Information security in the world: the case of the Agricultural Social Insurance Fund (KRUS) with particular focus on personal data protection

Katarzyna Banach, Martyna Lechowicz, Magdalena Szewczyk

Abstract

The information society, in which information is of growing significance, exposes its citizens to a particular category of cyber threats, namely breaches of information security and confidentiality, as well as the illegal use of personal data, which frequently results in identity theft. Therefore, in order to ensure information security, and particularly the protection of personal data, laws and rules have been established to define the manner in which such information is managed, processed, protected and distributed. Since 28 May 2018, both the data controller and the data processor have borne responsibility for breaches of data security. The forms of obtaining and using information are reflected in the applicable legislation. As a result, public entities develop Security Policies – documents that set out procedures and internal rules of conduct. Their purpose is to introduce standards for information security and to engage employees in actively safeguarding data.

The main objective of this paper is to present the method of ensuring information security with particular emphasis on the protection of personal data, using the example of the Agricultural Social Insurance Fund (KRUS).

Key words: information security, personal data, information, KRUS, personal data protection, security policy.

Katarzyna Banach, a student of post-graduate studies "Agriculture Social Insurance – Functioning, Administration and Legal aspects" at the President Stanisław Wojciechowski Calisia University in Kalisz, chief specialist, Farmers' Social Insurance Council Service Team, Head Office, Agricultural Social Insurance Fund (KRUS); **Martyna Lechowicz**, a student of post-graduate studies "Agriculture Social Insurance – Functioning, Administration and Legal aspects" at the President Stanisław Wojciechowski Calisia University in Kalisz, chief specialist, Office for Crisis Management, Defence and Information Security, Head Office, Agricultural Social Insurance Fund (KRUS); **Magdalena Szewczyk**, a student of post-graduate studies "Agriculture Social Insurance – Functioning, Administration and Legal aspects" at the President Stanisław Wojciechowski Calisia University in Kalisz, chief specialist, Office of the President, Head Office, Agricultural Social Insurance Fund (KRUS).

Introduction

The emergence of the information society is linked to "the dynamic development of broadly understood information technologies, enabling the acquisition, processing, sharing and storage of information"[1]. Consequently, the primary commodity is the digital product –information (documents, money, musical works, software). It is one of the most important factors shaping human communities. The invention of new means of transmitting information has become a factor leading to profound civilisational change. The widespread use of personal computers and the development of Internet access have enabled it to influence further areas of social life. This, in turn, has driven the broader development of digital technologies. Information has greatly increased in value – it has, in a sense, become a strategic element, as its significance has clearly grown not only for individuals but also for public and private institutions. Since information performs many essential functions – such as decision-making, cultural and knowledge-enhancing – it should be properly managed. The introduction of a Security Policy, aimed at developing internal procedures and regulations that define rules of conduct, enables the implementation of information protection standards and engages employees in actively safeguarding information.

The revolution in communication, considering the speed and reach of information exchange, came about thanks to the Internet, which provided quick and easy access to data – without temporal or geographical restrictions. Unfortunately, the Internet has also brought new risks and threats. These are associated with the security of information, ICT systems, and privacy. Information security requires that IT resources be safeguarded in such a way that information can be collected, processed, stored and transmitted securely, without exposure to any threats.

Methods of information protection, or information security

The primary task of the state is to ensure the security and freedom of its citizens. The provisions of the Constitution of the Republic of Poland of 1997[2] indicate that security relates to multiple contexts: public, state, citizen, internal and external, as

1. T.R. Aleksandrowicz, *Analityk informacji w administracji rządowej* [in:] *Analiza informacji w zarządzaniu bezpieczeństwem. Zarządzaniem bezpieczeństwem*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa, Difin SA Publishing House, 2013, p. 11.
2. Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. nr 78 poz. 483 ze zm.

well as ecological. Article 5 of the Constitution of the Republic of Poland provides that "the Republic of Poland shall safeguard the independence and inviolability of its territory, ensure the freedoms and rights of persons and citizens, and the security of citizens, protect the national heritage and ensure environmental protection guided by the principle of sustainable development"[3]. As can be seen, guaranteeing the security of citizens is a fundamental task of the state. Through its designated public institutions, the state safeguards the rights of citizens and protects their security, including information security. Each organisational unit introduces within its structure divisions responsible for information security. Security policies applicable within given institutions are developed, which define the scope of information being processed, how it is used and how it is protected.

"Information protection is a necessity and an obligation of organisations; legal requirements also impose on organisations the obligation to take organisational and technical measures in the area of information protection. The organisation should ensure and maintain an appropriate level of information security, meaning that information must be authentic, accessible only to authorised individuals, delivered at the right time and solely to appropriate recipients. Information security is a systematic approach to the protection of important information to ensure its safety. It involves people, processes, infrastructure and systems. Information security is not a fixed or one-time state, as practice shows that it must be systematically maintained, verified and monitored. Contemporary ICT tools and computer software mean that the struggle for information gains particular importance"[4].

Information is classified according to specific groups or categories. The first group includes general information, such as news disseminated by the mass media. For information purposes, content on current events, articles on contemporary issues, political or religious information, statements and photographs by reporters, as well as speeches by public figures may be made public. This category includes all works broadcast via radio or television.

