ECONOMICS AND CULTURE 21(2), 2024

DOI: 10.2478/jec-2024-0028

SYSTEMATIZATION OF PROCESSES OF VALUE-CREATING ACTIVITIES OF OPERATIONAL SUSTAINABILITY AND SOCIAL RESPONSIBILITY

Radka Vanickova

University of Economics and Management, Department of Management, Narozni 2600/9a,

158 00 Prague, Czech Republic, e-mail address: radka.vanickova@vsem.cz, ORCID: https://orcid.org/0000-0003-3559-5799

Received 20 May 2024; accepted 4 November 2024

Abstract

Research purpose. The primary objective is to create a proposal for a project on the implementation of GDPR into the process management of an organization. The secondary goals include an assessment of compliance with obligations under GDPR for the benefit of the analysed institution, as well as the identification of individual processes involving personal data processing across the organization.

Design / Methodology / Approach. In the theoretical-methodological part of the paper, literary research was done through a comparison of expert texts by both domestic and foreign authors, including legal regulations, directives, internal resources, and data, etc. Empirical data and results were obtained from internal sources per the formulation of research questions and objectives, as well as applied scientific research analyses. In the analytical part, the qualitative and quantitative research methods, semi-structured interviews, questionnaire surveys, analysis of internal documents, data and results comparison, synthesis and deduction method, data audit, and GAP analysis were used. The significance and contribution of GAP analysis enabled the delineation of project scope and prediction of individual project activities for implementation of the project proposal.

Findings. The semi-structured interview highlighted shortcomings in meeting requirements under GDPR. This finding was confirmed by analysis of internal documents and their comparison with information obtained in the theoretical part of the paper, which confirmed the absence of internal regulations for personal data protection and employee training. A questionnaire survey among employees revealed gaps in security and legal processes. Through data auditing and GAP analysis, weak points were identified between the planned and actual state of GDPR compliance within the organization´s established processes. The weaknesses revealed incomplete records of personal data processing activities, absence of data processing agreements, employee training, establishment of internal data protection processes, low level of implementation of legal and legislative regulations, and inadequate performance of the role of Data Protection Officer. The scope of the project proposal for achieving GDPR compliance was defined in 16 activities, including ensuring an adequate Data Protection Officer, avoiding excessive collection of unlawful and unnecessary personal data, and reviewing internal regulations. The project duration was planned for 72 days, or 52 working days in a calendar year, with a total cost of 1933,33 EUR. Based on obtained results, it can be concluded that the project is feasible, and the objective of the project was achieved.

Originality / Value / Practical implications. In conclusion, it is ascertained that the objective of the paper has been achieved: the project proposal has been implemented into the internal regulations of the organization. This ensures that the Data Protection Officer is adequately positioned and that processes and internal regulations for the security and protection of personal data are in place. The economic added value of the project is a return on invested costs of training, while social value is in societal benefits for people, and efficiency of spent resources is ensured by the sustainability of the project beyond established processes, allowing for new inputs in future. The potential of the paper lies in focusing on the effectiveness of costs allocated to the project and the effectiveness of established processes in terms of resource use in personal data processing.

Keywords: system process management; General Data Protection Regulation; personal data; data audit; GAP analysis.

JEL-Codes: K00; K19; K39.

* Corresponding author: vanickovaradka@gmail.com

Introduction

Personal data protection concerns any individual, natural, or legal persons and organizations all over the world, as it is part of human rights and freedoms, with the primary aim of protecting and preventing misuse. Personal data is provided to various institutions, e.g., when opening a customer loyalty card in a brick-and-mortar store, collecting a shipment from a carrier, sending a resume to a posted job offer, or filling in a complaint form for a purchased product.

Personal data includes basic identification and contact data of individuals, including photographs and audiovisual records, IP addresses, information on political opinions, as well as genetic and biometric data (Purificato et al., 2021). Some data can be sensitive to such an extent that its misuse may harm individuals in public and is thus protected by legislation. Personal data protection is integrated with the General Data Protection Regulation (GDPR) with effect from May 2018 for all EU Member states. One of the reasons for GDPR is human rights advocacy in event of unauthorized handling of personal data, with reference to Charter of Fundamental Rights and Freedoms and Act No. 101/2000 Coll., on personal data protection, which enables public and private organizations to process personal data beyond a set limit, provided that legal regulations and conditions for processing personal data are complied with and with consent of authorized person (Bellringer, 2022; Migeon & Bobbert, 2022). With the update of GDPR, the list of obligations has been extended; the change has resulted in the threat of non-compliance with the protection of legal regulations (Kunnapas, 2021). The added value of procedural management is the provision of a data protection officer with a record of processing activities. To comply with GDPR, organizations must accept and adhere to principles that arise from regulations, i.e., the data controller is only allowed to process selected personal data for a defined period (Pedrosa et al., 2020).

If the volume of personal data to process is too large and diverse, organizations do not have to deal with GDPR issues themselves. An example can be educational institutions processing the personal data of their employees, students/pupils, or legal representatives. As an extended service in the provision of advisory and consultancy services, such institutions offer the possibility to delegate (outsource) some of their responsibilities to (in compliance with GDPR) external entities (Barati & Rana, 2021; Cambronero et al., 2022). Some organizations may unintentionally violate GDPR by underestimating the importance of regulation, having a low portfolio of available knowledge, or insufficient monitoring of the scope of their obligations.

Literature Review

The constant development of technologies processing personal data may be a source of risk arising from a potential lack of security and misuse of data. An example is an intrusion into a school´s internal system to change data (Eva et al., 2022; Qin & Jiang, 2023). Regular assessment of management systemization and process improvement in line with GDPR and ESG principles is gaining importance and synergy in the potential benefits of shared processes (Peyrone & Wichadakul, 2023).

System process management

As mentioned by Bohmer (2023), any information on identified or non-identified natural person represents personal data, basic marking of which are e.g., names, surnames, date of birth, birth numbers, etc. Diamantopoulou et al. (2020) state that disclosure of birth numbers contradicts identification of persons, as it is considered specific data listed in Act No. 133/2000 Coll. and takes precedence in the processing of birth numbers; however, it does not exclude limited treatment of data in accordance with legislation. According to Beresecka et al. (2023), in some cases, the data controller does not consider the data they are processing, e.g., phone number, email or IP address, etc. as it is not purposed to raise doubts about the acquisition of the data. Hermanto et al. (2024) extended the list of personal data by other data, such as permanent address, contact address, bank account number, payment record, as well as data on previous purchases. Both Beresecka et al. (2023) and Hermanto et al. (2024) point to the category of special personal data, as its processing affects the privacy of the person concerned and thus requires more attention (Harper et al., 2022). An example of data processing can be found in the

education sector, which processes a considerable volume of personal data of pupils/students, their legal representatives, employees, and other persons in accordance with Act No. 561/2004 Coll. Educational institutions/schools are controllers designated by law, processing personal data themselves or through a processor, e.g., in the case of creating an external archive, payroll accounting, or security.

Personal data of entrepreneurs – natural persons are considered records subject to GDPR protection (Ketmaneechairat et al., 2024). Personal data processing is an act, or a set of operations or sub-activities performed systematically by a controller to retrieve, collect, record, organize, store, consult, use, disseminate, combine, align, restrict, erase, and shred it. Lachaud (2020) argues that the EU has created a public data protection system based on Directive No. 95/46/EC of the European Parliament and of the Council on protection of individuals concerning processing of personal data and on free movement of data (hereinafter referred to as "Directive No. 95/46/EC), as the EU responded to increasing number of data generated about individuals who did not have access to information (Lapwattanaworakul et al., 2023).

GDPR is not the only document associated with personal data protection, as stipulated in Act No. 110/2019 Coll., On Processing of Personal Data and Act No. 89/2012 Coll. of Civil Code, § 84 - § 90 (Vanickova & Bilek, 2021). Compliance with GDPR in the Czech Republic is ensured by the Office for Personal Data Protection (OPDP) (Yuan et al., 2021). Article 58 of GDPR specifies remedial powers of supervisory authority beyond administrative fines with a warning of violation of regulation or issuance of a warning without sanctions (Lisiak-Felicka et al., 2020). According to Article 83 of GDPR, the EU member states can set their own rules for imposing administrative fines on public authorities and public bodies per Section 62 of Act No. 110/2019 Coll. on Processing of Personal Data. According to Kurtz et al. (2018) and Sanz (2019), GDPR has contributed to making even laypersons become aware of the fact that handling of personal data cannot be arbitrary and therefore, it is necessary to introduce measures to prevent public handling and processing (Fieiras-Ceide et al., 2023). The right to information states that a data subject has the right to be informed of the processing of personal data at the time of their collection by the controller within a reasonable period depending on circumstances (Menges et al., 2021). The fulfilment of obligations is mostly implemented through notifications, mostly on organizations' websites (Gumilar et al., 2023). Exceptions when it is not necessary to inform the data subject of disclosure are specified in legislation (Garg et al., 2019). The right to the erasure of data cannot be considered an absolute right. Article 17 of GDPR defines strict conditions and exceptions under which this right can be exercised or denied even though the processing of personal data is suspended, i.e., the controller is allowed to handle personal data but not to process it (Pandit, 2023). The restriction of personal data lasts until particularity, overriding interest, or impossibility of further use by the data subject is assessed. The issue of erasure is not further specified; most often, personal data is anonymised in automated data processing (Di Cerbo et al., 2019; Fantoni et al., 2021). If the outcome affects an individual´s decision-making, it is not an automated decision. For example, in the case of schools and educational institutions, the automated decision is not required (Slawicki, 2020). Data subject reports imply obligations for entities, or personal data controllers, which they must incorporate into their internal processes to ensure that conditions are also in place for electronic submission of requests to identify individuals. The obligations imposed on data controllers by GDPR must be implemented in processes of value-creation activities, the management of which is most often carried out through project activities (Matulevicius et al., 2020).

Implementation of GDPR into system process management

The first step before implementing GDPR obligations into systemic process management is a risk analysis conducted to identify bottlenecks. Although it is not directly imposed by GDPR, Article 32 of GDPR considers the assessment of project risks´ effect on the effectiveness of sub-processes to be essential. Machova et al. (2022) suggest processes should be mapped beyond legally required documentation of contracts with suppliers. Other researchers such as Hatzivasilis et al. (2019) recommend applying a GAP analysis of personal data protection along with process mapping. The tools specified below are recommended for personal data processing in accordance with GDPR implemented

in business processes with data subject risks reflecting proportionality principles (Barati & Rana, 2021; Merlec et al., 2021).

