Digitalization and data protection in corporate accounting processes – an exploratory study of employee perceptions

Digitalizáció és adatvédelem a vállalati számviteli folyamatokban – a munkavállalói észlelések feltáró vizsgálata

HAJNAL ZSÓFIA Phd hallgató, Neumann János Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola (GSZDI), email: hajnal.zsofia@nje.hu

SZŰCS ÁRPÁD oktatási dékánhelyettes, Neumann János Egyetem, email: szocs.arpad@nje.hu

TANGL ANITA egyetemi docens, Neumann János Egyetem, Gazdálkodás- és Szervezéstudományok Doktori Iskola (GSZDI), email: tangl.anita@nje.hu

FAZEKAS ESZTER BSc szakos hallgató, Neumann János Egyetem

DOI: https://doi.org/10.65513/MaMi.2026.9.58

Abstract

Digitalization and data protection have become increasingly important in business environments, particularly in financial and accounting processes. This study examines employees' perceptions of digitalization security and workplace data protection. The research combines a literature review with a questionnaire survey conducted among financial and accounting employees at manufacturing companies in Hungary. Of the 123 responses collected, 117 were included in the final analysis. The results indicate statistically significant relationships between perceived digitalization security, the importance of workplace data protection, and the perceived adequacy of company data protection measures. However, no statistically significant relationship was found between data protection training and employees' confidence in using new digital tools. These findings provide insights into employee attitudes towards digitalization and data protection and highlight their relevance to security practice in finance and accounting processes.

Keywords: Digitalization, data protection, accounting information systems, cybersecurity

JEL codes: M15, M41, D83

Absztrakt

A digitalizáció és az adatvédelem egyre fontosabbá válik az üzleti környezetben, különösen a pénzügyi és számviteli folyamatokban. Ez a tanulmány a munkavállalók digitalizációs biztonsággal és a munkahelyi adatvédelemmel kapcsolatos észleléseit vizsgálja. A kutatás egy szakirodalmi áttekintést ötvöz egy kérdőíves felméréssel, amelyet magyar gyártóvállalatok pénzügyi és számviteli alkalmazottai körében végeztek. A 123 begyűjtött válaszból 117-et vettek figyelembe a végső elemzésben. Az eredmények statisztikailag szignifikáns összefüggéseket mutatnak az észlelt digitalizációs biztonság, a munkahelyi adatvédelem fontossága és a vállalati adatvédelmi intézkedések észlelt megfelelősége között. Azonban nem találtak statisztikailag szignifikáns összefüggést az adatvédelmi képzés és a munkavállalók új digitális eszközök használatába vetett bizalma között. Ezek az eredmények betekintést nyújtanak a munkavállalók digitalizációval és adatvédelemmel kapcsolatos attitűdjeibe, és kiemelik azok relevanciáját a pénzügyi és számviteli folyamatok biztonsági gyakorlatában.

Kulcsszavak: Digitalizáció, adatvédelem, számviteli információs rendszerek, kiberbiztonság

JEL kódok: M15, M41, D83

1. Introduction

Digitalization and data protection have become increasingly important issues in modern business environments. The growing use of digital technologies enables companies to improve the efficiency of their operations, automate processes, and manage information more effectively. However, the increasing reliance on digital systems also creates challenges related to cybersecurity and the protection of sensitive information. These challenges are particularly relevant to financial and accounting processes, in which employees regularly handle confidential financial records, business information, and other sensitive organizational data. Data protection is not limited to the privacy of individuals but also concerns the security and confidentiality of corporate information. Unauthorized access to or misuse of such information can result in financial losses, operational disruptions, and reputational damage. Consequently, companies need to implement appropriate technical and organizational measures to protect their information assets and reduce the risks associated with digitalization. In addition to technological safeguards, employees play an important role in maintaining informational security, as their knowledge, attitudes, and everyday practices can influence how securely digital systems and data are handled.

As digital technologies and cyber threats continue to evolve, organizations must consider not only the implementation of security measures but also how employees perceive digital security and data protection. Employees confidence in digital technologies, their attitudes towards workplace data protection, and their assessments of company security measures may all be relevant to organizational information security practices. The aim of this study is to examine employees' perceptions of digitalization security and workplace data protection in financial and accounting work environments. The research focuses on three main questions: whether employee's perceptions of the safety of digitalization are associated with the importance they attach to workplace data protection, whether these perceptions are associated with their assessments of the adequacy of company data protection measures, and whether participation in workplace data protection training is associated with employee's confidence in using new digital tools.

Following review of the relevant literature, an exploratory questionnaire-based survey was conducted to examine employees' perceptions of digitalization and data protection in the context of corporate financial and accounting process. The survey yielded 117 valid responses from employees working in financial and accounting positions.

The questionnaire addressed several aspects of workplace digitalization, including respondents' perceptions of its advantages and disadvantages, their assessments of the security risks associated with digital technologies, their preferences regarding the use of personal computers versus company-provided devices, and their preferences for office-based versus remote work. The survey also explored data protection practices in the workplace, including the provision of data protection training and employees' perceptions of the importance of protecting workplace data.

Based on the research objectives and the topics addressed in the questionnaire, three hypotheses were formulated to examine the relationships between employees' perceptions of digitalization security. The importance they attach to workplace data protection, their assessments of company data protection measures, and their confidence is using new digital tools in relation to data protection training.

The present study aims to answer the following hypothesis:

- H1: Is there an association between employees' perceptions of digitalization security and the importance they attach to workplace data protection?
- H2: Is there an association between employees' perceptions of digitalization security and their assessments of adequacy of company data protection measures?
- H3: Is participation in data protection training associated with employee's confidence in using new digital tools?

The survey results were visualized using figures prepared in Microsoft Excel. The statistical analyses were performed suing IBM SPSS Statistics to examine the hypotheses and assess the relationship between the variables under investigation.

