used to provide various types of services and to communicate. The importance of cyberspace for both the state and society is very important, therefore both public and private institutions have an obligation to protect it. Protection against cyberthreats should be a priority of state policy as well as the duty of entities responsible for the security of ICT systems (Karpiuk, Kelemen, 2022: 71). Cyberspace is an area allowing better fulfilment of public needs. In the age of digital government, it guarantees faster communication and more public services, and allows reaching a wider audience.

The modern public administration largely relies on ICT systems and networks that must be adequately protected against cyberattacks (Karpiuk, 2022c: 70). This protection is to be provided by the relevant authorities of the State. Thus, according to Article 32a of the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (consolidated text Journal of Laws of 2022, item 557 as amended), to prevent and counter terrorist incidents concerning the ICT systems of public administration bodies which are important for the continuity of the operation of the State, as well as the ICT networks listed in the uniform list of facilities, installations, equipment and services forming part of critical infrastructure or data processed in these systems, and the prevention, detection and prosecution of terrorist offences in this area, the Internal Security Agency may carry out a security assessment of these ICT systems.