Data audit and GAP analysis

As reported by Rosmawati et al. (2023), compliance audit and GAP analysis enable entities to set up methodological procedures and guidelines so that they consider data security (Orescanin et al., 2024). The synergistic effect occurs in saving time and reducing the amount of money invested in internal processes of value-creating activities, with emphasis on eliminating resource wasting, node analysis, data flows, personal data collection, input forms and contractual links with verifying data security in paper and digital form in integration with analysis of internal regulations and GAP analysis. In process mapping, Shabalina et al. (2020) suggest finding answers to questions "Who, What, Why, Who, Whom, When, and Where, how to collect personal data so that access is structurally identified and contractually secured to third parties including incident management?". The optimal output is to prepare an inventory of personal data for each activity linked to obligations and policies in accordance with GDPR and project risk (Goncalves et al., 2020). Project risk evaluation is addressed by Bloemendal (2022), who recommends identifying risks in GAP analysis with the aim of proposing standards, methodologies, and guidelines referring to research gaps and inconsistencies in the expected and planned state of project management.

Data protection impact assessment (DPIA)

Bellringer (2022) and Dewangan & Chandrakar (2023) argue that the necessity to assess Data Protection Impact Assessment (hereinafter referred to as "DPIA") arises with assumptions of high risk to rights and freedoms of natural persons, e.g., in systematic monitoring of public spaces in schools and educational institutions. During an inspection, the supervisory authority may request a justification as to why the identified risk has been evaluated as low or medium, and in case of a reduced validity value or biased classification, any difference can be evaluated as a breach of GDPR (Lubis et al., 2024). The Guidelines on Data Protection Impact Assessment outlines the application of DPIA by dividing it into individual stages, i.e., collecting information on the processing of personal data with DPIA analysis in monitoring compliance with principles and measures of GDPR with periodic review of data (Georgiou & Lambrinoudakis, 2021; Vazao et al., 2023). To determine whether DPIA is necessary, a list of types of data processing operations is created. The DPIA process monitors data coming in and out of subjects with the identification of risks and proposing possible solutions (Portillo-Dominguez & Ayala-Rivera, 2019; Raycheva et al., 2023; Veinhardt et al., 2023). Gobniece & Titko (2024) recommend primarily to perform DPIA in compliance with WP248 guidelines with the aim of verifying the relevance of data. Other authors state that if even one significant risk is identified, the controller is obliged to consult OPDP on the severity of findings and in accordance with the Prevention of Major Accidents (PMA) method, to assess consequences with the opinions of assessors (Georgiou & Lambrinoudakis, 2023; Hariyani et al., 2024;). Analysis of risk resources and assessment of accident risk aimed at preventing major accidents have a synergistic effect in the systemisation of management of the assessment process with a view to the future. The resulting score highlights the severity of the risk and appeals for urgency in taking rationalisation measures to eliminate risks and research gaps. Per the DPIA regulation that came into effect on 1 April 2023, assessment of consequences in the adoption of legislation is not mandatory, if it has already been assessed (Vanickova & Bilek, 2022).

Proportionality balancing test

Zieni & Heckel (2021) recommend using a proportionality balancing test in cases where the controller is authorised to process legal requirements. Rawindaran et al. (2021) refer to the application of a proportionality balancing test when using CCTV cameras in schools and suggest creating internal documents that will provide information on the retention period of CCTV footage and authorised access to footage. In relation to CCTV footage, Li (2024) advises that any viewing of footage should be regarding information obligation through information signs that warn about CCTV footage, e.g., who the data controller and processor are, what purpose of monitoring, what are subjects´ rights concerning disclosure of data to third parties, how long is retention period, etc. A debated topic in public is the

retention period of CCTV footage. Molina et al. (2023) believe that a reasonable retention period is three days, i.e., 72 hours. This is confirmed by Ahmed et al. (2020), who add that the retention period can be even longer if the organization has a compelling reason. Logachev et al. (2022) emphasize the archiving of written documentation as well as the marking of monitored areas. Other authors such as Di Sabato & Kozakova (2023) point to the necessity of integrating GDPR into operational activities, work processes, and guidelines, as well as business and technological changes throughout organizations while complying with GDPR (Merzeh et al., 2022). Lyulyov et al. (2024) admit that changing established processes and project activities of non-value-creating character are related to change management. If processes are to be managed more effectively, they need to be mapped so that sub-activities with a higher added value best meet corporate objectives and social benefits and contribute to business sustainability and accountability (Chochia et al., 2023).

Added value of systemic process management

Process management is an activity building on knowledge, skills, methods, practices, and tools of management identification and improvement (Capodieci & Mainetti, 2019). Establishing roles and responsibilities, process flow management, process efficiency evaluation, and identification of problems and causes are aimed at improving and supporting systemic management and application of communication tools and social channels for transmitting information and data and document digitalization and archiving.

The adaptation to constantly changing conditions influencing the development of the business while eliminating errors and risks, as well as identification of innovation opportunities meeting the requirements of stakeholders, creates values in systemic process management, the development potential of which has a positive impact on efficiency, which can then be measured, evaluated, and improved (Anywar et al., 2022).

Appropriately set established processes with monitoring, control audit, and specific changes in the company´s strategy appealing to increase in operational and financial performance are the motto of systemic improvement of a process-managed organization responding to market dynamics and growth rate, as well as to the development of substitutes and entry of new technologies with the transformation of organizational structure and changes in corporate culture and legislative restrictions in the field of resources (Barati et al., 2020; Sadigov, 2020).

Research Methodology

The primary goal of the paper is to create a project design for GDPR implementation into systemic process management. The secondary goals include the assessment of the current state of compliance with GDPR obligations in selected entities and the identification of personal data processing activities. To achieve goals, the following research questions were formulated:

- Is compliance with GDPR obligations transparent?
- Is the use of an external Data Protection Officer (DPO) more effective compared to delegating this task to a permanent employee?
- What is the relationship between data systems and employee attitudes towards personal data protection?
- Do employees have relevant information to ensure personal data protection and data security?
- Is personal data systemically protected from misuse by unauthorised persons?
- Is it necessary to revise all data in the personal data protection system?

Based on theoretical background and research findings, the following scientific assumptions were pronounced:

- If an organization does not carry out regular audits of outsourced services, it cannot ensure through compliance with GDPR obligations.
- In case of non-compliance with GDPR obligations, the organization lacks the capacity to independently ensure remediation.

The theoretical and methodological part of the paper builds on literary research, a comparison of domestic and foreign authors and legal regulations, legislation and directives, internal resources, and data analysis integrated with research questions and scientific assumptions. Due to the sensitivity of the data, an affidavit of confidentiality was signed, concerning misuse of personal data and information acquired by consulting internal documentation in the presence of an authorised person from management. The analytical part of the research includes qualitative research, semi-structured interviews, questionnaire survey, internal document analysis, comparison of data and results, methods of synthesis and deduction, data audit, and GAP analysis. The benefits, effects, and potential of GAP analysis enabled specifying the extent and quality of selected project activities with higher added value of project management applicable soon.

The primary step was conducting semi-structured interviews with a manager of the institution under study. The selected form of interview enabled a flexible response to information obtained during the interview. The analysis of internal documents allowed for the identification of GDPR obligations (see response to research question 1: "*Is compliance with GDPR obligations transparent*?" Based on the results acquired, a control checklist was prepared to assess compliance with GDPR requirements in terms of identifying matches, similarities, and differences. The semi-structured interview identified shortcomings in internal processes and analysis of internal documentation enabled specifying individual activities of the entity addressed. The control checklist included the basic obligations of an educational institution, for which assessment of the extent and quality of personal data obtained was necessary for the purpose of data processing, with emphasis on risk management and legislative measures. The research also showed non-compliance with GDPR obligations. The results confirm the first scientific assumption "*If an organization does not carry out regular audits of outsourced services, it cannot ensure through compliance with GDPR obligations*."

The second research question was formulated as follows: "*Is the use of an external Data Protection Officer (DPO) more effective compared to delegating this task to a permanent employee*?" The question was answered by comparing results in accordance with the scoring method. The obtained results showed whether it is more advantageous for an educational institution to use external or internal employees as a data protection officer. The identified advantages and disadvantages were scored in the interval 1 – 5 and ranked in order of importance. The highest score for advantages was 5, while in the case of disadvantages, it was 1. After the product of score values and the sum of cumulative advantage and disadvantage values, the weighting of criteria was set, the contribution of which consisted in independent assessment of eligibility of choice of alternative solutions. The findings from the semi-structured interview were used for the specification of a questionnaire survey among employees of the entity analysed for the purpose of personal data protection and data security. The respondents were asked 12 questions aimed at identifying the extent and quality of awareness of data protection and security. The questionnaire survey was distributed online (docs.google.com) between 24 April 2023 and 5 May 2023, with the participation of 83 % of employees. The results obtained were topics of responses to research questions 3a and 3b: *"Do employees have relevant information to ensure personal data protection and security?", "Is personal data protected systematically against unauthorised misuse by outsiders?"* As part of the so-called clean desk policy, an internal audit of handling personal data was performed on 5 May 2023 after working hours in cooperation with the management of educational institutions aimed at identifying risks and shortcomings. The audit confirmed a responsible approach of employees towards personal data protection. A secondary objective was an evaluation of the current state of compliance with GDPR obligations. To identify discrepancies between the planned and desired state, a GAP analysis was performed, preceded by a data audit. By analysing data, personal data collection nodes were created with the support of the management of the institution under study and authorised persons were assigned

to them. The data audit assessed selected activities carried out within data processing, with the definition of accesses, internal systems, contractual relationships, and security measures. Selected employees were tasked with detailed mapping of 51 activities in which personal data processing is conducted, in the period between 1 March 2023 and 31 March 2023. The output of the data audit was an analysis of personal data collection and a comparison of data resulting from GDPR. The GAP analysis identified gaps in the planned and future state of resulting values. Based on the interpretation of GAP analysis and data audit results, recommendations for changes integrated with rationalisation measures were proposed to systematically eliminate risks and strategically manage, measure, evaluate and develop processes in the setting of supporting activities and preventive measures in 18 selected areas, the development potential of which has higher added value. By answering 4th research question: "*Is it necessary to revise all data listed in the data protection system?"*, it was possible to formulate recommendations presented to the management of the institution under study with the aim of improving the current state and supporting the development of the future state in systemization of management processes integrated with GDPR.