2. Theoretical background

2.1. The integration of digitalization into the daily activities of companies

Nowadays, the term digitalization has become part of the everyday language. Digitalization is the process through which physical, information, documents, or objects are converted into a format that can be processed by computers. However, the concept extends far beyond the mere use of digital devices, it represents a fundamentally new way of thinking and operating. By adopting innovation tools and advances technologies, organizations can achieve unprecedented levels of efficiency, productivity, and performance. The development of digitalization is no limited to Hungary but has spread globally, affecting virtually every part of the world (Dominek et al., 2024). Over the past decades, we have witnessed the rapid integration of information and communication technologies (ICT) into our everyday lives. These technological advancements have transformed the way individuals communicate, work and access information, while also reshaping business operations across all industries (Horváth & Petrovics, 2021). The European Union has also recognized the importance of digitalization and, as a result, has developed numerous regulations, policies, and other strategic documents for its Member States. The EU's objective is to achieve digital sovereignty in a world that is open and highly interconnected. Furthermore, it aims to establish a human-centered and sustainable digital policy that benefits both citizens and business. This approach acknowledges and supports the importance of digital technologies

and their continuous development. One of the most influential documents in this field is the Digital Compass, which outlines four key areas. As a cross-sector illustration, the shift from traditional television towards streaming services has also been examined in the context of digital service transformation (Jenei et al., 2025), although that study does not investigate corporate accounting systems. Comparable service-sector research on eHealth has examined digital technologies alongside changing user expectations and the need for personalized human support (Zsarnoczky-Dulhazi et al., 2023). This provides a cross-sector illustration of user-centred digital transformation rather than direct evidence about accounting-data security.

- The importance of a digitally skilled workforce
- The efficiency, security, and sustainability of digital infrastructures
- The digital transformation of businesses
- The extensive digitalization of public services (Krasznay & Molnár, 2026).

The effective use of digital skills at an appropriate level and to an adequate extent is considered an essential competence in the 21st century. Therefore, it is already necessary to acquire basic digital knowledge in higher education to ensure that employees are adequately prepared to meet the demands of the labour market. However, given the continuous development of technology and the rapid pace on innovation. companies must also place considerable emphasis on developing various employee skills. These include creativity, media literacy, and basic communication skills (Korpics & Herendy, 2025). Organizational adaptation to technological change can also be considered in the broader context of human resource management under conditions of uncertainty. Malatyinszki (2009) examined the effects of the economic crisis on human resources, providing an earlier perspective on the employment-related consequences of disruptive economic changes. Although economic crises and digital transformation differ in their underlying mechanisms, both highlight the importance of organizational adaptation and the management of workforce-related challenges. There are numerous digital areas that can be utilized and further developed by both companies and employees. These include the use of the internet, e-invoicing, social media, cloud-based services, online e-commerce, and other ICT tools (Csiszár, 2022). One of the key outcomes of digitalization for businesses is the increasing importance of digital financial literacy. In this context, it is no longer sufficient to possess only a basic understanding of financial and accounting processes, it is also essential to be familiar with their digital aspects. One of the simplest examples is the use of smartphones and information and communication technology (ICT) devices, which enable faster and easier access to online markets, another example is the ability to monitor bank account balances and review financial transactions through online banking services (Sárközy, 2024). Within the European Union, numerous member states have taken significant steps towards digitalization, as well as towards improving the financial literacy and digital financial literacy (Novotny, 2005). An instructive distinction from another service context separates technical accessibility from the fuller, lived experience of accessible services (Farkas et al., 2023). While the cited study concerns tourism, this distinction offers a conceptual analogy for differentiating access to workplace digital tools from their actual usability for employees.

The OECD's official definition is as follows:

"Financial literacy: a combination of financial awareness, knowledge, skills, attitudes and behaviors necessary to make sound financial decisions and ultimately achieve financial well-being.

Digital financial literacy: a combination of knowledge, skills, attitudes and behaviors necessary for individuals to be aware of and safely use digital financial services and digital technologies with a view to contributing to their financial well-being" (OECD, 2023).

Digital financial literacy plays a crucial role in achieving financial well-being, both throughout the life cycle of companies and at the individual level. Financially literate individuals are able to understand basic financial concepts and use this knowledge to make effective financial decisions. These include, for example, interpreting cash flow, managing loans, and making informed decisions regarding various savings and investment opportunities (Koskelainen et al., 2023). Earlier Hungarian research addressed the impact of the economic crisis on savings (Gácsi et al., 2014). Investment opportunities and investor habits in Hungary were also examined by Zéman and Végh (2010); both studies provide financial decision-making context rather than direct evidence about workplace cybersecurity. The broader financial well-being context also includes structural risks: Kárpáti (2011) analysed demographic, labour-market and administrative pressures on pension systems in Arab countries. That research concerns socio-economic financial vulnerability, not digital accounting or cybersecurity.

2.2. Data protection and data security in SMEs

Digitalization is closely connected to information and enterprise management systems. In modern business environments, digital development and transformation are essential for improving operational efficiency supporting organizational growth. In particular, the implementation and continuous development of accounting information systems can improve the accuracy, transparency and efficiency of accounting processes, thereby supporting more informed decision-making by company owners and managers. However, alongside the benefits of digitalization, companies must also address the risks and challenges associated with the use of digital technologies (Badria & Hasanah, 2024). The implementation of digital technologies and data protection practices also has an organizational and managerial dimension. Malatyinszki (2015) examined the relationship between management and values, emphasizing the relevance of organizational culture and managerial attitudes. From this perspective, the development of responsible data management practices requires not only appropriate technological solutions and formal procedures but also organizational values that support accountability and responsible decision-making. Digitalization has created new opportunities for employees, businesses, consumers, and national economies. The widespread availability of digital information allows consumers to compare products and services across different markets, while companies can improve communication, information management and business operations. Nevertheless, these developments also introduce challenges related to information security, privacy and the regulation of digital activities. An appropriate legal framework is therefore necessary to protect individuals and business in an increasingly digital environment (Gubán & Sándor, 2021). As digitalization has advanced, cybercrime has become a significant concern for organizations of all sizes, including small and medium-sized enterprises (SMEs) and public institutions. Unauthorized access to databases, the theft of sensitive information, and attacks targeting financial systems can causes serious damage to business (Rab et al., 2026). SMEs form the backbone of the economy, providing millions of jobs and serving as the primary source of income for countless families. However, many SMEs lack adequate resources and cybersecurity capabilities to defend themselves against cyber threats, while cybercriminals continuously develop new and more sophisticated attack methods. Cyberattacks can consequently result in financial losses, operational disruptions, and reputational damage, potentially weakening a company's competitiveness and financial stability (Gulyas, 2025). Technological adaptation has also been examined in Hungarian cereal production (Baranyai et al., 2009); this production-sector example is

included as background to organizational technological change, not as evidence of accounting-data security outcomes.