Public information is also classified as non-confidential and is defined by the Act of 6 September 2001 on Access to Public Information, which stipulates that public information is any information concerning public matters. The act specifies a catalogue of information that is of a public nature[5]. According to Article 8 of this Act, an official ICT publication system – the Public Information Bulletin – was established to enable universal access to public information. Naturally, the Act also provides

3. Ibidem, Article 5.
4. I. Oleksiewicz, W. Krztoń, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warsaw, Rambler Press, 2017, p. 27–28.
5. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. 2022 poz. 902.

for the possibility of withholding public information pursuant to regulations on the protection of classified information and other legally protected secrets.

The next group comprises legally protected information, which includes two subgroups: special information, such as personal data, and sensitive information, i.e. professional secrets. Personal data is a category of information that enables the identification of a natural person[6]. The Act does not precisely define what constitutes personal data but states that it may be any data that allows it to be linked to a specific individual. Thus, it is information that allows for the determination of a person's identity. "Easily accessible and commonly used sources are used for this purpose. A person may be identified either indirectly or directly, i.e. by means of information such as: identification number, physical, physiological, mental, economic, cultural or social characteristics"[7]. Personal data may only be processed for a strictly defined purpose and with the consent of the data subject. Several categories of such data can be distinguished. These include:

1) "provided personal data – personal data knowingly provided by natural persons, e.g. when filling in an online form;
2) observed personal data – personal data automatically recorded, e.g. by means of cookies or online sensors, or CCTV enabling facial recognition;
3) derived personal data – personal data "created" from other data in a relatively simple and direct way, e.g. when calculating a customer's creditworthiness;

Inferred personal data – personal data generated using more complex analytical methods (e.g. by identifying correlations between data sets and using these correlations to categorise or profile likely future health outcomes). Inferred data is based on probabilities and is therefore less certain than derived data"[8].

As mentioned earlier, sensitive information includes professional secrets acquired while holding a particular position or performing a specific profession. This category may include journalistic, medical, commercial, banking or business secrets. A separate category of data subject to particular protection is classified information, which concerns the broadly understood security of the state, has its own classification, and associated confidentiality clauses. The Act on the Protection of Classified Information defines four levels of classification: "top secret", "secret", "confidential" and "restricted"[9].

6. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2019 poz. 1781, art. 6 ust. 1.
7. S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki-Organizacji-Państwa*, 2nd ed., Warszawa, CeDeWu, 2019, p. 198.
8. M. Gumularz, P. Kozik, *Ochrona danych osobowych. Kontrola i postępowanie w sprawie naruszenia przepisów. Poradnik ze wzorami*, 2nd ed., Warszawa, Wolters Kluwer, 2022, p. 24.
9. Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. 2024 poz. 632 ze zm.

According to the definitions set out in the Act of 5 August 2010 on the Protection of Classified Information, the clause:

- "Top secret" is applied to classified information, the disclosure of which would cause exceptionally serious harm to the Republic of Poland, e.g. endanger the independence, sovereignty or territorial integrity of the state, threaten internal security, or undermine national defence readiness;
- "Secret" is applied to classified information, the disclosure of which could cause serious harm to the Republic of Poland – for example, by impairing international relations, disrupting defence preparations, or causing major damage to the state's economic interests;
- "Confidential" is applied to classified information, the unauthorised disclosure of which would harm the Republic of Poland, e.g. by hindering foreign policy, threatening citizen security, or obstructing the operations of national security services;
- The lowest clause, "Restricted", is applied to classified information not assigned a higher classification, the unauthorised disclosure of which could negatively affect the functioning of public authorities or other entities in areas such as national defence, foreign policy, public safety, or the protection of citizens' rights and freedoms.

Each of the aforementioned security classifications is accompanied by specific requirements that must be met to ensure the protection of classified information from disclosure. The decision to assign a classification level to a given document is made by the person authorised to sign it. Such documents may be accessed exclusively by authorised individuals who hold the appropriate security clearance, obtained following the successful completion of a vetting procedure as set out in the legislation, as well as training in classified information protection. Access to these documents is strictly limited to the scope necessary for the performance of duties associated with a given position. Additionally, such access must be granted in conditions that prevent unauthorised disclosure – for example, in secure registry offices or other premises that meet the requirements laid down in the act and implementing regulations. Information is also classified according to quality criteria relating to its protection, such as:

1) "confidentiality – denotes the required degree of protection against unauthorised access; the confidentiality level is agreed upon by the persons or organisations supplying and receiving the information;
2) integrity – means that no unauthorised modifications have been made to the information;
3) availability – refers to the level of accessibility of data, processes and applications required by the user (or specified in the system requirements);

4) accountability – defines the ability to identify users of information and ICT systems, as well as the services they have used; this criterion also determines the ability to conduct effective post-incident analysis;
5) non-repudiation – concerns the possibility that a party involved in the information exchange may deny participation;
6) authenticity – denotes the ability to definitively establish which entity transmitted the data"[10].

These criteria depend primarily on the nature of the information itself, as well as the organisational and technical solutions adopted in the system that processes it.