Based on the results of the GAP analysis, it was possible to specify the extent and quality of 16 selected activities. For determining the significance of sub-activities, formulating methodological procedures, and time options, the Critical Path Method was applied to the network diagram through chains and nodes integrated with the date of project finalization, i.e., the shortest possible duration of the project and Gantt chart. The duration of the project was set at 52 working days in a calendar year. Risk analysis and method of Prevention of Serious Accidents (PSA) were used to determine risks and severity of consequences in conjunction with assessors´ opinions. Evaluation of project design with cost calculation, including selected project activities and real project duration, concludes the analytical part of the paper. The formulation of the overall conclusion and sub-conclusions based on the theoretical background, empirical data and scientific assumptions were carried out using the method of deduction.

The application of qualitative methods and practical results helped to fulfil the primary objective of the paper, i.e., creating the design of a project on the transformation of GDPR in internal processes, see the second scientific assumption "*In case of non-compliance with GDPR obligations, the organization lacks the capacity to independently ensure remediation*."

Research Results

At the beginning of the analytical part of the paper, a selected organization is introduced, which remains anonymous due to data sensitivity. The first part is aimed at evaluating the real state of GDPR implemented in the process management of the selected entity. The obtained results represent the basis for creating the design of the project on the transformation of management in the systemization of processes within value-creating activities, potential and contribution of which is primary.

GDPR in system process management

To ensure a holistic approach in the assessment of personal data protection and data security, internal documents, expert, and practical studies, as well as domestic and foreign published papers, were applied. To ensure data anonymisation, the identity of the analysed entity, which is a contributory organisation with up to 50 employees operating in education, was concealed. Therefore, the appointment of a data protection officer is a legal obligation (see Fig. 1).

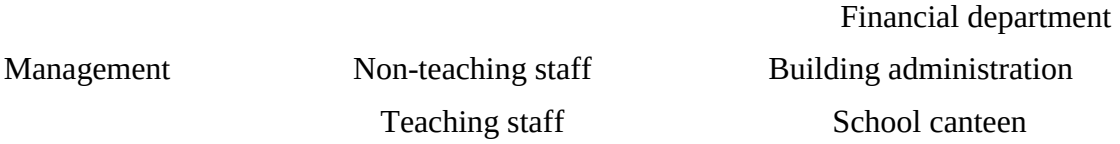


Fig. 1. Organization structure of selected educational institution (Source: Created by the author, 2024)

As seen in Figure 1, the management of the analysed entity is divided into two categories, teaching, and non-teaching staff, according to the specialization of individual departments dealing with economic, administration, and other activities. The building administration and school canteen staff have direct access to personal data, although to a limited extent.

Table 1. Evaluation of planned and performed activities (Source: Created by the author, 2024)

Ranking	Responsibilities	Ensured by	Value
1.	Data protection officer	Third-party company	√/x
2.	Records of processing activities	Third-party company	x
3.	Verification of contract processor	No record kept	x
4.	Reporting of personal data breach	No record kept	-
5.	Internal processes and documentation	Third-party company	√

The data protection officer performs the function of sourcing data and information published on the websites of analysed organisations and provides consultancy. As confirmed by the head of the interviewed entity (through a semi-structured interview) and documented in internal materials, the function is performed only partially, not comprehensively (see formulated research questions and scientific assumptions).

Records of processing activities are managed by a third-party company collecting information on training, OHS, accounting, and HR. The selected education institution states that it performs other activities beyond core and supporting activities, such as school canteen meals provided to staff and the public concerning social responsibility.

In contract processor verification, there is no record of personal data processors undergoing a process of verification of their competence in control and audit activities before signing a contract, as no record of processing contracts is available. Due to detected misconduct, contracts with external accounting and IT systems management companies were consulted, as revealed by a semi-structured interview with the Head, who stated that none of the contracts contained provisions for processing personal data.

The report on the breach of personal data security does not contain any record of incidents, as there was no incident in the monitored period. The internal data protection directive requires staff to report any breach of personal data security to the Data Protection Officer and report serious offences to the Office for Personal Data Protection (OPDP).

For purposes of mapping the current state of fulfilling GDP obligations, the above facts were considered (see Table 1). Employee training on personal data protection was not carried out, as confirmed in an interview with the director of the institution under study and by questionnaire survey. Although it is the responsibility of an external company to organize training for employees and managers under a mediation agreement, findings showed that the actual situation is different.

The process of submitting requests by data subjects shall be specified in the Information Memorandum, which, however, is not available. Data controllers are obliged to facilitate the exercise of rights of data subjects, e.g., through creating accessible forms to share consultative advice with DPOs and OPDP, producing a record of complaints and requests with the exercise of rights and consent to processing of personal data and submission of a list of internal regulations on processing of personal data and a list of personal data transmitted and processed by processors, concerning fact that management of analysed organization recommends, not mandates, written evidence of implementation of each activity.

Although the function of the Data Protection Officer is ensured, its performance is not effective, as the external company does not provide a comprehensive set of services resulting from the mediation

agreement. Incompleteness in records of activities concerning GDPR-compliant information under the responsibility of the data controller of the analysed entity can be considered serious misconduct.

Based on the results obtained, empirical data and conclusiveness of partial findings, it was possible to make a managerial decision on approaching an external or internal DPO in accordance with the application of a comparative method assessing the advantages and disadvantages of working with an external or internal DPO, see Table 2.

Table 2. Advantages and disadvantages of external and internal DPO (Source: Created by the author, 2024)

Advantages	**External DPO**	**b_i**	**Internal DPO**	**b_i**
	Continuous service	3 (0,14)	Direct presence in organization	5 (0,24)
	Knowledge of issue obtained in multiple organizations	4 (0,19)	Knowledge of environment	3 (0,14)
	Elimination of conflict of interests	2 (0,10)	Potentially lower costs for organization	4 (0,19)
Summary of advantages				
Disadvantages	Office outside organization	3 (0,16)	Paid holidays, sickness leave	3 (0,16)
	Lack of knowledge about organization	2 (0,11)	Training required	4 (0,21)
	Higher costs	5 (0,26)	Risk of conflict of interests	2 (0,11)
Summary of disadvantages				

In the context of managerial decision-making, the advantages, and disadvantages of having an external or internal DPO were rated according to b_i <1 and 5> score interval and significance. The highest score in terms of advantages was 5, while in case of disadvantages, it was 1. Based on previous experience of cooperating with an external company ensuring GDPR in incomplete compliance, direct contact with a DPO is essential; therefore, the location of the office directly in the organization is evaluated with 5 points compared to 3 points allocated to an office outside the organization. The work experience of a DPO in the same or similar field means a potential to develop knowledge capital (evaluated with up to 4 points). In terms of the time availability of DPO, the initial exercise of GDPR rights and obligations is particularly advantageous in terms of the availability of an internal employee. In the case of an external DPO, possible conflict of interest is almost eliminated, which is advantageous in terms of no direct contact. However, in the case of an internal DPO communicating with at least 3 competent persons, this appears to be a disadvantage, along with the costs of training an internal DPO. Nevertheless, in the long run, a return on investment is expected quantified in lower upfront costs. For an external DPO, an increase in labour costs represents a burden for the analysed entity (score up to 5 points). In terms of comparing advantages and disadvantages, the management of the analysed entity evaluated increases in costs for advisory and consultancy activities, e.g., in the form of preparing written documentation beyond the scope of the job, keeping records of new employees, training, etc. as disadvantageous. Based on the aggregate score for internal DPO, the result was favourable, which means that the analysed organization preferred an internal employee over an external one when selecting a DPO.

Data audit

The implementation of GDPR obligations into internal processes was not performed properly since the actual state does not correspond with the reported one. To implement remediation, the core and supporting processes of the entity under study need to be transformed to provide a detailed overview of sub-activities.

Based on the analysis and data collection, GAP analysis was applied to internal processes, which enabled the identification of gaps. The process of data audit is described in the following steps:

Step 1: Identification of personal data collection nodes

A total of 10 main personal data collection nodes were identified, with each node describing an area in which one or more activities related to personal data processing take place; each of the areas has its own responsible person). Figure 2 provides an overview of four nodes, i.e., four key activities within the internal processes of selected institutions.

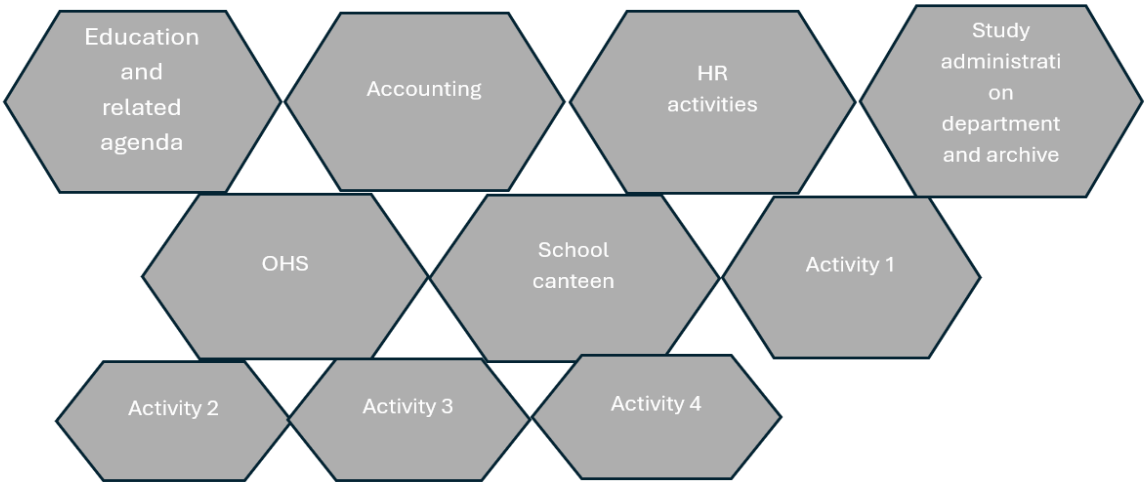


Fig. 2. Core processes – identification of nodes (Source: Created by the author, 2024)

The first row of nodes is related to the primary (core) activities of the analysed entity. The second row consists of supporting activities related to core processes. The third row presents other activities representing additional activities to internal processes. The additional services can be used by both students and employees beyond the primary target group.

Step 2: Identification of personal data processing activities

In each of the main nodes, multiple activities related to data processing can take place at the same time. The identification of individual functions was conducted using a questionnaire addressed to managers of selected areas in the analysed institution. Within 10 main nodes, a total of 51 activities related to operations within personal data processing were identified (see Fig. 3).