In response to the growing need for cybersecurity, numerous legal regulations have been introduced, including the General Data Protection (GDPR), the European Union's comprehensive legal framework for the protection of personal data. The GDPR governs the processing of personal data relating to natural persons and establishes the principle of freely given consent for data processing. Under the Regulation, data subjects have the right to determine how their personal data are used. If an organization processes personal data based on consent, it must be able to demonstrate that such consent has been validly obtained. Furthermore, the GDPR must be implemented in a manner that is fully consistent with the legal system of each Member State (Makk, 2021). The GDPR defines personal data as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified directly or indirectly, by reference to one or more identifiers, such as a name, an identification number, location data, an online identifier, or one or more factors specific to that person physical, physiological, genetic, mental, economic, culture, or social identity, if personal data are processed in such a way that the data are considered anonymized, and the processing falls outside the scope of the GDPR. Consequently, organizations that effectively anonymize personal data in accordance with the Regulation comply with the relevant GDPR requirements (Erdélyi & Leiter, 2024). The General Data Protection Regulation (GDPR) applies not only to the protection of employee's personal data but also to the personal data of customers and clients. The following categories illustrate the different types of data that organizations may need to manage and protect:

1. Business-related information: company name, registered office address, business address, and other corporate details.
2. User identification data: customers name, age, gender, nationality, contact information, and email addresses.
3. Transaction-related data: unique transaction identifiers generated during interactions between business and their customers.
4. Internal business performance data: information on sales volumes, purchase prices, selling prices, revenue, and other business performance indicators.
5. User behavioral data: clickstream data, domain names, website visited, browsing history and other information related to users' online behaviors.
6. Market analysis data: information used to analyze market trends, identify changes in customer demand, recognize emerging consumer needs, and support the development of new business strategies.

The protection requirements applicable to these categories depend on the nature of the information and circumstances in which it is processed. For example, transaction records and business performance data may contain personal data when they can be linked to identifiable individuals. Appropriate data management practices are therefore important for both regulatory compliance and the protection of confidential corporate information (Fanni, 2025). Data security and cybersecurity are also important in preventing financial and other forms of corporate crime. Businesses may face traditional financial crimes, including bribery, insider trading, embezzlement, tax evasion, money laundering, and counterfeiting (Kiss & Kovács, 2025). In addition, cyber-enable crimes such as identity theft, credit card fraud, banking fraud, online fraud, and phishing can threaten both corporate information systems and financial assets. If a company becomes the victim of any type of criminal activity, the incident should be reported immediately to the competent authority. In Hungary, cybersecurity incidents should be reported to the National Cyber Security Center (NCSC Hungary). Furthermore, if the incident involves

a bank account, payment services, or securities the affected financial institution should also be notified without delay (Kovács & Terták, 2024). The following table summarizes the main effects of digitalization and data protection on companies financial and accounting processes, based on the relevant literature:

1. Table: *The effects of digitalization and data protection on companies financial and accounting processes*

Area	Impact of digitalization	Impact of data Protection	Effect on accounting processes
Data entry	Electronic invoices, automated data entry	Regulation of access to data	Faster and more accurate data entry with fewer manual errors
Invoicing	E-invoicing and automated invoice processing	Protection of personal and business data contained in invoices	More efficient, faster, and more secure invoicing
Bookkeeping	Accounting software and automated accounting processes	Access control and authorization management	Faster accounting processes and greater control
Document management	Digital document storage and cloud-based systems	Secure storage, data backup	Reduced use of paper-based documents and easier data retrieval
Data processing	Rapid processing and analysis of large volumes of data	Data management regulations and data minimization	More efficient decision-making and reduced data security risks
Access to information	Remote access and online accounting systems	User permissions and authentication	More flexible working arrangements while maintaining control over data access
Data security	Implementation of digital security solutions	Cybersecurity, encryption, and regular backups	Enhanced protection of sensitive financial and personal data
Auditing and control	Digital records and automated control mechanisms	Ensuring data traceability and integrity	More transparent and efficient auditing and control processes
Employees	Introduction of new digital tools and automated tasks	Data protection awareness and appropriate data handling practices	More efficient work, accompanied by a greater need for employee training
Corporate decision-making	Real-time financial information and data analytics	Ensuring reliable and appropriately managed data	Faster and more informed managerial decision-making

Source: (Zhong et al., 2022)

Overall, digitalization can improve the efficiency, speed, transparency, and automation of accounting processes, while data protection and cybersecurity measures help safeguard the information processes through these systems. However, the effectiveness of organizational protection also depends on how employees perceive digital security and the adequacy of the measures implemented by their employers.

Understanding these perceptions is particularly relevant in financial and accounting environments, where the secure handling of sensitive information is an essential part of daily operations.

3. Research Method

To establish the theoretical foundation for this study, a literature revies was conducted using Web od Science and Google Scholar as the primary sources for identifying relevant academic publications the review covered scientific literature published in both Hungarian and English, with a particular focus on studies published between 2020 and 2026. The selected publications addressed key topics related to the study, including cybersecurity in the corporate environment, the role of digitalization in organizational development and business operations, and data protection in the workplace. Particular attention was paid to literature relevant to digital security perceptions, employee attitudes toward data protection, and the role of data protection training.

Following the literature review, a quantitative, questionnaire-based study was conducted to examine employees' perceptions of digitalization and data protection in the context of corporate financial and accounting processes. Data were collected between November 2025 and March 2026. The questionnaire was distributed via email to various manufacturing companies and shared in Facebook groups to reach employees working in financial and accounting positions.