In the information society, information has become the driving force of modern civilisation, regarded as a resource, commodity, and product for sale. Today, it plays an extremely important social role, and its power affects both personal and professional life.

"One of the most important aspects of safeguarding information security is the development by an organisation of an information security policy. This is a documented set of principles, practices and procedures by which a given organisation defines how it protects information system assets and processes information. It is a document that demonstrates the management's commitment to information security and also sets out how information security contributes to fulfilling and supporting the organisation's vision and mission. The development of a security policy consists of several stages, including:

– needs analysis – identifying threats, assessing potential losses, inventorying the information system, defining requirements, analysing possible solutions, determining the optimal investment approach;
– defining the security policy – setting goals, defining dependencies, establishing information flows, publishing security rules, planning training, and setting out methods for monitoring and controlling the enforcement of the security policy;
– implementing the security policy – publishing the security policy, establishing teams, assigning tasks, verifying knowledge of the policy, conducting practical training, and informing staff of important events and changes;
– security monitoring and control – comparing actual practice with the planned policy, performing a security audit, reviewing incidents, monitoring system activity, collecting and analysing information, and checking employee awareness of security principles"[11].

10. K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, 2nd ed., Warszawa, PWN, 2017, p. 17.
11. S. Wojciechowska-Filipek, Z. Ciekanowski, op. cit., p. 157.

Each of the above elements affects the quality of the implemented information security policy. It may appear that preparing such a document is not a challenge for an organisation or institution. Unfortunately, this is a mistaken assumption. In the era of the information society, the rapid pace of change and the dynamic development of new forms of communication make it essential to introduce a properly prepared security policy that incorporates all the necessary elements of information protection.

The general data protection regulation – GDPR

Since 1997, Poland has operated under the Personal Data Protection Act (UODO), which regulates the principles of personal data processing and the obligations of the data controller. The Act was introduced in response to the need to implement the provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[12].

However, it was not until the repeal of the aforementioned directive and "the entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation – GDPR) that a social shock occurred"[13].

"The personal data processing rules that had been in force for 21 years were not replaced but updated and significantly reinforced. (...) The protection system continues to rely on fundamental principles, such as purpose limitation, data minimisation, and storage limitation; it still requires a legal basis for processing and tightens this requirement for sensitive data; it still grants data subjects the right to access, rectify and object to the processing of their data, etc. However, elements of this framework have been modernised due to the growing influence of the Internet and new technologies on personal data protection"[14].

12. G.P. Wójcik, *Obowiązki przedsiębiorców wynikające z RODO*, 1st ed., Warszawa, CeDeWu, 2021, p. 13.
13. A. Sobczak, *RODO Rozproszona władza publiczna,* 1st ed., Kraków, Wyd. Uniwersytetu Jagiellońskiego, 2019, p. 11.
14. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa, C.H. Beck, 2016, p. 6.

Figure 1. The ten most significant changes introduced by the GDPR

1. Direct liability of the data processor
2. Data breach notification
3. New and expanded citizens' rights
4. Profiling restrictions
5. Appointment of a data protection officer (DPO)
6. Data inventory and documentation requirements
7. Consent
8. Expanded information obligations
9. Data protection impact assessment
10. Data transfers outside the European Union

Source: G.P. Wójcik, Obowiązki przedsiębiorców wynikające z RODO, 1st ed., Warszawa, CeDeWu, 2021, p. 17.

"Ensuring the proper protection of processed data, especially personal data, is gaining increasing importance. Processing of such data may have negative consequences for society (as a collective) and for individual members thereof.

Cyberattacks resulting in data leaks, the rise of cybercrime, identity theft, the illegal sale of data for marketing purposes, and the uncontrolled and unlawful processing of data are just some of the socially harmful phenomena that must be eliminated in the public interest. (...)

Ensuring the protection of personal data is also essential for individuals, as it affects the effectiveness of the right to privacy. This right encompasses principles and rules relating to various spheres of an individual's life, with their common denominator being the individual's right to live their own life in accordance with their own will, with external interference limited to the absolute minimum"[15].

In Poland, the regulations began to apply directly on 25 May 2018. A new supervisory authority for personal data protection was established – the President of the Personal Data Protection Office (PUODO), who replaced the former supervisory authority – the Inspector General for the Protection of Personal Data (GIODO).

The GDPR applies to every EU-based entrepreneur who deals with personal data. The responsibility for compliance lies with the Data Controller, i.e. the organisational unit that determines the purposes and means of personal data processing – in this study, it is the Agricultural Social Insurance Fund (KRUS). This institution was

15. M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych,* Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018, p. 21.

established under the Act of 20 December 1990 on the Social Insurance of Farmers[16], which, pursuant to Article 2(1) of the said Act, provides that the Fund administers farmers' social insurance. The Agricultural Social Insurance Fund is managed by the President of the Fund, who is a central body of government administration.

A recommended good practice is the appointment of a Data Protection Officer (DPO). The GDPR does not provide a definition of this role, and its provisions only refer to the DPO's place within the organisation's structure and the tasks assigned to them.

An enterprise should have internal regulations in place concerning the protection of personal data. These must define the security measures applied to maintain data integrity, confidentiality and accountability, as well as the availability of processing systems and services.