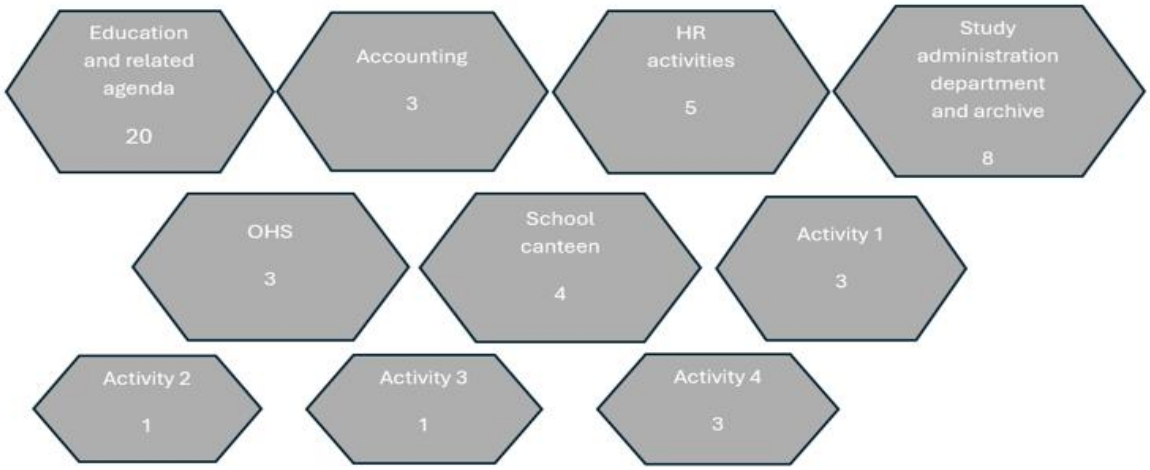


Fig. 3. Core processes with a number of activities related to personal data processing (Source: Created by the author, 2024)

For selected activities, the questionnaire survey primarily verified the purpose of personal data processing, retention period of documents, etc. Only 4 out of 10 nodes were complete. 3 out of 51 activities were identified as redundant, such as requesting the name of the health insurance company, ID card number, personal identification number, and permanent address. In 6 out of 51 activities, there was no sharing of subjects´ data that were processed and distributed. Another 10 activities out of 51 identified were not included in Filing and Shredding Rules and Procedures, there was no insertion in another selected document with an indication of the deadline for archiving and shredding. For none of the 51 activities, information on security incident management was published, which means that in the event of a breach of regulation, the system of incident reporting is operational. Given the GDPR directive, which refers to the obligation to report security incidents, it can be confirmed that employees of the selected institution analysed are not familiar with internal regulations and do not have knowledge applicable to managing processes of sub-activities related to GDPR.

The obtained results were compared with internal records on activities related to personal data processing performed by an external company. The objective assessment showed that for 6 out of 10 nodes, no record is kept, and in some cases, sub-activities specification in selected areas, such as school canteen (4 activities) and other activities performed by the study administration department and archive is missing.

The last activity in Step 2 was risk assessment. In two cases, it was specified that taking of CCTV footage and shredding of documents are activities related to personal data processing in a high-risk manner. The documentation provided by the external company did not include proportionality balancing tests or a Data Protection Impact Assessment (DPIA). The process of risk assessment was not started in the analysed institution. Risk identification and assessment including proposals for risk elimination measures in data protection and data security systems were absent. According to DPIA guidelines called WP248, it is necessary to set up a functional DPIA that would consider the security of the system.

Step 3 – specification of data flows

Step 3 deals with mapping IT systems and data flows dealing with the processing of personal data available to external employees.

Each of the identified nodes is extended by information on individual activities. For nodes with multiple activities, a sub-activity is given in selected job positions. The yellow arrows show the interconnectedness of internal employee activities. Regarding the performance of obligations, the management of the analysed institution has access to all processed data, while DPOs only have access

to selected activities related to the performance of their work position. The key activities and data flows are specified below:

- Secondary education and school activities – a total of 15 activities in the "Bakaláři" system, with teachers or class teachers only having access to 13 of them. Data in the internal system are accessible to selected persons only. The remaining two activities are related to the creation of websites, where 1 activity deals with the transfer of footage from the CCTV system to the internal system. The collected data are only accessible to internal representatives of the IT department and external IT company that manages the "Bakaláři" system, including building management.
- HR activities – payment system used in 1 activity. Data are distributed to an external accounting company and representatives of the analysed subject verbally in terms of management of the attendance system and access to system management. Other data in a printed form are processed by the HR officer (no further data transfer is performed).
- Accounting – an accounting program is used for selected activities, accessible by internal accountants and representatives of specific subjects. A bank account is available for all activities and is operated by the internal accountant and the school management.
- Study administration department and Archive – the study administration department clerk is responsible for selected activities. For 3 out of 8 activities, information is accessible also to class teachers. In 4 cases, processors who hold personal data are addressed, in 2 of which they communicate with representatives of the "Bakaláři" system, e.g., representatives of Alive, a shredding company that provides ISIC cards through the National Cancer Database (NCDB) portal. Written documentation is physically transported using special security boxes designed for shredding. Through a shared drive, data are mediated between the study administration department clerk and the management of the analysed institution.
- OHS – authorisation for documentation related to OHS is the responsibility of an HR officer in charge of keeping records of accidents and training and related documentation. The building manager acts as an internal employee responsible for OHS, as they have access to training materials. In the event of an accident, the accident is reported to the health insurance company via email in accordance with Section 29 of the School Act.
- School canteen – a total of 3 activities are linked to the diners´ portal managed by the manager of the school canteen and internal accountant. The shredding process takes place at the end of each working day.
- Activity 1 – selected activities are performed in the Alpha internal portal operated by a study administration department clerk and selected teachers. The data are accessible both by Alpha representatives and data processors.
- Activity 2 – implemented under the guidance of a selected teacher. In some cases, upon request of the subject, personal data can be shared via email, although it is not a standard. The data are kept in a printed form and stored in the school office (no further data transfer takes place).
- Activity 3 – is performed in cooperation with selected teachers and management. Data processing is performed in the Beta system and data are accessible to portal representatives, system managers, and processors.
- Activity 4 – The GAMA portal is used for 2 out of 3 activities, as it has extended accessibility to study administration department officers, selected teachers, and external representatives of GAMA. Access to the website to make changes and updates to data is accessible to study administration department clerks, internal IT representatives, and external an IT company.

Since the external IT company manages several internal systems simultaneously, a contractual commitment accepting the importance and benefit of data audit is primary.

Step 4 – determination of compliance with contractual obligations

As seen from the graphical illustration (see Fig. 4), 11 contractual obligations were identified, for which the effectiveness of the contract related to data protection was verified. The contract with GAMA in the "Bakaláři" program, aimed at the catering sector, can be considered optimal. The company that provides document shredding service based on an order system is confidential due to anonymisation, although a contract for receipt and disposal of documents to be shredded based on protocol issued fulfils GDPR requirements in the activity of eliminating data carriers. In the case of a company providing accounting software for a fee, the contract did not contain provisions relating to the processor´s authorization to subcontract without prior notification to the controller. In the case of external accounting and IT companies, contracts did not contain obligations relating to data protection and data security. Similarly, in the case of an external company operating a payment system in which employee personal data are processed, a cooperation agreement is lacking. The contracts with the above organizations were audited or verified in terms of contractual obligations concerning personal data protection and security. In 3 cases, it was confirmed that contractual conditions are set in accordance with GDPR, with minor misconduct.

Regarding the provision of personal data to an external accounting company and interdependence of personal data systems operated by an external IT company, feedback on the absence of the above clauses appears to be alarming, as the analysed institution is exposed to risk consequences which can have undesirable impacts on the whole organization. A proposed partial solution is to take immediate remediation or termination of contractual relationships with partner organizations.

Step 5 – data security specification

Processed data are archived in a printed or electronic form on the premises of the given institution. Printed documents are available in a limited number only, in individual departments, mostly in the Financial Department in lockers. Handling of documents is allowed for selected authorized persons. Data processed electronically are managed by an internal IT employee, while an external IT company provides software support for applications in website management. Servers and backup sources are in the server room, i.e., in a separate lockable room with limited access for data management and maintenance. Access security is ensured using passwords including numbers and characters containing upper and lower-case letters, which do not change, i.e., remain unchanged for unlimited time. At the same time, antivirus protection and automatic data updates are set.

Archiving and disposal of data in a paper form is governed by internal filing and shredding rules. Rules for archiving and disposal of email communication are not fixed. In case of termination of graduate status, students do not have access to the internal system. There is no disposal of personal data posted on the website of the institution. The installation and control of CCTV are performed by an external IT company, management of the analysed institution, and building administration. A total of 33 security cameras are installed on the premises of the institution to monitor all entrances, halls, and passages outside the building. The camera footage is without sound; the retention period is four days, considering public holidays and days off. In case of petty thefts, movement of unauthorized persons on the premises of the institution, their unauthorised entrance into the building, etc., no record is kept that could prove the application of the proportionality balancing test in the operation of CCTV recording.

The analysis of data security showed shortcomings in data archiving and disposal. The system is not updated regularly through changing passwords, there is no balancing test of camera footings, and the contribution of information boards is minor. Personal data protection and data security systems require in-depth data analysis and review.

Step 6 – summary of GAP analysis

Summarizing results of GAP analysis and specification of non-compliance with GDPR in the formulation of rationalization proposals were made with the aim of removing gaps. To ensure compliance with GDPR, it was necessary to make corrections in:

- Inadequate performance of job duties on the side of DPO: to recruit a new DPO from internal staff.
- Incomplete records of data processing activities: to identify incomplete or lacking activities of the school canteen (Activity 1–4), including activities performed by the study administration department related to archiving records of data processing activities.
- Failure to verify processors and contractual clauses: setting up processes for verifying processors before signing the contract and creating a standardized personal data protection addendum to be signed for all processing contracts (4).
- Prevention of unlawful data processing: immediately suspending data processing activities, e.g., in an indication of the name of the health insurance company, ID card number, etc.; informing concerned persons of change in the processing of personal data with additional consent for processing.
- Redundant personal data processing: ceasing performance of redundant activities; informing selected persons of changes in processing and taking corrective measures.
- Requiring consent: do not request evidence of redundant or inaccurate consent; create a form for obtaining the consent of students or their legal representatives concerning personal data processing confirmed by the signature of the persons concerned.
- Non-compliance with information obligations for selected activities (6): ensuring that subjects are informed of the processing of personal data by setting up processes to monitor compliance with information obligations.
- Absence of a retention period for personal data (10 activities): updating filing and shredding rules in accordance with retention policy, completion of missing data.
- Limitation in security incident management: obligation to report security incidents to DPO and develop a security incident management response plan.
- Inadequacies of risk analysis process: setting up processes of regular risk assessment, adding information signs on premises of the analysed institution.
- Absenting proportionality balancing test: application of balance tests on the use of CCTV.
- Absenting Data Protection Impact Assessment **(**DPIA): ensuring DPIA is in line with DPIA guidelines according to WP248.
- Incomplete wording of internal guidelines: completing organisational measures related to Activities 2 - 4. About the insufficient number of lockers, proposing which documents need to be archived. Accepting rules on the exercise of rights of subjects, informing employees of changes in accordance with internal regulation referring to data protection regulation. Ensuring data transparency.
- Lack of staff training on internal regulations: training of staff on protection of personal data and data security, adherence to work procedures and guidelines.
- Incomplete documentation reviewing complaints and consents with personal data processing with the exercise of the subject´s rights, security incidents, and CCTV footage. Handing over records to the Data Protection Officer.
- Impossibility of setting up a system of exercise of subject´s rights: providing subjects with standardized forms to facilitate the exercise of rights and obligations under GDPR.
- Implementation of inspections and control mechanisms: setting up regular inspections on the protection of personal data and data security for processors.

