
TECHNOLOGY, CYBERSECURITY AND PERSONAL DATA PROTECTION IN THE CONTEXT OF MULTIGENERATIONAL HUMAN RESOURCE MANAGEMENT

Prof. Mariana Usheva, PhD

International Business School, Bulgaria

Abstract. The present report presents results of a five-year generational study (2019-2024) in this part of the study on the role of technology, cybersecurity and personal data protection as key factors in human resource management in a multigenerational workforce. The study analyzes how different generations (T, X, Y, Z and Alpha) perceive digital security, what the main risks and challenges are when implementing information technology, and how HR policies can create trust, competence, and inclusion. By combining empirical data and modern scientific sources, recommendations are offered for effective and ethical transformation of the organizational environment with an emphasis on digital maturity and security.

Keywords: technology, cybersecurity, generations, personal data, human resources, trust, digital culture

JEL: M12, M15, J24, D83, K31

Introduction

In today's world, technology plays a key role in all aspects of life, including human resource management. With the development of digital platforms and automation, organizations increasingly rely on software solutions to optimize the processes of selection, training, management of generational diversity, and retention of talent. However, this technological advancement also brings with it new challenges related to cybersecurity and personal data protection. Multigenerational human resource management requires not only adaptability to the different needs and expectations of employees of different age groups, but also ensuring their security and privacy in the digital age. Personal data protection becomes critically important, as any breach can lead to serious legal and reputational consequences. Therefore, the integration of effective cybersecurity and personal data protection strategies is essential for successful multigenerational human resource management.

The presence of multiple generations within an organization – from Traditionalists (Generation T) to Digital-oriented Generations Z and Alpha – puts in front of HR managers with the complex task of balancing different technological expectations, security attitudes, and work styles. Generational diversity affects not only the preferred communication tools and learning

methods but also the perception of risks associated with digitalization, automation, and personal data protection.¹

The research identifies clear, pronounced generational specificities in the context of digital transformation. Special attention deserves aspects of information security, ethics in data management, and cybersecurity in a multigenerational work environment. The analysis considers not only the technological preferences of different age groups, but also their degree of sensitivity to privacy, trust in digital systems and readiness to comply with regulatory requirements standards like GDPR.

Based on the results obtained, specific recommendations are formulated for HR specialists, managers, and organizational leaders. Designers to create sustainable, inclusive, and safe digital work environments that take into account age diversity not as a barrier, but as a strategic advantage.

Exhibition

A generational approach to technology and security

Generational differences in the workforce have a significant impact on the adoption and use of technology, especially when it comes to security, privacy, and trust in automated systems. Different generations demonstrate not only varying degrees of digital competence, but also contrasting attitudes toward the risks, opportunities, and ethical dimensions of digitalization.

Generation T (born from 1941 to 1964) is characterized by a high need for structured information and personal contact. Traditionalists perceive technology as a functional tool, but not as a core element of the work culture. When it comes to information security, this generation tends to stick to established procedures, paper documents, and personal verification. They value traditional methods of communication and prefer direct face-to-face contact, which allows them to build trust and ensure the reliability of information. This caution and attention to detail make them particularly careful when using digital technologies and online platforms, as they often prefer physical archives and manual checks to confirm important data. Choudrie et al. (2020) also highlight that older employees often experience

¹ Results of a five-year study are presented, described in detail in the trilogy Usheva, M. (2025) *Multigenerational Human Resources Management: from Generation T to Generation Alpha*. Materials from two of the books are used, as follows: Usheva, M. (2025). *Multigenerational Human Resources Management: from Generation T to Generation Alpha. Individual Psychological Characteristics of Generations*, Book 1, Sofia, Publishing House of the International Business School (IBS)/ IBS Press, ISBN: 978-619-7610-32-1 (Print), ISBN: 978-619-7610-33-8 (E-book). Available at: <https://zenodo.org/records/14749133>

Usheva, M. (2025). *Multigenerational Human Resources Management: from Generation T to Generation Alpha. Peculiarities and Motivational Specificity of Generations*, Book 2, Sofia: Publishing House of the International Business School (IBS) / IBS Press. ISBN: 978-619-7610-37-6 (Print), ISBN: 978-619-7610-36-9 (E-book), DOI: 10.5281/zenodo.14915685. Available at: <https://zenodo.org/records/14915685>

anxiety when they have to use digital systems with a high degree of complexity, which requires additional support from HR policies.