At the Agricultural Social Insurance Fund (KRUS), a Security Policy for the Protection of Personal Data and Instructions for Managing IT Systems Used for the Processing of Personal Data in KRUS were introduced by Order No 15 of the President of KRUS of 9 July 2024. These documents set out the principles, procedures and responsibilities concerning personal data protection.

According to the GDPR, "each entity must independently assess the risk that the processing of personal data may pose to the rights and freedoms of the data subjects. These values must be the primary consideration"[17].

The GDPR "does not explicitly refer to a risk management process or indicate a specific method for conducting such an assessment. Each entity must carry it out independently, taking into account many factors specific to it, such as: size, organisational structure, technical capabilities, the scope and type of data, and the purpose of processing. One effective systematic method of risk assessment is the implementation of a risk management process within the organisation"[18].

At this point, it is worth highlighting the importance of personal data protection in particularly demanding circumstances, such as those brought about by the COVID-19 pandemic, especially in connection with the increase in remote working.

To begin with the most important point – remote work does not exempt one from complying with the GDPR. "The GDPR provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics' in accordance with national law and under the conditions

16. Ustawa z dnia 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników, Dz.U. 2024 poz. 90 ze zm.
17. UODO, https://uodo.gov.pl/pl/126/208, access 7.02.2025.
18. Ibidem.

specified therein (...)"[19]. Remote work is permissible and has a legal basis, but in order to safeguard personal data protection, adherence to established standards and recommendations is essential.

The Personal Data Protection Office (PUODO) issued guidelines concerning data security when working outside the office. These relate to the use of devices, email, and access to networks and cloud services. It is essential to remember that equipment and software provided by the employer are to be used solely for professional duties. Users must always act in accordance with the security procedures adopted by the organisation[20].

Remote work entails a number of obligations in the field of personal data protection. It is equally important to ensure full compliance with the provisions of the GDPR. This applies to both employees and employers. Only strict adherence to the rules and guidelines will ensure the security of work and protect against the risk of data loss or leakage.

Personal Data Protection at the Agricultural Social Insurance Fund

Pursuant to Article 59(3) of the Act of 20 December 1990 on the Social Insurance of Farmers and Article 24 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, p. 1), the following were introduced at the Agricultural Social Insurance Fund (KRUS) by Order No 15 of the President of KRUS of 9 July 2024:

1. KRUS Security Policy for the Protection of Personal Data.
2. Instructions for Managing IT Systems Used for the Processing of Personal Data at the Agricultural Social Insurance Fund[21].

These documents are important guidelines aimed at ensuring compliance with both EU and national legal provisions concerning the secure processing of personal data.

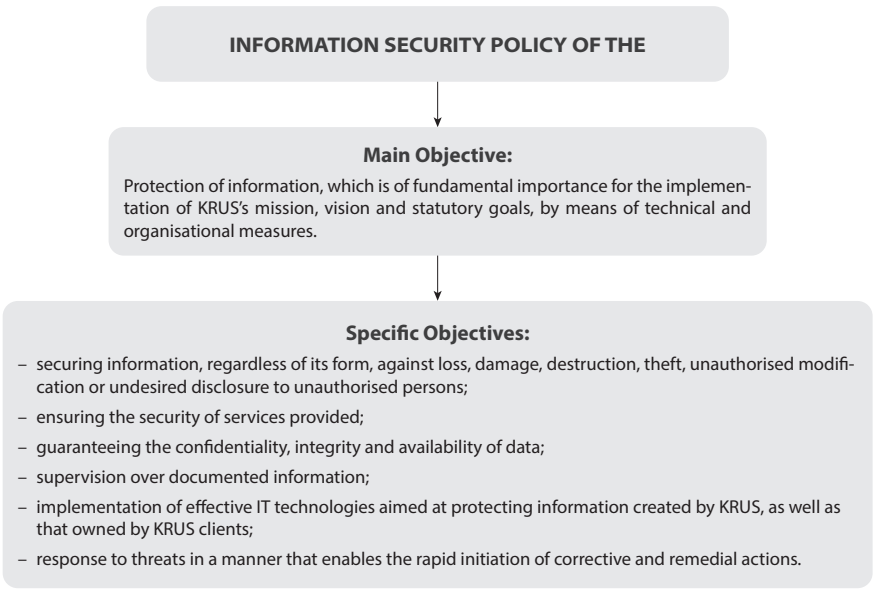
19. UODO, https://uodo.gov.pl/pl/138/1463, access 26.04.2022; Statement by Andrea Jelinek, Chair of the European Data Protection Board, on the processing of personal data in the context of the COVID-19 pandemic, 19 March 2020.
20. UODO, https://uodo.gov.pl/pl/138/1459, access 26.04.2022.
21. Zarządzenie Nr 15 Prezesa Kasy rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, Dz. Urz. KRUS 2024 poz. 16.