A total of 123 responses were received. Six respondents were excluded from the statistical analysis because they reported not using any digital devices in their work. As study focused on perceptions of digitalization security and workplace data protection in a work context involving digital technologies, these respondents did not meet the inclusion criteria. Consequently, the final analytical sample consisted of 117 respondents.

The questionnaire examined employees' perceptions of the security of digitalization, the importance they attach to workplace data protection, their assessments of the adequacy of company data protection measures, and their confidence in using new digital tools in relation to data protection training. The collected data were analyzed using IBM SPSS Statistics, while Microsoft Excel was used to prepare figures illustrating the results. Statistical procedures were selected according to the research hypotheses and the types of variables examined.

The present study aims to answer the following hypothesis:

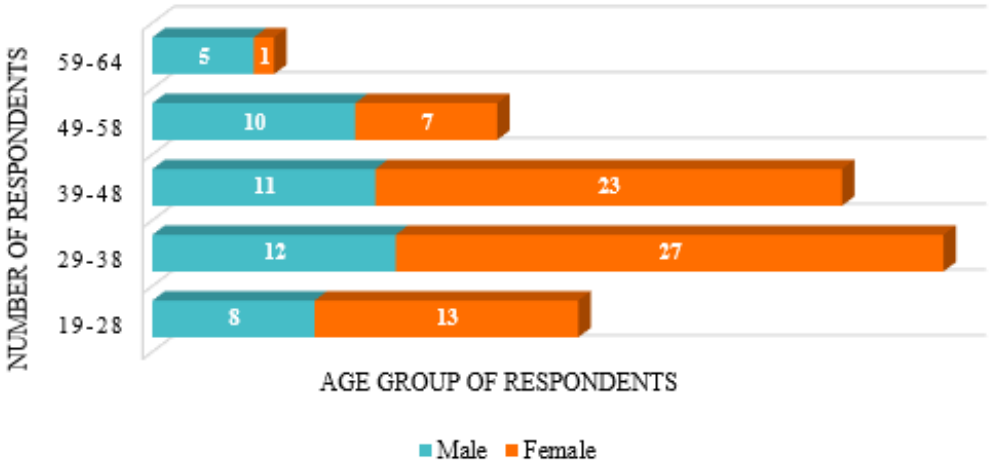
- H1: Is there an association between employees' perceptions of digitalization security and the importance they attach to workplace data protection?
- H2: Is there an association between employees' perceptions of digitalization security and their assessments of adequacy of company data protection measures?
- H3: Is participation in data protection training associated with employee's confidence in using new digital tools?

For the first and second hypotheses, Pearson's chi-square test of independence was used to examine the relationships between categorical variables. This method was selected because both hypotheses focused on associations between employees' perceptions of digitalization security and their responses concerning workplace data protection and company security measures. Fisher's exact test was also considered due to the presence of low expected cell frequencies in the contingency tables. Cramér's V was used to assess the strength of the identified associations.

For the third hypothesis, simple linear regression analysis was conducted to examine the relationship between workplace data protection training and employee's confidence in using new digital tools. Participation in training was measured as a binary variable (yes/no), while employees' confidence was assessed on a five-point scale. Linear regression was selected to examine whether the provision of workplace training was associated with differences in employees reported confidence levels. The statistical significance of the model was assessed using the F-test and the regression coefficient, while the coefficient of determination R^2 was used to evaluate the model's explanatory power.

4. Results

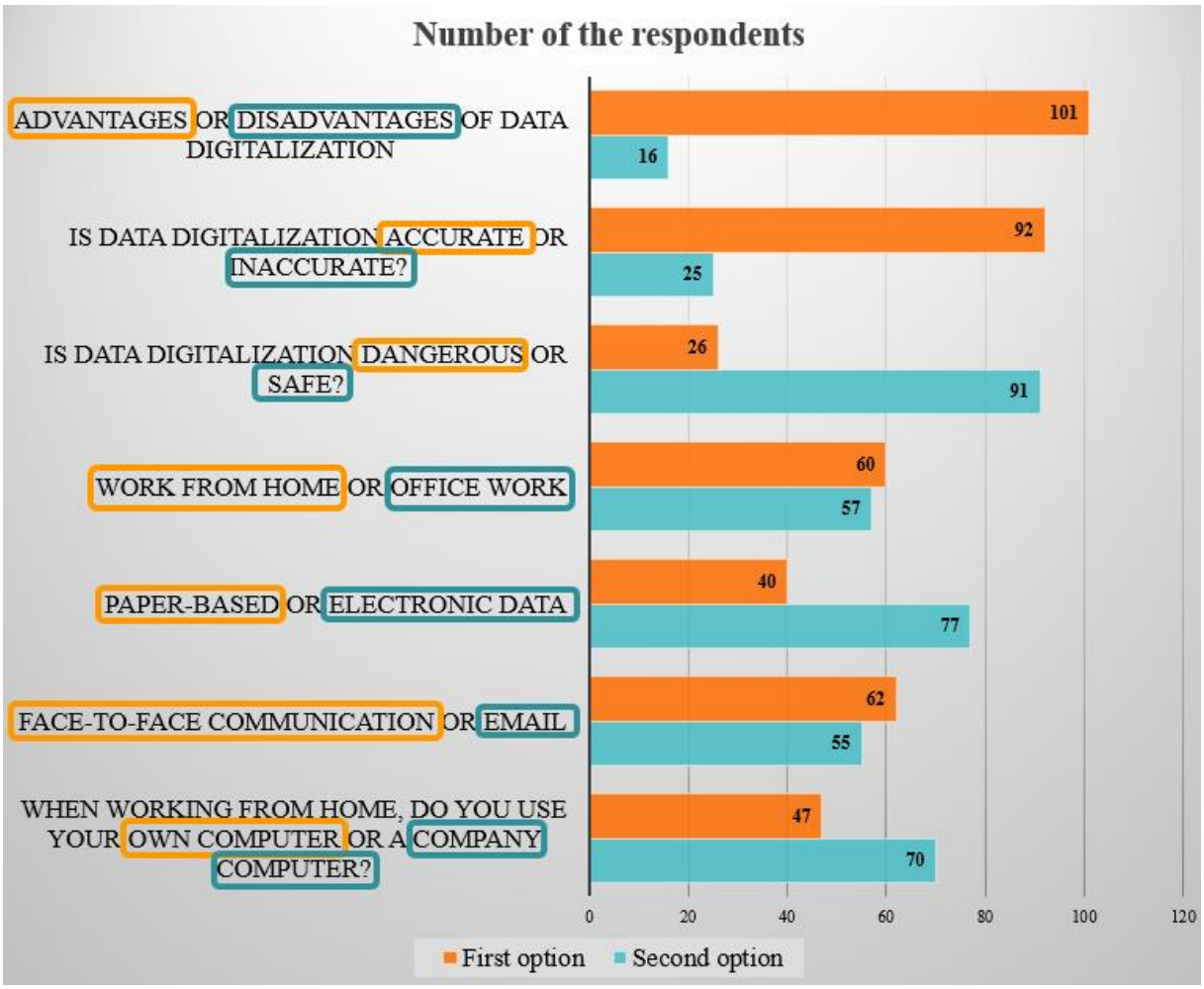
To substantiate the first hypothesis, several key questions were examined, with particular emphasis on the respondents age and gender distribution, as well as their attitudes towards digitalization and data protection within a company. The distribution of respondents by age group and gender is illustrated in the following figure.