A total of 17 areas were mapped in which shortcomings were identified. Based on the results of the GAP analysis and data audit, recommendations for systemic changes were formulated in the internal processes of the analysed institution. The recommended measures in fulfilling GDPR obligations have a synergistic effect on the systemization of management of value-creating activities since continuous improvement and development of key activity potential is the motto of an economically sustainable and socially responsible business. Based on a comprehensive summary of GAP analysis with the definition of partial corrections, the management of the analysed institution made a managerial decision to develop a new version of the proposal of the project for transformation of process management integrated with GDPR.

Systemization of value-creation activities

The main objective of the paper is to create a proposal for a project to implement GDPR into the management of value-creating activity processes while eliminating gaps identified using GAP analysis. The intention of the project is to remedy the current situation and create a new version of a more valuable output to develop the potential of key activities within internal processes. The management of the analysed institution formulated several criteria that are crucial for the acceptance of innovative project proposals. In terms of duration, the project will be launched on 1 September 2024, which is the latest possible date in view of the beginning of the new school year. The total cost of the project is EUR 2020,20. The staff participating in the implementation of the project will be paid a remuneration of EUR 5,66/hour, with working hours being 4 hours a day for four staff members.

The aim of the project is to remedy inconsistencies with GDPR in internal processes by eliminating gaps so that project activities are continuous, not overlapping, and set up in accordance with GDPR. Table 3 specifies project activities by their scope and duration.

Table 3. Project activities (Source: Created by the author, 2024)

Activities	Specification of project activities	Duration/days	Preceding activities
A	Ensure a new DPO and record-keeping activities	5	-
B	Revision of records on data processing activities	3	A
C	Setting up process of verification of processors´ authorization Creation of standardized addendums to existing contracts	6	A, B
D	Elimination of redundant or unlawful personal data processing, taking relevant measures	2	A, B
E	Revision of consent forms for personal data processing, taking relevant measures	5	A, B
F	Ensuring information obligation concerning personal data processing for selected activities	1	A, B, C, D, E
G	Revision of filing and shredding rules	1	A, B, F
H	Management of security incident reporting, implementation plan	3	A, B, C, D
I	Initiation of risk analysing process	4	A, B, H
J	Revision of information signs about the CCTV system	1	A
K	Application of balancing tests of CCTV system	3	A, B, J
L	Ensuring DPIA in accordance with WP248 guidelines	1	A, B, I, K

M	Creation of forms for the exercise of data subjects´ rights	1	A
N	Revision of internal regulations	2	A, C-L, N
O	Employee training on personal data protection and data security, information of changes and setting up of training plan	2	A, C-L, N
P	Application of control mechanisms	2	H, I, L, N, O

Table 3 shows that the project includes 16 activities (GAP analysis identified 17 areas, with some of them being consolidated, e.g., in ensuring a new DPO, revision of records of personal data processing activities, review of internal guidelines, and setting up control mechanisms including staff training).

The primary project activity is ensuing a new DPO, overseeing management of the complaint process, specification of data subjects´ rights, monitoring consents with personal data processing, and employee training. The status of compliance with GDPR obligations is set along with the specification of tasks of the new DPO, who will undergo GDPR training on confidentiality and signing of an addendum to the contract. The primary task of the new DPO is the termination of the contract with the external company due to non-compliance with contractual obligations and commitments, revision of records on data processing activities, data audit, and questionnaire survey with reference to legislative regulations. The revised records are forwarded to responsible persons in individual departments of the analysed institution aiming at familiarizing them with changes and updates in written documentation. The process of verifying processors and the creation of standardized and additional documents is the responsibility of managers of relevant departments. Elimination of redundant or unsolicited personal data is the responsibility of the data computerization officer and includes e.g. prevention of 2 data leaks in IT systems, 2 text edits in manually processed documents converted into electronic form, 1 edit on an online form, etc. Removing data that has been recorded without legal authorisation is a necessary act of transforming the management of internal processes. Redundantly required consent must be removed from forms no later than at the beginning of the new school year, regardless of the duration of the project. A key activity is setting up processes of processing obtained consents concerning, e.g., publication of photographs according to guidance and information obligations on personal data processing for 6 project activities. The model for data collection and analysis is information notices, e.g., Activity 1, where obligation is fulfilled. The necessary information is obtained from records on processing activities, which will ensure fulfilment of information obligation concerning disclosure of individual communications to data subjects in case of new processes and inspection of filing and shredding rules that will be supplemented by 10 absenting items, e.g., establishing procedure of archiving and disposal of data in email communication and on websites. The management of the security incident reporting process is the responsibility of IT staff. In the set process, incident reporting steps are defined together with the assignment of partial responsibilities.

The reporting of personal data security breaches to data subjects is carried out in line with currently applicable legislation, procedural risk identification and revision of information signs informing about the CCTV system on the premises of the analysed institution. The proportionality balancing test of the CCTV system, which is subject to WP248 guidelines, will facilitate the exercise of subjects´ rights by creating a standardized form. The form shall contain data subjects´ identification, date, and signature with the justification of the request. Based on the review of internal guidelines, it is appropriate to add measures related to Activities 2 – 4 regarding archiving documents stored in lockers. An information memorandum has been drawn up to specify the exercise of data subjects´ rights and an information memorandum has been drawn, in which the above elements are listed and supplemented by information on newly introduced forms. Employee training on personal data protection and data security, information on changes and legislative provisions confirm the importance and benefits of selected activities within the internal process. The creation of a training plan, which includes dates of training

and the process of familiarising staff with changes, new regulations, and measures, will better monitor compliance with GDPR rights and obligations.

The empirical data presented in Table 3 were used to create a node-oriented network diagram (see Fig. 4), which shows the shortest possible duration of the project with a defined critical path.

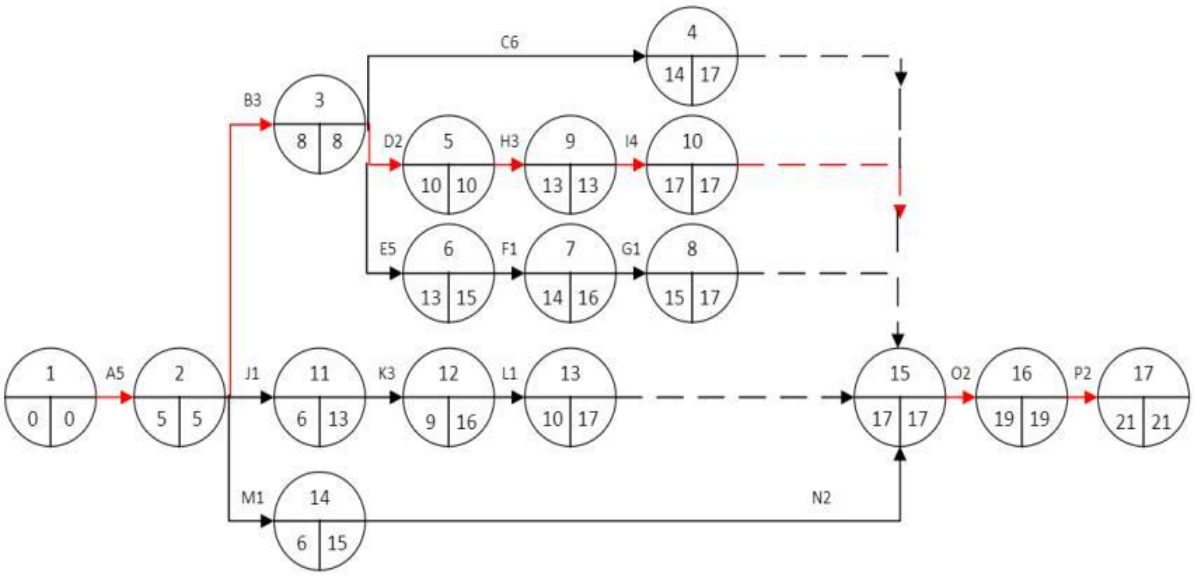
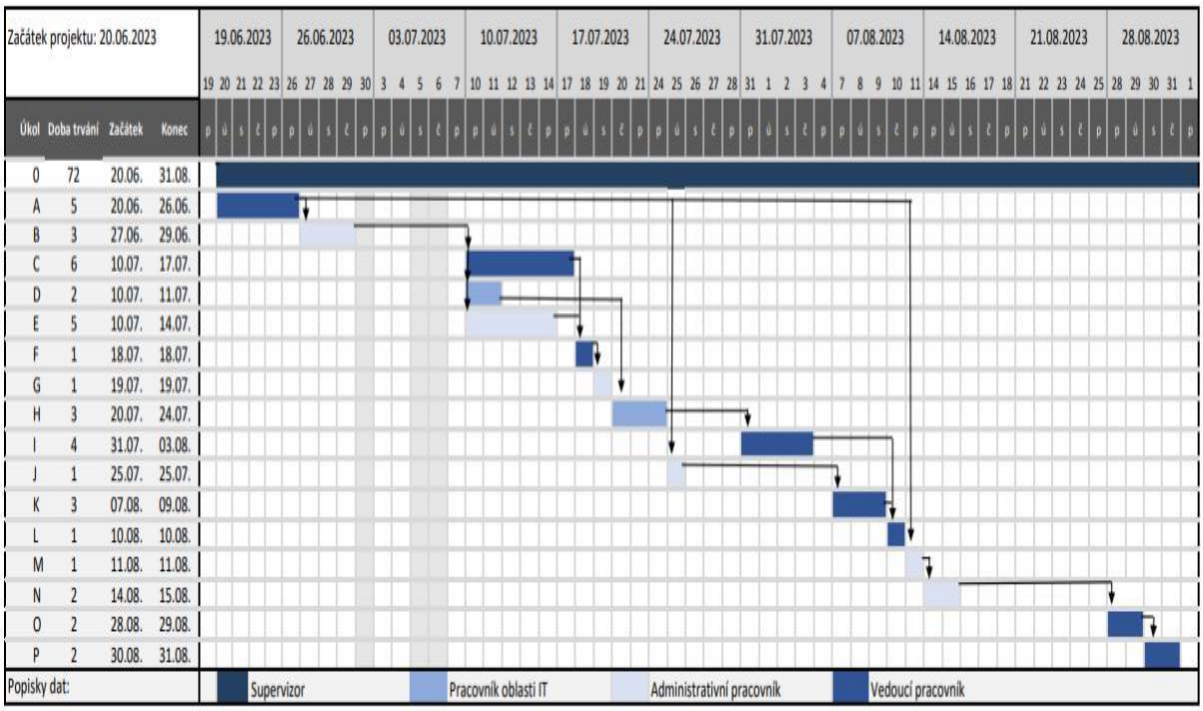


Fig. 4. Network diagram of project activities (Source: Created by the author, 2024)

As seen in the network diagram (see Fig. 4), the shortest possible duration time is 21 days. The critical path is highlighted in red. In these activities, there is no time buffer, which means that any delay in the start or extension of duration of the project has an undesirable impact on its completion. A Gantt chart in Table 4 shows resources and time buffers in the project.