Additionally, to ensure the proper protection of KRUS's other information assets, the Information Security Policy was developed and implemented. Its main purpose is to protect assets by maintaining, improving and developing the information security management system (referred to within KRUS as the Integrated Management System), which facilitates the identification of threats and minimisation of the risk of data loss. This system is in place across all units and organisational structures of KRUS and is compliant with the following:

1) standards: ISO 9001, ISO/IEC 27001 and ISO 37001, Order No 3 of the President of KRUS of 2 February 2023 on the maintenance and development of the Integrated Management System at KRUS, based on the requirements of applicable standards: ISO 9001, ISO/IEC 27001 and ISO 37001, and on the definition of responsibilities within the Integrated Management System;
2) standards of managerial control for the public finance sector.

It is worth noting that all KRUS employees have access to the said Integrated Management System, which enables them to stay up to date with new guidelines, review the internal legal regulations in force, and fulfil the requirement – twice a year – of passing knowledge tests aimed at verifying their understanding of the tasks performed and the procedures in force.

Figure 2. Objectives of KRUS's Security Policy



Source: Own elaboration based on „Księga Zintegrowanego Systemu Zarządzania KRUS", 23rd ed., 1.10.2024.

The person responsible for performing tasks related to the processing and protection of personal data is the Data Protection Officer (DPO) – that is, the Director of the Office for Crisis Management, Defence and Information Security at the KRUS Head Office, appointed by the President of the Fund. The responsibilities of the DPO include:

1) "informing the Data Controller (the Agricultural Social Insurance Fund) and the employees who process personal data about their obligations arising from data processing and advising them in this regard;
2) monitoring compliance with personal data protection regulations, including the Security Policy and Instructions, as well as the distribution of responsibilities and activities to raise awareness;
3) providing recommendations on data protection impact assessments and monitoring their implementation, including carrying out inspections in KRUS regional branches in this area;
4) drafting guidelines and recommendations concerning personal data protection;
5) cooperating with the supervisory authority and acting as the contact point for the authority on matters related to processing, including prior consultations, and, where applicable, conducting consultations on any other issues;
6) drafting and updating the Security Policy and Instructions and ensuring compliance with the rules set out therein;
7) maintaining a consolidated register of personal data filing systems processed within the Fund"[22].

The Data Protection Officer collects documentation of the risk analyses conducted at KRUS regarding identified personal data protection risks and the plans to mitigate those risks, and raises employee awareness at KRUS concerning the risks and security incidents related to personal data protection. The DPO also maintains a consolidated data register within the Fund, which compiles registers of data filing systems submitted by: the Information Security Coordinator – KBI (each director of a KRUS regional branch), and the Personal Data Filing System Coordinator – KZDO (each head of an organisational unit at the KRUS Head Office). The register is kept in either electronic or paper form.

The responsibilities of the Information Security Coordinator (KBI) and the Personal Data Filing System Coordinator (KZDO) include, among others:

1) "organising personal data processing and ensuring its security through the implementation of appropriate technical and organisational measures designed to effectively apply the principles of data protection and to introduce necessary safeguards into the processing to meet the requirements of the GDPR and to protect the rights of data subjects;

22. Polityka bezpieczeństwa w zakresie ochrony danych osobowych Kasy Rolniczego Ubezpieczenia Społecznego, załącznik nr 1 do zarządzenia nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r.

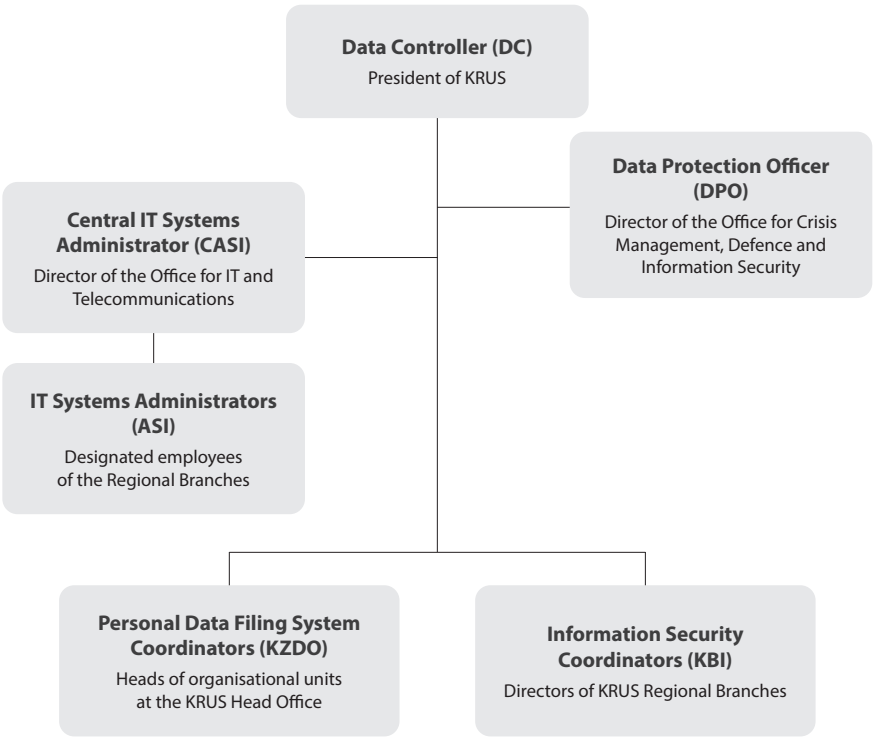
2) implementing appropriate technical and organisational measures to ensure that only personal data necessary to achieve each specific processing purpose is processed;
3) conducting systematic assessments, through risk management processes, of whether the level of security is adequate – taking into account the risks associated with the processing of personal data, in particular the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise processed;
4) deciding on the disclosure of personal data to other individuals or entities;
5) in the case of delegating the processing of administered data to another entity, preparing and concluding a personal data processing agreement;
6) notifying the Data Protection Officer (DPO) of the personal data filing systems for which they are coordinators, and reporting any need to update or delete such systems;
7) promptly informing the DPO, in accordance with the procedure laid down in the Integrated Management System (hereinafter referred to as "IMS"), of identified irregularities and incidents in the area of personal data protection concerning the administered filing systems;
8) cooperating with the DPO to improve methods and techniques of securing and protecting personal data filing systems;
9) supervising the principles for protecting, storing and destroying backup copies of personal data filing systems; (...)
10) submitting to the DPO, by 20 January each year, an annual report for the previous year, covering the number, subject matter and recipients of the personal data made available;
11) granting, modifying and revoking authorisations for individuals to process personal data within the assigned systems/filing systems (...).
12) furthermore, KBI and KZDO are responsible for maintaining:
    – a register of persons authorised to process personal data in filing systems;
    – a register of authorisations issued to IT System Administrators;
    – a register of persons authorised to perform the function of IT System Administrator (ASI) (...);
    – a register of personal data filing systems processed at the Fund (...);
    – a register of processing activities (...), which must be submitted to the DPO upon each update;
    – a register of disclosures of personal data (...);
    – a list of buildings, rooms or parts of rooms that constitute areas in which personal data is processed, which must also be submitted to the DPO upon each update"[23].