1. Figure: Gender and age distribution of respondents (count: 117):

Source: Author's own work based on the questinnaire survey

Overall, 46 male and 71 female respondents participated in the survey. The majority of participants were between the ages of 19 and 48, with more than 94 respondents, belonging to this age range. No respondents over the age of 65 participated in the survey. Following this, respondents were asked several questions aimed at examining the role of digitalization in their workplace. For each question, participants could choose between two possible answer options. The results are illustrated in the following figure.

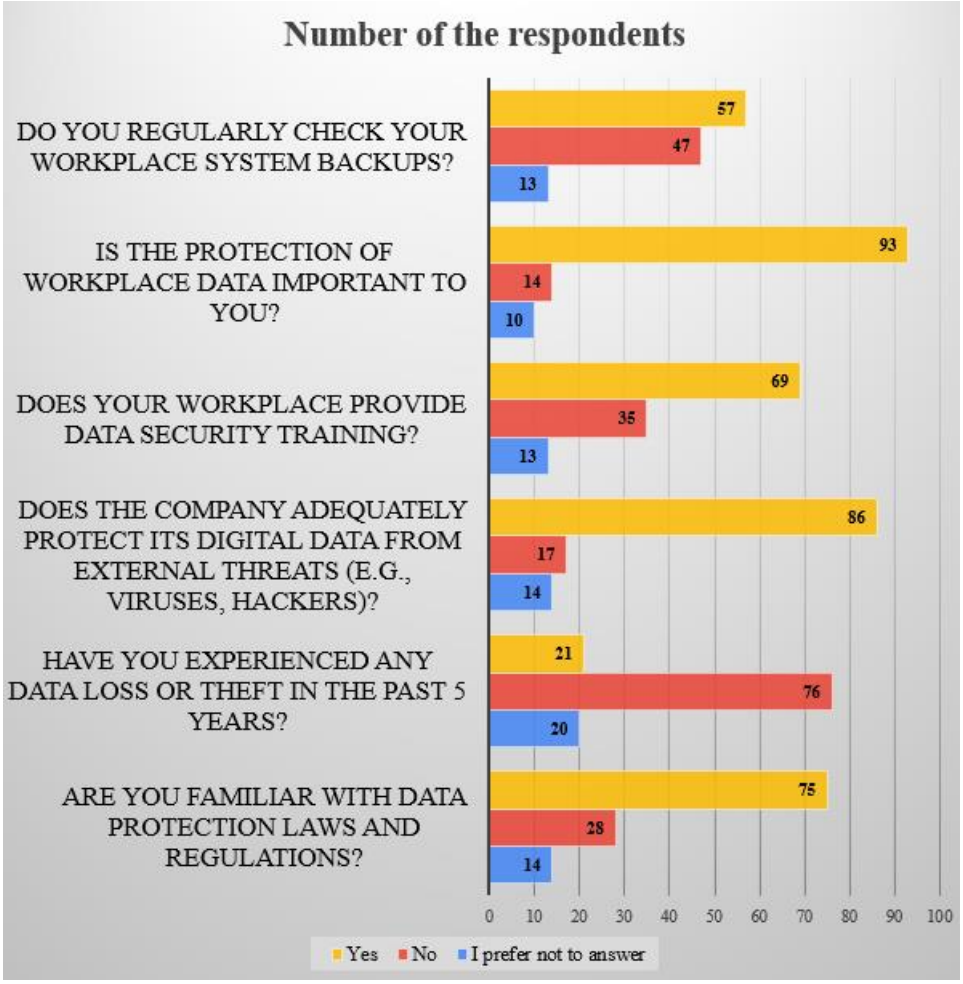


2. Figure: Opinions of the respondents (count: 117):

Source: Author's own work based on the questinnaire survey

The first question examined whether respondents perceive digitalization as an advantage or rather as a disadvantage in their work. A total of 101 respondents considered digitalization to be beneficial, while only 16 respondents viewed it as rather disadvantageous. The following question investigated whether respondents believe that digitalization makes data more accurate or inaccurate. The majority of participants, 92 respondents, considered data to be more accurate due to digitalization, while 25 respondents perceived it as less accurate. The next question focused on whether respondents consider digitalization to be dangerous or rather safe. In this case, 91 respondents indicated that they perceive digitalization as safer than dangerous. Regarding the preference between office-based and home-based work, respondents expressed relatively divided options. A total of 60 participants preferred working from home, while 57 respondents preferred working in an office environment. Concerning paper-based and electronic data processing and storage, 40 respondents preferred paper-based documents, whereas 77 participants preferred electronic documents. A similarly divided result was observed regarding the preference between personal and email-based communication. A total of 62 respondents preferred face to face communication, while 55 participants preferred communication via email. The final question in this group examined the preference between using a personal computer and a company provided computer. A total of 70 respondents preferred using a company computer, whereas 47 participants preferred using their own devise.