Table 4: Gantt chart of project activities with resources and time buffer (Source: Created by the author, 2024).

Legend: beginning of project, task, project duration, beginning, termination, data specification, supervisor, IT specialist, administrative worker, manager



For purposes of project assessment in relation to the implementation of GDPR in process management of value-creating activities, risk analysis was performed as well as calculation of costs with identification of risk severity, resources, and time buffers aimed at setting up security measures, see Table 5.

Table 5. Risk analysis (Source: Created by the author, 2024)

GDPR	Source of risk	Danger of risk emergence	Risk severity evaluation (PMA)				Security measures
			P	Z	H	Level of risk	
	Delay	Faulty processing of personal data	2	3	3	18	Scheduling
	Erroneous input data	Poor identification with GDPR	3	4	4	48	Specification and checking of project input data, setting up processes and control mechanisms in accordance with GDPR
	Lack of employee training	Leakage of personal data	3	4	4	48	Implementation of training
	Incomplete transformation	Error in understanding GDPR obligations	3	4	4	48	Familiarization with GDPR and relevant documentation
	Insufficient information on changes	Failure to adopt change management by employees	3	3	3	27	Appropriately selected project communication to employees

The Prevention of Major Accidents (PMA) was selected for risk analysis calculation. PMA rates 3 risk components on a scale from 1 to 5. The risk analysis (see Table 5) identified 5 risks (the highest value of risk level reached a score of 48 for 3 risks out of 5). The first identified risk with a value of 48 is failure to detect compliance with GDPR obligations. Setting up internal processes and control mechanisms for continuous monitoring of GDPR compliance is necessary. Personal data leakage resulting from lacking employee training is another risk (48). Insufficient or faulty compliance with GDPR obligation is a cause of process management transformation; therefore, a thorough study of legislation and legislative regulations is primary.

The project was designed with a view to calculate the costs of change management considering the scope and quality of the project. Two permanent employees were selected for implementing project activities, with another employee involved in 2 tasks, and another one was assigned the role of supervisor). The project timeline is set with an implementation period in July and August 2024 due to a lower volume of work activities distributed in a ratio of 50 % of permanent employees´ time and 50 % of working on project activities. By contracting a new DPO, their training, and reimbursement of travel costs, total costs were estimated at 1,93 EUR, i.e. (1 EUR = 24,75 CZK, status as of 05/20/2024), see Table 6.

Table 6. Calculation of change management cost (Source: Created by the author, 2024)

Cost items	Duration/hours	Total costs/EUR
Working on project/Employee 1	96	543,03
Working on project /Employee 2	52	294,14
Working on project /Employee 3	20	105,05
Working on project /supervisor	57	322,42
Training time	16	90,51
Training of a new DPO	-	537,77
Travel costs	-	40,40
Total	-	1933,32

The total cost of the project is calculated at 1933,32 EUR including staff remuneration, travel costs, and training/1 employee. The total remuneration amount is 1355 EUR; the cost of meals is set at 20,20 EUR/day.

The cost calculation does not include a specific cost within the project, namely remuneration for employees in the position of DPO. Compared to the project budget, which was estimated at EUR 2020,20 by the management of the analysed institution, calculated costs are at an optimal level, with a slight reserve. The overall costs did not include remuneration for employees in the position of DPO, as it does not represent additional cost, but a more cost-effective alternative of valuing the performance of staff members compared to a lump sum payment to an external employee.

Based on the results obtained, empirical data, rational findings, and sophisticated solutions proposed, the project can be evaluated as economically feasible and socially responsible. The remuneration at the amount of EUR 60,61 per month paid to DPO should be increased after a probation period of 3 months after obtaining a certificate of competence preliminary approved by the management of the analysed institution. The increase in remuneration will be determined later.

Discussion

Based on qualitative research implemented in the form of a semi-structured interview with a director of the analysed institution and analysis of internal documentation, it was possible to answer the first research question: *"Is compliance with GDPR obligations transparent?"*

The selected institution uses an external company to ensure GDPR obligations. According to the contractual arrangement, the external company should manage the performance of responsibilities of the DPO and provide consultancy, preventive security inspections at least 1 a year, training of managers, and management of documents related to personal data protection. If needed, the external company provides standardized forms, e.g., for consent with personal data processing or addendums to employee contracts. In terms of ensuring GDPR obligations, the analysed institution relies on contractual arrangements with external companies; therefore, no regular audits are performed. Transparency is not ensured.

Through theoretical background, interpretation of results of semi-structured interviews and partial findings including an analysis of internal documents, it was possible to confirm scientific assumption 5: *"If an organization does not carry out regular audits of outsources services, it cannot ensure thorough compliance with GDPR obligations"*.

Using a comparative analysis in conjunction with a scoring method, it was possible to research question 2: *"Is the use of an external Data Protection Officer (DPO) more effective compared to delegating this task to a permanent employee?"*

In response to the research question above is the statement that the use of an external DPO is not more effective. A proposed solution is to entrust this position to a permanent employee of the institution. The findings obtained through semi-structured interviews are used to formulate questions for a questionnaire survey distributed to employees, which provides an answer to the first and second part of research question 3: *"What is the relationship between data system and employee approach to data protection?"*

A total of 83 % of employees participated in a questionnaire survey containing 12 questions. The results confirmed the non-existence of employee training on personal data protection and data security. Moreover, findings confirmed the interest of employees in this type of training in an online form (56 % of respondents and face-to-face training (44 %). The questionnaire was compiled so that it evaluates employees´ knowledge of GDPR issues including explanation of acronyms and matching terminology with definitions of terms. Shortcomings were found in the recording of personal data, e.g., photographs, CCTV footage, or disclosure of email addresses containing the name and surname of contact persons, business phone numbers, etc. Shortcomings were also found in failure to secure personal data (as stated by 76 % of respondents). The respondents were also asked about security measures set and adhered to in the analysed institution. 52 % of respondents answered that they consider switching off PCs/notebooks when leaving the workplace to be a proper duty of every employee. According to the results, 24 % of respondents lock documents with personal data in lockers. Most respondents consider GDPR obligations important; however, according to 12 %, it is redundant. The respondents included representatives of the financial department (16 %), teaching staff (56 %), and other non-teaching staff (28 %). Despite a lack of employee training on personal data protection and data security, employees have a basic awareness of this issue. The results confirm the existence of knowledge gaps in reporting security incidents, which need to be prevented.

The inspection of workplaces concerning the so-called clean desk policy was conducted in the context of internal rules and regulations concerning personal data handling, according to which written documentation containing employee and student personal data should be stored in lockers in lockable offices. As for electronic records, employees must not leave their computers switched on when leaving their offices. Employees commit to the above from the start of their employment by signing a Confidential Information Agreement, according to which they must lock their desks and offices and prevent access to information in PCs and laptops to other persons.

An unannounced inspection took place in the afternoon, on a working day, after working hours. It aimed to find out whether employees adhere to established rules of personal data protection and data security, specifically, whether documentation containing employee and student personal data were freely available in offices, whether computers were switched off and data were stored and secured. A total of 3 offices, 4 teachers´ offices, and 4 classrooms. The inspection found that there were freely accessible documents with names and addresses of natural persons, including a list of students in individual classes and a list of lockers with numbers and attendance in relevant calendar months. Despite this, no evidence was provided to confirm the severity of the potential misuse of personal data. The management of the analysed institution commented on the name list of students available in individual classrooms as a reminder of classroom service. The numbers on personal lockers are a reminder of students´ duties, as stated by the director of the analysed institution. Considering the objectivity of information communicated and the factual reasoning of the management of the institution, it shall be stated that classrooms are also visited by other students from and outside the institution, as they regularly attend school for extracurricular and educational activities. The management of the institution stated that some rooms in the institution do not have enough lockers for storing documents containing personal data. Although inspection found documents containing personal data freely accessible in some rooms, the conclusion is that employees are concerned about data protection and security, although certain shortcomings were identified. The corrective actions taken with the aim of ensuring compliance with

GDPR standards and risk elimination have a positive impact whose scope will be determined in the future.

Based on the results of GAP analysis and data audit, it was possible to fourth research question *"Is it necessary to revise all data listed in the data protection system"* The results highlighted insufficient compliance with GDPR obligations by DPO, incomplete record-keeping on activities concerning data processing, and absence of a process for verifying data protection addendums in processing contracts. The findings confirmed unlawful processing in the case of two persons´ personal data and redundancy in administrative actions concerning requested consents for 3 activities. Non-compliance with information obligations was identified in 6 activities. The absence of a retention period for personal data was confirmed in 10 activities. There are no competent person in charge of the security incident reporting process; no procedures for reporting and handling incidents, including the identification of data subjects were found. The process of risk management is not set up, the proportionality balancing test on the use of the CCTV system is not applied, and the contribution of information signs is minor. Internal regulations do not include organizational arrangements for handling personal data. The rights of data subjects, complaints, security incidents, and conditions for the exercise of data subjects´ rights are not optimally addressed. Employees lack training on the issue of GDPR; therefore, they are not aware of internal regulations and legislative measures on this issue. The scientific assumption 6: *"In case of non-compliance with GDPR obligations, the organization lacks the capacity to independently ensure remediation"* was not confirmed, as the selected institution updated the DPR transformation project proposal in line with the systemization of management of value-creating processes independently in form of corrective measures.