23. Ibidem.

The broad scope of responsibilities assigned to the directors of KRUS regional branches enables them to properly carry out official duties related to information security and personal data protection. It is important to remember that the organisational units of KRUS – namely, the regional branches and their subordinate local offices – are the primary point of contact between employees and KRUS's external clients, including the insured, benefit recipients, and contractors carrying out delegated tasks. This is why it is so important that individuals acting as Information Security Coordinators (KBI) properly perform the duties assigned to them.

As previously mentioned, the above tasks are also carried out by the heads of organisational units at the KRUS Head Office – i.e. directors of substantive departments and plenipotentiaries of the President appointed to lead designated teams. The work they perform as part of their responsibilities should likewise reflect the requirements of KRUS's Security Policy.

Figure 3. Structure of functions assigned under the KRUS Security Policy



Source: Own elaboration based on: Zarządzenie nr 15 Prezesa KRUS z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych and Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Given that the processing of personal data largely occurs through software and IT systems specifically designed for this purpose, it is important to highlight two key roles: CASI (Central IT Systems Administrator) and ASI (IT Systems Administrator). The President of the Fund appointed the Director of the Office for IT and Telecommunications at the KRUS Head Office as the Central IT Systems Administrator. The CASI is primarily responsible for:

1) "managing central IT systems, in particular implementing within these systems rules stemming from legal provisions, and – in the case of IT services provided by external entities – ensuring and preparing the draft of personal data processing agreements;
2) organising and coordinating training for persons designated to perform the duties of IT Systems Administrators regarding personal data processed electronically using an IT system;
3) exercising substantive supervision over the activities of ASIs employed at the Head Office;
4) issuing technical guidelines and instructions to ASIs in the organisational units of the Fund"[24].

The individuals appointed as IT Systems Administrators (ASI) are responsible for overseeing the correct operation of systems. Each "ASI is accountable for the functioning of IT systems, particularly for:

1) maintaining and upgrading the technical-system infrastructure;
2) registering and deregistering users in the IT system;
3) granting permissions for specific functions;
4) defining password change procedures and frequency, as well as password creation rules;
5) performing data backup procedures, ensuring their secure storage, verifying backup integrity, and overseeing their deletion;
6) implementing procedures in the event of personal data protection breaches;
7) conducting training for individuals designated to perform tasks related to the processing of personal data, covering the protection of personal data processed in electronic form using an IT system, taking into account the internal regulations in force at the Fund"[25].

Both of these roles are essential in ensuring and supervising the proper protection of IT systems. Information security must cover the aforementioned information system assets as well as the processing of the data they contain.

24. Ibidem.
25. Ibidem.

As stipulated by the GDPR, each organisation assesses the risk to the data subjects whose personal data it processes. It is therefore essential to follow the established rules.

Based on this, the Agricultural Social Insurance Fund processes personal data in accordance with the following principles:

1) lawfulness, fairness and transparency;
2) purpose limitation;
3) data minimisation;
4) accuracy;
5) storage limitation;
6) integrity and confidentiality.

A person whose personal data is processed at KRUS has the right to request from the controller access to their data, the right to rectification, erasure or restriction of processing, the right to withdraw consent at any time (if processing is based on consent), and the right to lodge a complaint with the supervisory authority (i.e. the President of the Personal Data Protection Office – PUODO) if they believe their personal data is being processed in breach of the General Data Protection Regulation[26].

In the event of a personal data breach, it must be reported to the supervisory authority without undue delay – no later than 72 hours after the breach is identified, and this decision lies with the Data Controller (DC). Organisational units of the Fund, acting as data processors, report the breach to the DPO.