The following group of questions focused on data security and data protection. In this section, respondents could choose from three possible answer: „Yes", „No", and „I prefer not to answer". The results are illustrated in the following figure.



3. Figure: Opinions of the respondents (count: 117):

Source: Author's own work based on the questinnaire survey

The first question concerned whether respondents regularly check workplace backups. A total of 57 participants stated that they regularly perform such checks, while 47 respondents indicated that they do not usually check them. Additionally, 13 participants did not wish to this question. The following question examined whether respondents consider the protection of workplace data to be important. In This case, the majority of respondents, 93 participants, answered "Yes", while only 14 respondents answered "no", and 10 participants did not wish to provide an answer. The following question examined whether workplaces provided training related to data security and data protection. A total of 69 respondents answered "yes", 35 participants answered "no", and 13 respondents chose not to answer the question. The following question examined whether respondents believe that their company adequately protects its digital data from external threats, such as unwanted viruses and hackers. A total of 86 participants considered their company's protection measures to be adequate, while 17 respondents answered „no" and 14 participants chose not to provide an answer. The following question examined whether respondents had experienced any data loss or data theft within the past five years. The majority of participants answered „no" to this question, with 76 respondents indicating that they had to

experienced such incidents. However, 21 participants answered „yes", while 20 respondents chose not to provide an answer, representing the highest number of non-responses recorded in the survey. The final question investigated, whether respondents were familiar with general data protection laws and regulations. A relatively high proportion of participants, 75 respondents, answered „yes", while 28 respondents answered „no", and 14 participants chose not to provide an answer. These questions provided the foundation for the subsequent stages of my research.

The first and second hypotheses were examined using Pearson's chi-square test of independence in IBM SPSS Statistics. The third hypothesis was initially investigated using regression analysis. Responses classified as "I prefer not to answer" were excluded from the relevant analyses.

The first hypothesis examined whether there was an association between employees' perceptions of digitalization as safe or dangerous and the importance they attached to workplace data protection. Both variables were measured using binary response options yes/no.

For the first hypothesis, the null and alternative hypothesis were defined as follows:

H^0: There is no statistically significant association between employees' perceptions of digitalization as safe or dangerous and the importance they attach to workplace data protection.

H^1: There is a statistically significant association between employees' perceptions of digitalization as safe or dangerous and the importance they attach to workplace data protection.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	11,080[a]	1	<,001		
Continuity Correction[b]	8,919	1	,003		
Likelihood Ratio	9,209	1	,002		
Fisher's Exact Test				,003	,003
N of Valid Cases	103				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 3,14.

b. Computed only for a 2x2 table

Symmetric Measures[c]

		Value	Approximate Significance
Nominal by Nominal	Phi	,328	<,001
	Cramer's V	,328	<,001
	Contingency Coefficient	,312	<,001
N of Valid Cases		103	

c. Correlation statistics are available for numeric data only.

4. Figure: Relationship between the variables

Source: Author's own work based on the questinnaire survey

Pearson's chi-square test of independence revealed a statistically significant association between the two variables $X^2(1) = 11.080$, $p < 0.001$. Fisher's exact test also indicated a statistically significant association $p = 0.003$. The strength of the association was assessed using Cramér's V, which was 0.328, suggesting a moderate association between the variables.

Based on these results, the null hypothesis was rejected in favor of the alternative hypothesis. The findings indicate that employees' perceptions of the safety of digitalization were statistically associated with the importance they attached to workplace data protection in the sample examined. However, the results do not establish a casual relationship between the two variables.

The second hypothesis examined whether there was an association between employees' perceptions of the safety of digitalization and their assessments of the adequacy of company data protection measures.

For the second hypothesis, the null and alternative hypothesis were defined as follows:

> H^0: There is no statistically significant association between employees' perceptions of the safety of digitalization and their assessments of adequacy of company data protection measures.
>
> H^1: There is a statistically significant association between employees' perceptions of the safety of digitalization and their assessments of adequacy of company data protection measures.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	18,854[a]	1	<,001		
Continuity Correction[b]	15,900	1	<,001		
Likelihood Ratio	15,229	1	<,001		
Fisher's Exact Test				<,001	<,001
N of Valid Cases	107				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 2,88.

b. Computed only for a 2x2 table

Symmetric Measures[c]

		Value	Approximate Significance
Nominal by Nominal	Phi	,420	<,001
	Cramer's V	,420	<,001
	Contingency Coefficient	,387	<,001
N of Valid Cases		107	

c. Correlation statistics are available for numeric data only.

5. Figure: Relationship between the variables

Source: Author's own work based on the questinnaire survey

Pearson's chi-square test of independence revealed a statistically significant association between the two variables $X^2(1) = 18.854$, $p < 0.001$. Fisher's exact test also indicated a statistically significant association $p = 0.001$. The strength of the association was assessed using Cramér's V, which was 0.420, suggesting a moderate to relatively strong association between the variables.

Based on these results, the null hypothesis was rejected in favor of the alternative hypothesis. The findings indicate that employees' perceptions of the safety of digitalization were statistically associated with the assessments of the adequacy of company data protection measures in the sample examined. However, the results do not establish a causal relationship between the two variables.

The third hypothesis examined whether participation in workplace data protection training was associated with employee's confidence in using new digital technologies. To investigate this relationship, a regression analysis was conducted using IBM SPSS Statistics.

For the third hypothesis, the null and alternative hypothesis were defined as follows:

> H^0: There is no statistically significant relationship between participation in workplace data protection training and employee's confidence in using new digital tools.
>
> H^1: There is a statistically significant relationship between participation in workplace data protection training and employee's confidence in using new digital tools.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,078[a]	,006	-,004	,903	,006	,622	1	102	,432

a. Predictors: (Constant), Does your workplace provide data security training?