The partial analyses indicate that outsourced services must be operated on a regular basis, as administrators cannot rely on comprehensive performance without verifying facts. If the analysed institution decides to choose an external or internal DPO, it is advisable to independently assess minimalist, realistic, and pessimistic scenarios of sophisticated solutions, as a choice between variables does not guarantee operational and financial efficiency and social benefits. As confirmed by results, the analysed institution can draw a GDPR transformation project proposal implemented in internal processes independently, provided that at least one employee (preferably a permanent employee) possesses knowledge of key issues at least at a basic level.

Conclusions

Benefits and opportunities

The paper has benefits for the analysed institution as well as other public institutions and non-governmental organizations operating in the same or similar sector. Through a data audit, the effectiveness of processes in the organization was verified with a concrete example. With the support of a comparative method, managerial decisions were made on using services of either an external or internal DPO in accordance with GDPR. The selected option was an internal DPO, for which a positive impact on wage and other costs and liability was confirmed.

The need for expertise in GDPR at least at the minimum level has a synergistic effect in identifying gaps in shared processes and sub-activities in planning and performing GDPR obligations that are a priority.

The creation of guidelines and proposals for rationalization measures has added value to research and innovation activities, the contribution of which is verified, tested, and evaluated as an important input capital of development projects of professional organizations listed in monitoring and research reports with an emphasis on Environmental, Social, Governance (ESG) at international and national level of bilateral cooperation.

The theoretical part of the paper can be applied to the design of professional education programs at universities, with a focus on economic, managerial, and socio-legal disciplines, e.g., in study programs like Sustainable business, Process management, Public Administration and records management, where the issue of GDPR transformation into process management has development potential.

According to the author of the paper, the benefit of the paper is in deepening professional knowledge and practical experience with the aim of a detailed understanding of the transformation process. The application of findings obtained and partial analyses with verification of theoretical knowledge, research questions and scientific assumptions connect the theoretical part of the paper with application one to achieve systemization of process-managed organization with acquisition of procedures applicable in practice.

Impacts and limitations

The essential impact is seen in anonymous data protecting the identity of the analysed organisation. Other organizations cooperating with the same external company have not been alerted to non-compliance with GDPR. The design of the project of transformation of GDPR into process management of educational institutions was limited by human resources, time, and resources. Recommendations for changes related to legislation have an impact on the transformation of internal processes, which need to be regularly monitored, systematically managed, evaluated, and strategically developed. The development of digital technologies across all industries that use machine learning and artificial intelligence brings a large volume of data, whose contribution and impact are the subject of discussions and debates on the use of CCTV systems with granting of consent with personal data processing.

The implementation of GDPR in internal processes is a methodological tool to address sub-problems comprehensively and systematically in conjunction with data auditing. Responsibility for processes across organizational structure requires the setting up of a matrix management system, which is hindered by a linear approach that requires transformation.

It is necessary to follow process management guidelines considering data digitalization and resource sharing, the added value of which has a potential for the future.

Potential of systemization of value-creating activities

The transformation of managerial tools in the public sector enables the streamlining of administrative activities by improving services provided and cost-effective use of funds considering the principles of ESG. In synergy with the return of investments in employee training, the project has both economic and social benefits in the development of employee training by deepening know-how.

The improvement of internal processes in the medium and long term and efficient and effective use of funds in the project is significant in a systemic concept, since comparison of employee performance management with the ability to identify gaps or critical points with the aim of ensuring remedy in terms of effectiveness and productivity of work, while considering decentralization of powers and responsibilities is added value of a process-managed organization. The competency responsibilities of current and future management systems in providing digital services are key from a factual and technological point of view, about purpose, goal, and external incentives in integrating management quality and process performance according to Data Quality Analysis, Data Lineage, machine learning, and automated decision-making.

The use of ChatGPT technologies in a real environment with an impact on the effectiveness of work performance management, customer satisfaction with the help of artificial intelligence in the communication of queries related to problems and shared alternatives of individual solutions to problems and causes, automation of tasks and analysis of text data is evidence of development of digital technologies and e-platforms providing online services, whose offer is related to backup of personal data and data storage from legal, ethical, and security point of view. Limitations can be seen in understanding complex tasks and work operations that require the presence of a rational person who is able to objectively assess the current situation and predict future states to make sophisticated decisions on the development of key activities with the aim of increasing the added value of production and operation processes within business, investment, strategic, and work activities. The sustainability of standardized designs and key actions in improvement, refinement, simplification, acceleration, waste reduction, adaptability, flexibility, agility, and other reengineering activities represent the development potential of expected results in corporate sustainability and accountability.

Methods, practices, systems, and tools for continuous improvement of corporate and inter-company processes integrated with strategies and objectives are subject to activities that have a positive impact on eliminating redundant or faulty activities within supporting processes of shared services, optimization of performance, and labour efficiency with a higher added value of transformed processes. Systemization of process management of internal activities has the potential to achieve the value of planned results considering continuous improvement of operational and economic efficiency more easily in saving costs, time, and resources with verification of effectiveness of set processes and sub-activities of a socially responsible organization.

References

Ahmed, J., Yildirim, S., Nowostaki, M., Elezaj, O., & Abomohara, M. (2020). GDPR compliant consent driven data protection in online social networks: A blockchain-based approach. *Proceedings-3rd International Conference on Information and Computer Technologies (ICICT 2020)*, 307-312, 9092226. https://doi.org/10.1109/ICICT50521.2020.00054

Anywar, M., Schreiweis, B., & Ulrich, H. (2022). Strategies and recommendation for data loading of FHIR-based data marts with focus on GDPR compliance. *Studies in Health Technology and Informatics*, *298*, 127-131. https://doi.org/10.3233/SHTI220921

Barati, M., & Rana, O. (2021). Checking GDPR compliance for cloud-based services. *Proceedings of 2021 IEEE World Congress on Services (SERVICES)*, *2*. https://doi.org/10.1109/SERVICES51467.2021.00013

Barati, M., Rana, O., Petri, I., & Theodorakopoulos, G. (2020). GDPR compliance verification in internet of things. *IEEE Access*, *8*, 119697-119709, 9127459. https://doi.org/10.1109/ACCESS.2020.3005509

Bellringer, M. (2022). Worthy of trust: Protecting minority privacy in diversity reporting. *Journal of Data Protection and Privacy*, *5*(2), 173-182.

Beresecka, J., Hronec, S., Hronec, M., Vicianova, J. H., & Svetlikova, V. (2023). Education and socially responsible management as an effective communication tool in local self-government. *Forum Scientiae Oeconomia*, *11*(2), 197-210. https://doi.org/10.23762/FSO_VOL11_NO2_10

Bloemendal, M. T. (2022). On the advent of environmental, social and governance reporting and its intersection with privacy. *Journal of Data Protection and Privacy*, *5*(1), 39-49.

Bohmer, R., Busbach, U., & Kiesel, B. (2023). The Kehler management systems: Integration of external stakeholders in the quality assessments of municipal administrations. *Economics and Culture*, *20*(2), 32-45. https://doi.org/10.2478/jec-2023-0014

Cambronero, M. E., Martinez, M. A., de la Vara, J. L., Cebrian, D., & Valero, V. (2022). GDPR Validator: a tool to enable companies using cloud services to be GDPR compliant. *PeerJ Computer Science*, *8*, e1171. https://doi.org/10.7717/PEERJ-CS.1171

Capodieci, A., & Mainetti, L. (2019). Business process awareness to support GDPR compliance. *ACM International Conference Proceeding Series*, a2. https://doi.org/10.1145/3361570.3361573ACM

Chochia, A., Kerikmae, T., & Skvarciany, V. (2023). Global economic challenges for sustainable entrepreneurs. *TalTech Journal of European Studies*, *13*(1), 3-7. https://doi.org/10.2478/bjes-2023-0001

Dewangan, N. K., & Chandrakar, P. (2023). patient-centric token-based healthcare blockchain implementation using secure internet of medical things. *IEEE Transactions on Computational Social Systems*, *10*(6), 3109-3119. https://doi.org/10.1109/TCSS.2022.3194872

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance. *Lecture Notes in Computer Science*, *11980*, 238-257. https://doi.org/10.1007/978-3-030-42048-2_16

Di Cerbo, F., Lunardelli, A., Matteucci, I., Martinelli, F., & Mori, P. (2019). A declarative data protection approach: From human-readable policies to automatic enforcement. *Lecture Notes in Business Information Processing*, *372*, 78-98. https://doi.org/10.1007/978-3-030-35330-8_5

Di Sabato, V., & Kozakova, J. (2023). Investigation of CSR activities connected to Covid-19 in Czech and Slovak Businesses. *Economics and Culture*, *20*(1), 114-124. https://doi.org/10.24478/jec-2023-0010

Eva, G., Liese, G., Stephanie, B., Sylvie, R., & Greet, S. (2022). Position paper on management of personal data in environment and health research in Europe. *Environment International*, *165*, 107334. https://doi.org/10.1016/j.envint.2022.107334

Fantoni, G., Al Zubaidi, S. Q., Coli, E., & Mazzei, D. (2021). Automating the process of method-time-measurement. *International Journal of Productivity and Performance Management*, *70*(4), 958-982. https://doi.org/10.1108/IJPPM-08-2019-0404

Fieiras-Ceide, C., Vaz-Alvarez, M., & Tunez-Lopez, M. (2023). Designing personalisation of European public service media (PSM): Trends on algorithms and artificial intelligence for content distribution. *Profesional de la Informacion*, *32*(3), e320311. https://doi.org/10.3145/epi.2023.may.11

Garg, R., Varadi, S., & Kertesz, A. (2019). legal considerations of IoT applications in fog and cloud environments. *Proceedings of 27th Euro Micro-International Conference on Parallel, Distributed and Network-Based Processing*, 8671620, 193-198. https://doi.org/10.1109/EMPDP.2019.8671620

Georgiou, D., & Lambrinoudakis, C. (2023). DPIA for cloud-based health organizations in the context of GDPR. *European Conference on Information Warfare and Security*, 187-198.