According to the relevant order, the Data Protection Officer is required to document all incidents involving breaches of personal data protection and the actions taken to prevent similar events in the future.

"Any employee who discovers or suspects a personal data protection breach, whether in the system or on traditional media, is obliged to immediately inform their supervisor or the appropriate ASI, KBI, KZDO, or CASI, who then notifies the DPO, who in turn informs the DC"[27]. Following identification and confirmation of the incident, an explanatory procedure is conducted and corrective actions are taken.

The imposition of duties on KRUS employees ensures the prompt detection of breaches and enables better verification of any shortcomings. The purpose of corrective measures is to eliminate similar incidents in future operations of the Fund.

The Security Policy for the Protection of Personal Data of the Agricultural Social Insurance Fund also obliges all its organisational units to compile a list of buildings, rooms or parts of rooms that constitute the area in which personal data is processed. A consolidated register of these areas is maintained by the Data Protection Officer at KRUS.

26. Ibidem.
27. Ibidem.

To ensure the physical security of the data processed at the KRUS Head Office, regional branches, and subordinate local offices, access control is implemented for buildings and rooms where personal data is processed.

At the Head Office, supervision of this control is exercised by the Director of the Office for Administration and Investments, while in the regional branches and subordinate local offices, it is overseen by the Information Security Coordinators (KBI). In addition, all KRUS employees are required to be familiar with the "Instructions on Basic Security Rules for KRUS Employees"[28], which set out the basic principles for information security in daily operations. Controlling access to buildings and rooms significantly impedes unauthorised individuals from accessing data that should not be disclosed to persons lacking appropriate authorisation.

As previously mentioned, Annex 2 to Order No 15 of the President of the Agricultural Social Insurance Fund of 9 July 2024 is the Instruction on the Management of IT Systems Used for the Processing of Personal Data at the Agricultural Social Insurance Fund, which was developed to establish rules for processing personal data in the IT systems used by the Fund. Accordingly, the Office for IT and Telecommunications at the Head Office developed a set of procedures, which have been published in the KRUS Integrated Management System.

KRUS employees, as users of systems processing personal data, must have a unique user ID and password for authentication and access control. All personal data processed in the Fund's IT systems is stored on electronic data carriers, which are characterised by durable data storage. The correctness of storing and labelling information carriers containing personal data is the responsibility of: CASI – in the KRUS Head Office, and KBI – in regional branches and local offices, both of whom are also responsible for making backup copies.

"In the event of detecting or suspecting an incident threatening the security of the IT system, the procedures in force at the Fund must be followed"[29].

All of the above-mentioned principles, procedures and methods of handling personal data aim to ensure proper protection of access to such data, its correct processing, and secure storage with restricted access – limited only to authorised employees of the Agricultural Social Insurance Fund.

28. Instrukcja podstawowych zasad bezpieczeństwa dla pracowników KRUS, 15th ed. 16 August 2021.
29. Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Kasie Rolniczego Ubezpieczenia Społecznego, załącznik nr 2 do zarządzenia nr 17 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 24 maja 2018 r.

Summary

"The security threats faced by the information society are real and present in the daily reality of any entity, therefore becoming acquainted with, achieving, maintaining and enhancing information security is essential for ensuring an organisation's competitive advantage, financial liquidity, profitability, and legal compliance"[30].

In recent years, the concepts of "secure" processing, storage, and transmission of information have taken on new importance. Platforms such as WikiLeaks have made it clear that even highly classified documents can be disclosed quickly, easily, and anonymously. For this reason, users of modern technological conveniences must pay close attention to how and in what form they transmit their information or documents. The trust previously placed in applications and systems once used without hesitation has long since been undermined. The same concern arises among those responsible for broadly understood information processing, or those who own such information, who increasingly lack confidence in existing safeguards and are seeking newer and better ways to ensure that their information is protected. Personal data collected and processed by organisations, companies and institutions must be protected not only by law but also by additional systems that ensure their appropriate use and secure storage. No institution can afford to lose or disclose data belonging to its clients – be they internal or external.

Therefore, the development of a robust Information Security Policy is of crucial importance for an institution such as the Agricultural Social Insurance Fund (KRUS). The tools defined in this policy are intended to ensure proper protection of information. Regular evaluations of existing safeguards are also essential – this includes audits, which serve as inspections to assess the methods and outcomes of task implementation in terms of their compliance with specific requirements, standards, or norms. The audit evidence collected allows for an informed evaluation, while the adopted security measures and organisational solutions ensure adequate protection against the improper release of information that is meant to remain secure. This is particularly important for personal data protection.

Information security at KRUS has been ensured, among other means, through the internal regulation entitled "Information Security Policy of the Agricultural Social Insurance Fund". Its aim is to "identify the actions that need to be taken, and

30. I. Oleksiewicz, W. Krztoń, op. cit., p. 9.

to establish rules and principles to be applied in order to properly protect personal data during processing – both in paper form and in IT systems"[31].