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	,507	1	,507	,622	,432[b]
	Residual	83,252	102	,816		
	Total	83,760	103			

a. Dependent Variable: How confident do you feel using new technologies?

b. Predictors: (Constant), Does your workplace provide data security training?

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Correlations		
		B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
1	(Constant)	3,652	,109		33,580	<,001	3,436	3,868			
	Does your workplace provide data security training?	,148	,187	,078	,788	,432	-,224	,520	,078	,078	,078

a. Dependent Variable: How confident do you feel using new technologies?

6. Figure: Relationship between the variables

Source: Author's own work based on the questinnaire survey

The analysis yielded a correlation coefficient of $r = 0.078$, indicating a very weak positive relationship between the variables. The coefficient of determination was $R^2 = 0.006$, meaning that the regression model explained approximately 0.6% of the variance in employee's confidence in using new digital technologies. This indicates that the model had very limited explanatory power.

The ANOVA test indicated that the regression model was not statistically significant, F = 0.622, p = 0.432. Similarly, the regression coefficient for the predictor variable was not statistically significant ß = 0.148, p = 0.432.

Since the p-value exceeded the 0.05 significance level, the null hypothesis could not be rejected. Therefore, the analysis did not provide sufficient statistical evidence of an association between participation in workplace data protection training and employees confidence in using new digital technologies in the sample examined. This finding should not be interpreted as proof that data protection training has no effect, rather, no statistically significant association was detected in the present study.

6. Conclusion

The results of this study indicate a statistically significant association between employees' perceptions of digitalization as safe or dangerous and the importance they attach to workplace data protection. This finding suggests that employees' perceptions of digital security are related to their attitudes towards protecting workplace data. In the context of financial and accounting processes, where employees handle sensitive financial and organizational information, these attitudes are particularly relevant to the development and maintenance of appropriate data protection practices.

The second hypothesis was also supported by the statistical analysis. A statistically significant association was identified between respondents' perceptions of the safety of digitalization and their assessments of adequacy of company data protection measures. This result highlights the importance of considering employees' perceptions when evaluating workplace information security practices. However, these findings reflect employees' assessments rather than the objective effectiveness of companies' security measures.

In contrast, the analysis of the third hypothesis did not identify a statistically significant association between participation in workplace data protection training and employee's confidence in using new digital technologies. The regression model was not statistically significant, F (1,102) = 0.622, p = 0.432, and explained approximately 0.6% of the variance in employee's confidence $R^2 = 0.006$. Therefore, the results do not provide sufficient statistical evidence to conclude that participation in data protection training is associated with employee's confidence in using new digital tools in the sample examined. Nevertheless, this finding should not be interpreted as evidence that such training is ineffective. Further research is needed to investigate the potential relationship, taking into account factors such as the content, frequency, and practical relevance of training, as well as employees previous experience with digital technologies.

The following table presents the results of the hypothesis tests:

2. Table: *The results of the hypothesis tests:*

Research questions:	Research Methods:	Analysis results:
H1: Is there an association between employees' perceptions of digitalization security and the importance they attach to workplace data protection?	Chi-square test	□
H2: Is there an association between employees' perceptions of digitalization security and their assessments of adequacy of company data protection measures?	Chi-square test	□
H3: Is participation in data protection training associated with employee's confidence in using new digital tools?	Regression analysis	X

Source: Compiled by the authors based on the research findings

Overall, the findings provide exploratory insights into employees' attitudes towards digitalization security and data protection in financial and accounting work environments. The results highlight the relevance of employee perceptions for organizational data protection practices and suggest that companies should consider both technological safeguards and employees' awareness when developing information security policies and training programs. In particular, financial and accounting departments may benefit from particular training tailored to the digital tools, data management tasks, and security risks encountered in their daily work.

The findings are broadly consistent with the literature emphasizing the importance of digital security awareness and workplace data protection. However, the relationship between data protection training and employee's confidence in using new digital technologies requires further investigation. Since the study was based on a questionnaire survey of 117 valid respondents, the findings should be interpreted in light of sample and the exploratory nature of the research. Future studies could use larger and more diverse samples and examine how training content, frequency, and practical application relate to employees' confidence and data protection practices. Future research should also consider participants' socio-economic heterogeneity when selecting survey samples and interpreting responses. In a different empirical context, Berde and Remsei (2025) found employment income and reluctance to have additional children to be important explanatory factors for Ukrainian refugee women's intention to return. Their study does not investigate digital accounting or cybersecurity; it illustrates the potential relevance of background characteristics in survey-based analysis.

References

Badria, N., & Hasanah, N. (2024). The Role of Digital Accounting for SMEs in Facing Business Challenges in the Digital Era. *Accounting and Finance Studies*, *4*(4). https://doi.org/10.47153/afs44.11192024

Baranyai, Zs., Kodenko, J., Belovecz, M., Végh, K., & Széles, I. (2009). Technological challenges of Hungarian cereal production – analysis of situation and alternatives. Cereal Research Communications, 37(Suppl. 4), 457–460.

Berde, É., & Remsei, S. (2025). Turning the triple burden of Ukrainian depopulation into a quadruple burden: The results of a survey among Ukrainian refugee women. Economics and Sociology, 18(1), 296–312. https://doi.org/10.14254/2071-789X.2025/18-1/16

Csiszár Csilla Margit. (2022). A digitális transzformáció helyzete Magyarországon és az Európai Unióban. *Fenntarthatóság XII. Nemzetközi Tudományos Konferencia*, 417–427. https://www.academia.edu/94846213/A_digit%C3%A1lis_transzform%C3%A1ci%C3%B3_helyzete_Magyarorsz%C3%A1gon_%C3%A9s_az_Eur%C3%B3pai_Uni%C3%B3ban

Dominek, D. L., Ceglédi, S., & Barnucz, N. (2024). The Study of Instructors' Digital Competence in Higher Education—Comparative Analysis. *Információs Társadalom*, *24*(3), 84. https://doi.org/10.22503/inftars.XXIV.2024.3.5