Generation X (born from 1965 to 1980) is more adaptable, but relies on proven technologies and procedures. They expect security, reliability, and clearly defined standards when using digital systems. This generation perceives cybersecurity as a set of protocols and guidelines that must be strictly followed. They are ready to adopt new technologies, as long as they are well-founded and tested for their effectiveness and security. Generation X values the balance between innovation and established practices, looking for ways to integrate innovations within existing structures and rules. Their approach to cybersecurity is pragmatic and oriented towards minimizing risks by following established methodologies and standards. They typically value technologies that facilitate work while maintaining stable and familiar workflows.

Generation Y (born between 1981 and 1996) has been fully formed in a digital environment. They not only accept but also expect a high degree of technological integration. When it comes to cybersecurity, Millennials are aware of the risks but often rely on automated security tools such as antivirus programs, two-factor authentication, and cloud encryption. They seek a balance between security and convenience, preferring solutions that offer maximum protection without compromising ease of use. Millennials tend to use mobile applications and social networks for professional purposes, which requires them to be particularly attentive to privacy settings and control over personal information. Their approach to cybersecurity is dynamic and flexible, reflecting their desire to continuously improve and adapt to new technologies. Barrot et al. (2021) also note that this generation prefers interactive and personalized training on topics related to personal data protection and technological ethics.

Generation Z (born between 1997 and 2009) sees technology as a natural extension of their identity. Their behavior includes a high degree of digital flexibility, as they are accustomed to using multiple devices and platforms for communication, work, and entertainment. However, they are also sensitive to privacy and cybersecurity. Generation Z understands the importance of protecting personal data and actively seeks ways to control and manage their online identity. They tend to use VPN services, password managers, and other tools to enhance security, while demanding transparency from companies about how their data is processed and stored. This approach to cybersecurity reflects their awareness of potential risks and their desire to maintain control over their digital footprint. Al-Qudah et al. (2024) emphasize that Generation Z representatives are highly influenced by the organization's technological reliability, including its security practices and transparency in personal data protection, when adopting digital solutions.

Generation Alpha (born from 2010 to 2024) is not yet of working age, but analyses indicate that digital security will be perceived not as a „policy“ but as an irrevocable standard. This generation is growing up in a world where technology is an integral part of everyday life, and they will expect a high level of protection and security from the very beginning. For them, cybersecurity will not be just a set of rules, but a fundamental aspect of any digital service or product. They will demand intuitive and integrated security solutions that do not disrupt the user experience, while at the same time ensuring the safety of their data. Generation Alpha is likely to have higher expectations of employers and service providers regarding cybersecurity, insisting on transparency and accountability in this area. According to Prensky (2012), they will demand from organizations full transparency about data usage, the ability to control their own digital identity, and integrated protection through artificial intelligence and biometric technologies.

Regulatory and ethical standards in the context of cybersecurity

With the increasing digitalization of organizational processes and the increased mobility of the workforce, personal data protection and information security management are becoming a priority issue for organizations. The implementation of international regulations, such as the EU's General Data Protection Regulation (GDPR), requires coherence between technological solutions and human resources, with particular attention to transgenerational differences.

GDPR sets clear requirements for informed consent, transparency, limited access and the right to be forgotten, which require not only legal and technical mechanisms but also a cultural shift in how employees perceive privacy. This is a challenge in an environment where age groups show different sensitivities to digital ethics and data protection.

Generation T and X tend to stick to written instructions, paper consent forms, and prefer face-to-face communication when handling personal information. They perceive the risk of data leakage as high and are often more cautious about providing electronic access to personal files. Training aimed at understanding GDPR rights and responsibilities through real-life examples and simulations is recommended for them. This training should include practical exercises that demonstrate how to apply the principles of the GDPR in everyday tasks, as well as how to respond to potential security breaches. In addition, it is important to emphasize the importance of informed consent and transparency in the processing of personal data, using language that is easily understood and appropriate to their experience and knowledge. Through such measures, organizations can help these generations feel more confident and competent in the digital environment, while ensuring regulatory compliance.

Generation Y demonstrates a higher awareness of the right to personal data protection, but is not always aware of the details of the regulation. They

often assume that companies already implement security standards and expect technology platforms to automatically guarantee protection. However, it is important to provide specific information and training that explains exactly what the GDPR means and how it affects their rights and obligations. This includes familiarizing them with concepts such as informed consent, the right to access personal data, the right to rectification and erasure of data, and the right to restriction of processing. Training should be interactive and practical, using real-life examples and case studies to illustrate how to apply these rights in the context of daily work. In this way, Generation Y will be able to better understand their responsibilities and become more active participants in the process of personal data protection. According to Barrot et al. (2021), Millennials prefer modular online courses and adaptive guidelines integrated into the platforms they work with daily.