Georgiou, D., & Lambrinoudakis, C. (2021). Data protection impact assessment (DPIA) for cloud-based health organizations. *Future Internet*, *13*(3), 66. https://doi.org/10.3390/fi13030066

Gobniece, Z., & Titko, J. (2024). Staff competencies for digital transformation: Results of bibliometric analysis. *Virtual Economics*, *7*(1), 25-46. https://doi.org/10.34021/ve.2024.07.01(2)

Gumilar, G., Budiarto, E., Galinium, M., & Lim, C. (2023). Personal Data Protection Framework for Web developers and API providers under UU PDP. *International Conference on Informatics, Multimedia, Cyber and Information Systems*, 189-194. https://doilorg/10.1109/ICIMCIS60089.2023.10349040

Goncalves, E., Teixeira, P., & Silva, J. P. (2020). Development of GDPR-compliant software: Document management system for HR department. *Iberian Conference on Information Systems and Technologies*, 9140922. https://doi.org/10.23919/CISTI49556.2020.9140922

Hariyani, E., Supriono, S., Hanif, R. A., Silalajhi, S. P., & Wiguna, M. (2024). Determinants influencing fraud detection: Role of internal auditors' quality. *Problems and Perspectives in Management*, *22*(2), 51-60. https://doi.org/10.21511/ppm.22(2).2024.05

Harper, S., Mehrnezhad, M., & Mace, J. (2022). User privacy concerns in commercial smart buildings. *Journal of Computer Security*, *30*(3), 465-497. https://doi.org/10.3233/JCS-210035

Hatzivasilis, G., Chatziadam, P., Petroulakis, N., Katehakis, D. G., & Panayiotou, M. (2019). Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and heathcare organizations. *IEEE International Workshop on Computer Aided Modelling and Design of Communication Links and Networks*, 8858165. https://doil.org/10.1109/CAMAD.2019.8858165

Hermanto, I. R., Widyarini, L. A., & Darma, D. C. (2024). Digitalization impact on sustainable firm performance of small, medium, and large businesses. *Virtual Economics*, *7*(1), 7-24. https://doi.org/10.34021/ve.2024.07.01(1)

Ketmaneechairat, H., Maliyaem, M., & Puttawattanakul, P. (2024). Towards a management system framework for the integration of personal data protection and data governance: A case study of Thai laws and practices. *International Journal of Technology*, *15*(1), 219-229. https://doiorg/10.14716/ijtech.v15i1.5885

Kurtz, C., Semmann, M., & Bohmann, T. (2018). Privacy by design to comply with GDPR: A review on third-party data processors. *Americas Conference on Information Systems 2018: Digital Disruption*

Kunnapas, K. (2021). Legal engineering of the anti-abuse rule in ATAD: Architecture of the regression tree model. *TalTech Journal of European Studies*, 11(2), 65-82. https://doi.org/10.2478/bjes-2021-0015.

Lachaud, E. (2020). What GDPR tells about certification. *Computer Law and Security Review*, *38*, 105457. https://doi.org/10.1016/j.clsr.2020.105457

Lapwattanaworakul, J., Srisa-An, C., & Aribarg, T. (2023). Blockchain-based auxiliary systems for pseudonymization and consent management. *TEM Journal*, *12*(4), 2470-2480. https://doi.org/10.18421/TEM124-59

Li, J. (2024). Digital engineering audit management strategy based on machine learning combined with wireless communication network. *Journal of Intelligent and Fuzzy Systems*, *46*(2), 5391-5403. https://doi.org/10.3233/JIFS-230759

Lisiak-Felicka, D., Szmit, M., Szmit, A., & Vaiciuniene, J. (2020). GDPR implementation in local government administration in Poland and the Republic of Lithuania. *Advances in Intelligent Systems and Computing*, 1052, 49-60. https://doi.org/10.1007/978-3-030-30443-0_5

Logachev, M. S., Laamarti, Y. A., Rudneva, S. E., Zemlyakov, D. N., & Barkov, A. (2022). Information system for monitoring and management of the quality of educational programs: Development of functioning algorithms. *International Journal of Instruction*, *15*(3), 429-450. https://doi.org/10.29333/iji.2022.15324a

Lubis, H. Z., Sari, M., Ramadhany, A. A., Ovami, D. C., & Brutu, I. R. (2024). Effect of internal audit, internal control, and audit quality on fraud prevention: Evidence from the public sector in Indonesia. *Problems and Perspectives in Management*, *22*(2), 40-50. https://doi.org/10.21511/ppm.22(2).2024.04

Lyulyov, O., Pimonenko, T., Saura, J. R., & Barbosa, B. (2024). How do e-governance and e-business drive sustainable development goals? *Technological Forecasting and Social Change*, *199*, 123082. https://doi.org/10.1016/j.techfore.2023.123082

Machova, R., Zsigmond, T., Zsigmondova, A, & Seben, Z. (2022). Employee satisfaction and motivation of retail store employees. *Marketing and Management of Innovations*, *1*, 67-83. https://doi.org/10.21272/mmi.2022.1-05

Matulevicius, R., Tom, J., Kalal, K., & Sing, E. (2020). A method for managing GDPR compliance in business processes. *Lecture Notes in Business Information Processing*, *386*, 100-112. https://doi.org/10.1007/978-3-030-58135-0_9

Menges, F., Latzo, T., Vielberth, M., Reiser, H. P., & Pernul, G. (2021). Towards GDPR-compliant data processing in modern SIEM systems. *Computers and Security*, *103*, 102165. https://doi.org/10.1016/j.cose.2020.102165

Merlec, M. M., Lee, Y. K., Hong, S. P., & In, H. P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. *Sensors*, *21*(23), 7994. https://doi.org/10.3390/s21237994

Merzeh, H. R. J., Kara, M., Aydın, M. A., & Balık, H. H. (2022). GDPR compliance iot authentication model for smart home environment. *Intelligent Automation and Soft Computing*, *31(*3), 1953-1970. https://doi.org/10.32604/IASC.2022.021297

Migeon, J. H., & Bobbert, Y. (2022). Leveraging zero trust security strategy to facilitate compliance to data protection regulations. *Intelligence Computing*, *508*, *847*-863. https://doi.org/10.1007/978-3-031-10467-1_52

Molina, M. F., Betarte, G., & Luna, C. (2023). A privacy and security-aware blockchain based design for a digital certificates system. *CLEI Eletronic Journal*, *26*(1), 03. https://doi.org/10.19153/cleiej.26.1.3

Orescanin, D., Hlupic, T., & Vrdoljak, B. (2024). Managing personal identifiable information in data lakes. *IEEE Access*, *12*, 32164-32180. https://doi.org/10.1109/ACCESS.2024.3365042

Pandit, H. J. (2023). Making sense of solid for data governance and GDPR. *Information*, *14*(2), 114. https://doi.org/10.3390/info14020114

Pedrosa, M., Zuquete, A., & Costa, C (2020). RAIAP: Renewable authentication on isolated anonymous profiles: A GDPR compliant self-sovereign architecture for distributed systems. *Peer-to-Peer Networking and Applications*, *13*(5), 1577-1599. https://doi.org/10.1007/s12083-020-00914-5

Peyrone, N., & Wichadakul, D. (2023). A formal model for blockchain-based consent management in data sharing. *Journal of Logical and Algebraic Methods in Programming*, *134*, 100886. https://doi.org/10.1016/j.jlamp.2023.100886

Portillo-Dominguez, A. O., & Ayala-Rivera, V. (2019). Towards an efficient log data protection in software systems through data minimization and anonymization. *Proceedings of 7th International Conference in Software Engineering Research and Innovation*, 9105382, 107-115. https://doi.org/10.1109/CONISOFT.2019.00024

Purificato, E., Wehnert, S., & De Luca, E. W. (2021). Dynamic privacy-preserving recommendations on academic graph data. *Computers*, *10*(9), 107. https://doi/org/10.3390/computers10090107

Qin, F., & Jiang, C. (2023). The construction of university teachers' performance management system under the background of big data technology. *Lecture Notes on Data Engineering and Communications Technology*, *180*, 974-982. https://doi.org/10.1007/978-3-031-36115-9_87

Raycheva, R., Kostadinov, K., Mitova, E., Stefanov, G., & Stefanov, R. (2023). Challenges in mapping European rare disease databases, relevant for ML-based screening technologies in terms of organizational, FAIR and legal principles: scoping review. *Frontiers in Public Health*, *11*, 1214766. https://doi.org/10.3389/fpubh.2023.1214766

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers, 10(11), 150.* https://doi.org/10.3390/computers10110150

Rosmawati, R., Apandi, R. N. N., Widarsono, A., & Sugiharti, H. (2023). Accounting information systems for internal auditor's perception: case study at higher education institution with legal status. *Journal of Engineering Science and Technology*, *18*(2), 1309-1322.

Sadigov, M. M. (2020). State financial management as the basis for innovative development: Cross-country analysis. *Marketing and Management of Innovations*, *4*, 191-201. https://doi.org/10.21272/mmi.2020.4-15

Sanz, R. M. G. (2019). Processing personal political opinion data in electoral activities: All in the public interest. *Revista de Estudios Politicos, 183,* 129-159. https://doi.org/10.18042/cepc/rep.183.05

Shabalina, S., Shabalin, E., Kurbanova, A., Shigapova, A., & Vanickova, R. (2020). Social media marketing as a digital economy tool of the services market for the population of the Republic of Tatarstan. *Advances in Intelligent Systems and Computing*, *908*, 356-367. https://doi.org/10.1007/978-3-030-11367-4_35

Slawicki, P. (2020). Precontractual agreements in selected legal systems. *TalTech Journal of European Studies*, *10*(3), 26-44. https://doi.org/10.1515/bjes-2020-0020

Vanickova, R. & Bilek, S. (2021). Employee privacy protection versus interests and property employer. *International Journal of Law and Management*, 63(6), 537-552. https://doi.org/10.1108/IJLMA-06-2016-0055

Vanickova, R. & Balek, S. (2022). Practical legal aspects of the use of publicly accessible roads in the management of agriculture and forest land. *Tomsk State University Journal*, *477*, 269-276. https://doi.org/10.17223/15617793/477/31

Vazao, A. P., Santos, L., Costa, R. L. D. C., & Rabadao, C.(2023). Implementing and evaluating a GDPR-compliant open-source SIEM solution. *Journal of Information Security and Applications, 75,* 103509. https://doi.org/10.1016/j.jisa.2023.103509

Veinhardt, J., Sroka, W., & Gvozd, M. (2023). Employee procrastination in light of national cultural traits and corporate social responsibility. *Forum Scientiae Oeconomia*, *11*(3), 145-158. https://doi.org/10.23762/FSO_V0L11_N03_8

Yuan, J., Biennier, F., & Benharkat, N. (2021). Data centered and usage-based security service. *Lecture Notes in Computer Science*, 12632, 457-471. https://doi.org/10.1007/978-3-030-76352-7_42

Zieni, B., & Heckel, R. (2021). TEM: A transparency engineering methodology enabling users' trust judgement. *Proceedings of the IEEE International Conference on Requirements Engineering*, 94-105. https://doi.org/10.1109/RE51729.2021.00016