Erdélyi, D., & Leiter, M. P. (2024). Kérdezz bármit, tudom a választ! – avagy a ChatGPT adatvédelmi kérdései, különös tekintettel a személyes adatok védelmére és a kockázati besorolásra. *Rendvédelem*, *13*(1), 64–75. https://doi.org/10.53793/RV.2024.1.4

Fanni, T. (2025). A SZEMÉLYES ADATOK ÉS AZ ADATVÉDELEM SZEREPE A PIACI VERSENYT ÉRINTŐ EURÓPAI UNIÓS PLATFORMJOGSZABÁLYOKBAN. *Debreceni Jogi Műhely*, *22*(1–2), 205–227. https://doi.org/10.24169/DJM/2025/1-2/9

Farkas, J., Raffay, Z., Kárpáti, J., Fekete-Frojimovics, Z., & Dávid, L. D. (2023). The dialectics of (deep) accessible tourism and reality—Hermeneutics of a journey to Madrid. Sustainability, 15(4), 3257. https://doi.org/10.3390/su15043257

Gácsi, R., Végh, K., Zéman, Z., & Bárczi, J. (2014). Savings affected in Hungary by the economic crisis. In Z. Zéman (Ed.), Controller Info Studies I (pp. 79–85). Copy & Consulting Kft.

Gubán, Á., & Sándor, Á. (2021). A KKV-k digitálisérettség-mérésének lehetőségei. *Vezetéstudomány / Budapest Management Review*, *52*(3), 13–28. https://doi.org/10.14267/VEZTUD.2021.03.02

Gulyas, K. (2025). KKV-k vállalatmenedzsmentjének „újkeletű" kihívásai és lehetőségei: a kiberbűnözéstől az online vállalkozástámogatásig. *TAYLOR Gazdálkodás- És Szervezéstudományi Folyóirat*, *16*(1), 41–52. https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/45881/44835

Horváth, I., & Petrovics, Z. (2021). Digitalizáció a munkában. *Pro Futuro*, *11*(2). https://doi.org/10.26521/profuturo/2021/2/10239

Jenei, S., Nagy, R., Moreno-García, E., Dávid, L. D., Pallás, E. I., & Végh, K. (2025). The rise of streaming services: A challenge to traditional television? Journal of Cultural Analysis and Social Change, 10(4), 2547–2559. https://doi.org/10.64753/jcasc.v10i4.3291

Kárpáti, J. (2011). The pension systems of Arab countries in the light of socio-economic risks. Public Finance Quarterly, 56(2), 179–192.

Kiss, M., & Kovács, L. (2025). A pénzügyi kiberbűnözés rendszertana. *Gazdaság És Pénzügy*, *12*(3), 385–402. https://doi.org/10.33926/GP.2025.3.4

Korpics, M. K., & Herendy, C. (2025). Could digital competence be one of the most important key competencies of the future? *Információs Társadalom*, *25*(4), 71. https://doi.org/10.22503/inftars.XXV.2025.4.4

Koskelainen, T., Kalmi, P., Scornavacca, E., & Vartiainen, T. (2023). Financial literacy in the digital age—A research agenda. *Journal of Consumer Affairs*, *57*(1), 507–528. https://doi.org/10.1111/joca.12510

Kovács, L., & Terták, E. (2024). A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. *Gazdaság És Pénzügy*, *11*(1), 6–29. https://doi.org/10.33926/GP.2024.1.2

Krasznay, C., & Molnár, D. (2026). Az Európai Unió digitális stratégiai autonómiája: célok és perspektívák. In *Az európai stratégiai autonómia és Magyarország haderőreformja* (pp. 71–89). Ludovika Egyetemi Kiadó. https://doi.org/10.36250/01218_04

Malatyinszki, S. (2009). A válság hatása az emberi erőforrásokra. *Körös Tanulmányok, 12*, 65–72. https://real.mtak.hu/191991/

Malatyinszki, S. (2015). A menedzsment és az értékek. *Tudásmenedzsment, 16*(1), 51–55. https://real.mtak.hu/191984/

Makk, A. (2021). Az adatvédelem alapjogi és magánjogi természete. In *Jogi tanulmányok 2021* (pp. 164–178). Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar. https://edit.elte.hu/xmlui/handle/10831/106561

Novotny, Á. (2005). Digitális Európa – valóság vagy vágyálom? In *Agria Media 2004: A digitális identitás az útlevelünk Európába* (pp. 151–163). Eszterházy Károly Főiskola Líceum Kiadó. https://publikacio.uni-eszterhazy.hu/6543/1/151_163_Novotny.pdf

OECD. (2023). OECD/INFE 2023 international survey of adult financial literacy. OECD Publishing. https://doi.org/10.1787/56003a32-en

Rab, Á., Szikora, T., & Török, B. (2026). Az internethasználat attitűdjei és az online bizalom Magyarországon 2019–2024 között. *Információs Társadalom*, *26*(1), 81. https://doi.org/10.22503/inftars.XXVI.2026.1.13

Sárközy, H. (2024). Pénzügyi műveltség, pénzügyi jólét és a digitális pénzügyi műveltség 2023. évi eredményei és összefüggései nemzetközi összehasonlításban. In *II. Csernyák László Konferencia Közleményei* (pp. 88–104). Budapesti Gazdasági Egyetem. https://doi.org/10.29180/978-615-6342-90-4_7

Zéman, Z., & Végh, K. (2010). Befektetési lehetőségek és a befektetői szokások Magyarországon. Szám-Adó, 19(5), 3–8.

Zsarnoczky-Dulhazi, F., Zsarnoczky, M. B., Kopper, B., Karpati, J., Molnar, C., Gogo, F. C. A., & Dávid, L. D. (2023). Promising European research results to improve hospitality in healthcare by eHealth.

International Journal of Hospitality Management, 112, Article 103411. https://doi.org/10.1016/j.ijhm.2022.103411

Zhong, R., Zhang, Q., & Zhao, Y. (2022). Research on Enterprise Financial Accounting Information Security Model Based on Big Data. *Wireless Communications and Mobile Computing*, *2022*(1). https://doi.org/10.1155/2022/7929846