A key role in implementing these actions is played by the Data Protection Officer (DPO) at KRUS, who acts on behalf of the Data Controller – the President of the Fund – to fulfil obligations under the GDPR and the Act of 10 May 2018 on the Protection of Personal Data, and ensures the proper operation of the protection system. Given the size of the organisation and the volume of personal data processed, the Data Controller has delegated most tasks to regional branch directors (KBI) and heads of organisational units at the Head Office – i.e., directors and team leaders (KZDO), who oversee the activities of KRUS's organisational units. This solution has enabled KRUS to comply with the GDPR and the aforementioned act without restructuring its organisational framework.

The comprehensively developed "Information Security Policy of the Agricultural Social Insurance Fund" provides a clear indication that personal data protection at this institution is effectively secured. As outlined in the previous chapter, the core objective of the policy is to protect information assets by maintaining, improving and developing the Information Security Management System (Integrated Management System), which makes it easier to identify threats and minimise the risk of data loss.

It is worth emphasising that the security policy and its supporting documents offer a well-structured and concise framework for handling data that must be protected – both in the interest of KRUS and its internal and external clients.

However, legal and system safeguards alone do not guarantee that information security breaches will never occur. That is why the human factor, which may breach regulations either accidentally or intentionally, must be properly trained.

The continuous development of digital technologies, including artificial intelligence, and the growing importance of information, call for constant monitoring and analysis of the topic. Consequently, continuous updates to requirements and security measures are necessary.

In the event of an information security breach, it is crucial to analyse the incident, draw appropriate consequences and conclusions, and introduce any necessary changes to prevent recurrence.

In the age of a rapidly evolving information society, numerous new challenges and opportunities emerge. It is vital to address as many of these challenges as possible. Today, the most important ones include: threats to security, independence from the

31. Polityka bezpieczeństwa w zakresie ochrony danych osobowych Kasy Rolniczego Ubezpieczenia Społecznego, załącznik nr 1 do zarządzenia nr 15 Prezesa Kasy Rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r.

Internet, and information manipulation. It is necessary that future strategies for social development take these challenges into account – even if their complete elimination is not possible.

It is currently difficult to clearly determine which of these challenges is the most pressing. Rapid social change and the constant development of the modern world make predicting the future course of these changes especially difficult.

Bibliography

Aleksandrowicz T.R., *Analityk informacji w administracji rządowej* [in:] *Analiza informacji w zarządzaniu bezpieczeństwem. Zarządzaniem bezpieczeństwem*, red. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa, Wyd. Difin SA, 2013.

Błażewski M., **Behr J.**, *Środki prawne ochrony danych osobowych*, Wrocław, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2018.

Gumularz M., **Kozik P.**, *Ochrona danych osobowych. Kontrola i postępowanie w sprawie naruszenia przepisów. Poradnik ze wzorami*, Wydanie 2, Warszawa, Wolters Kluwer, 2022.

Instrukcja podstawowych zasad bezpieczeństwa dla pracowników KRUS, Wydanie XVII, 28 października 2024.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz. U. nr 78 poz. 483 ze zm.

KRUS, *Przetwarzanie danych osobowych*, https://www.gov.pl/web/krus/przetwarzanie-danych-osobowych--rodo, access 26.04.2022.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/679*, Warszawa, C.H. Beck, 2016.

Księga Zintegrowanego Systemu Zarządzania KRUS, Wydanie XXIII, 1 października 2024.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydanie II, Warszawa, PWN, 2017.

Oleksiewicz I., **Krztoń W.**, *Bezpieczeństwo współczesnego społeczeństwa informacyjnego w cyberprzestrzeni*, Warszawa, Rambler Press, 2017.

Oświadczenie Przewodniczącej Europejskiej Rady Ochrony Danych Andrea Jelinek w sprawie przetwarzania danych osobowych w kontekście pandemii COVID-19 z 19 marca 2020 roku.

Sobczak A., *RODO Rozproszona władza publiczna*, Wydanie I, Kraków, Wyd. Uniwersytetu Jagiellońskiego, 2019.

UODO, https://uodo.gov.pl/pl/138/1459, access 26.04.2022.

UODO, https://uodo.gov.pl/pl/126/208, access 7.02.2025.

Ustawa z 6 września 2001 r. o dostępie do informacji publicznej, Dz. U. 2022 poz. 902.

Ustawa z 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2019 poz. 1781.

Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. 2024 poz. 632 ze zm.

Ustawa z dnia 20 grudnia 1990 r. o ubezpieczeniu społecznym rolników, Dz. U. 2024 poz. 90 ze zm.

Wojciechowska-Filipek S., **Ciekanowski Z.**, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni. Jednostki-Organizacji-Państwa*, Wydanie II, Warszawa, CeDeWu, 2019.

Wójcik G.P., *Obowiązki przedsiębiorców wynikające z RODO*, Wydanie I, Warszawa, CeDeWu, 2021.

Zarządzenie Nr 15 Prezesa Kasy rolniczego Ubezpieczenia Społecznego z 9 lipca 2024 r. w sprawie wprowadzenia w Kasie Rolniczego Ubezpieczenia Społecznego Polityki bezpieczeństwa w zakresie ochrony danych osobowych oraz Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, Dz. Urz. KRUS 2024 poz. 16.

received: 10.02.2025
accepted: 18.04.2025