Generation Z demands complete digital transparency and control. They are actively interested in how, by whom, and for what their data is used. This generation is accustomed to living in a digital environment and understands the importance of protecting personal data. They expect companies and organizations to be open and transparent about their data collection, processing, and storage practices. Generation Z is willing to use privacy management tools, such as privacy settings on social networks and apps, and often checks the privacy policies of the platforms they use. To meet these expectations, organizations need to provide clear and accessible information about their data protection practices, as well as offer easy-to-use privacy management tools. Training for this generation should focus on practical skills and knowledge that will help them exercise their rights and control their digital presence. According to Al-Qudah et al. (2024), Generation Z prefers technologies that ensure user control, including adjustable privacy settings and clear feedback on data usage, which directly affect their trust and willingness to adopt digital systems.

To address these disparities, organizations need to develop comprehensive training and awareness strategies that cover all age groups. This includes not only providing information on legal requirements and best practices, but also fostering a culture of respect for privacy and data security. It is also important to create clear and easy-to-follow procedures for reporting breaches and incidents, as well as ensuring that data protection systems are constantly maintained and updated. Only through such a comprehensive approach can organizations ensure that all employees, regardless of their age, are engaged and active participants in the process of protecting personal data.

In this context, HR departments must play a dual role – both educating employees on cyberethics and privacy, and ensuring that technological systems and internal policies are adapted to different generational expectations. As Lee and Coughlin (2015) point out, designing digital

systems that account for generational needs, expectations, and limitations is essential for meaningful engagement, especially in areas such as employee training and technological adoption.

Generational security policies and best practices

The effective data protection and sustainability and the introduction of technologies into the organization depends not only on the availability of technical infrastructure, but also on the implementation of generational-sensitive security policies. HR departments should design approaches that take into account differences in technology behavior, attitudes towards privacy, and styles of perceiving information of different age groups. Different generations of employees have unique preferences and ways of working, which require adapted data protection strategies. The next tables (Table 1-1, Table 1-2, Table 1-3, Table 1-4, and Table 1-5) present specialized security policies and best practices aimed at five different generations – from Generation T to Generation Alpha. They are shown the key areas of focus, necessary technological tools, and additional notes that can help organizations create effective and sustainable measures to protect their assets and data. This includes the use of database management software, data, online learning platforms, gamified learning approaches, mobile risk assessment applications, and even artificial intelligence for adaptive protection. These measures not only increase security but also promote a culture of awareness and responsibility among employees, regardless of their age.

Table 1-1. Security policies and best practices for Generation T (born 1941 to 1964).

Policies and Practices	Technological tools	Additional notes
Formalized documentation.	Paper diaries and registers.	Provides clear trace and accountability . It is important to use standardized forms and templates for easy understanding and implementation.
Paper protocols for accessing personal data.	Physical locked cabinets.	Guarantees physical security of documents. Regular inspections and audits to ensure compliance with regulations.
Live seminars with the participation of information security experts.	Projectors and flipcharts.	Personal contact and opportunity to ask questions. Organizing regular meetings and workshops to raise awareness.

Individual consulting at data – related incidents.	Telephone emergency lines cases.	Fast response and personalized attention. Establish rapid response procedures at incidents and staff training to deal with them with situations.
--	----------------------------------	--

By following these policies and practices, organizations can provide a solid foundation for security that meets the needs of Generation T.

Table 1-2. Security policies and best practices for Generation X (born 1965 to 1980).

Policies and Practices	Technological tools	Additional notes
Integrated systems with clear described data protection instructions.	Database management software data.	Easy access and management of information. Use of centralized data management systems and access rights.
Ability to check access to official documents accounts.	Two - factor authentication systems.	Increased security and access control. Regular access log audits and notifications at unusual activity.
A system of training videos, supplemented with help materials.	Online learning platforms.	Flexibility and convenience at Creating a library of resources and frequently asked questions content updates.
Provided „assistant center“ at occurred difficulties.	Chatbots and telephone lines.	Fast and efficient problem solving. Multilingual service support and extended working hours.

With these policies and practices, organizations can address the specific needs of Generation Xers and increase their awareness of information security.

Table 1-3. Security policies and best practices for Generation Y (born 1981 to 1996).

Policies and Practices	Technological tools	Additional notes
Online platforms with modular information security training.	LMS (Learning Management Systems) ¹	Personalized and adaptive training. Ability to track progress and issue certificates.

¹ *LMS (Learning Management System)* is a software a platform that supports the creation, management and tracking of learning processes, providing tools for developing online courses, administering students and teachers, conducting tests and analyzing learning results. Examples of such systems are Moodle, Blackboard and Canvas, which are used in educational institutions, corporate environments and professional development organizations.

Gamified approaches to engagement in GDPR and cyberethics training.	Gaming platforms and applications. ¹	Increase motivation and engagement. Include elements such as points, rankings, and rewards.
Digital self - assessment apps habits and risks.	Mobile risk assessment applications. ²	Continuous awareness and improvement. Regular reminders and grade updates.
Anonymous channels reporting security breaches and breaches.	Anonymous systems reporting. ³	Promote open communication and trust. Ensure confidentiality and protection of whistleblowers.

Through these policies and practices, organizations can engage Generation Y and make them active participants in information security processes.

Table 1-4. Security policies and best practices for Generation Z (born from 1997 to 2009).

Policies and Practices	Technological tools	Additional notes
Customized settings for data protection and transparency.	Privacy management platforms. ⁴	Control over personal data and preferences. Possibility of individual settings and notifications.

1 *Gaming platforms and apps* often include security measures to protect users and their data. Steam, one of the largest digital platforms games, uses two-factor authentication (2FA) to increase account security. Epic Games Store also offers 2FA and data encryption to ensure consumer safety information. Mobile Games like Pokémon GO use SSL / TLS protocols to secure communication between players and servers.

2 *Mobile Risk assessment applications* help users identify and manage potential threats. The COVID Symptom Study app, developed by ZOE and King's College London, uses user data to evaluate risk of contracting COVID-19 and provide personalized recommendations. MyFitnessPal, a nutrition and fitness tracking app activities, uses algorithms to assess health risk based on the entered data and provides advice on improving lifestyle.

3 *Anonymous systems reporting* allow employees and citizens to submit reports of irregularities without fear of reprisals. An example of such system is EthicsPoint, which provides a platform for anonymous reporting unethical practices and violations in a corporate environment. Whistleblower Security is another a solution that offers secure communication and anonymity for individuals wishing to submit illegal signal activities.

4 *Privacy Management Platforms (PMP)* are *software* solutions that help organizations manage and protect the personal data of their customers and employees in compliance with various data protection regulations such as the General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR) in the European Union and CCPA (California Consumer Privacy Act). An example of such a platform is OneTrust, which offers tools for risk assessment, consent management and automation of personal data processing processes. Another example is TrustArc, which provides certification and privacy consulting services. These platforms provide tools and features that make it easier the processes of collecting, storing, processing and sharing personal data, while at the same time guarantee compliance with legal requirements security requirements and standards.

Real -time notifications when accessing or changing information.	Monitoring and warning systems.1	Immediate reaction at suspicious activity. Automated messages and actions at deviations.
Active participation in the selection of internal company applications and platforms.	Surveys and feedback forums connection.2	Employee involvement and commitment. Regular consultations and discussions on new technologies.
Ability to visualize the level of protection through dashboards and analytics.	Dashboards and analytics tools.3	Clear presentation of the current security situation. Regular reports and graphs for trend analysis.

With these policies and practices, organizations can meet the high expectations of Generation Z and provide them with the tools they need to effectively protect data.

Table 1-5. Security policies and best practices for Generation Alpha (born from 2010 to 2024).

Policies and Practices	Technological tools	Additional notes
Fully digitalized environment with automated security control systems.	AI -based security systems.4	High degree of automation and efficiency. Using machine learning for continuous improving protection.

1 *Monitoring and alerting systems* are designed to monitor various aspects of the IT infrastructure and *send* notifications at occurrence of problems or deviations from normal operation. An example of such Nagios is a system that monitors servers, networks and applications and sends alerts via email or SMS. Other popular system is Zabbix, which offers similar features and can be integrated with various cloud services and IoT devices.

2 *Surveys and feedback forums Connections* are tools that allow users to share their opinions and suggestions. in connection with products , services or processes. An example of a questionnaire tool is SurveyMonkey, which offers an easy way to create and distribute surveys online. The Reddit forum can also be used as a feedback platform. connection where Users can discuss and rate various topics and products.

3 *Dashboards and analytics tools* provide real - time data visualization and analysis that helps organizations make informed decisions solutions. An example of such tool is Google Analytics, which provides detailed web statistics traffic and user behavior. Tableau is another popular a tool that allows creating interactive dashboards and visualizations of data from various sources.

4 *AI- based security systems* use artificial intelligence to detect and prevent threats in real time. An example of such system is Darktrace, which uses machine learning to identify unusual patterns of behavior in networks and systems, signaling potential cyberattacks. Other An example is IBM Watson for Cyber Security, which combines AI and big data. data for threat analysis and assisting security teams in their work.

Biometric identification and access solutions.	Fingerprint scanner fingerprints, facial recognition. ¹	Increased security and convenience. Integration with mobile devices and other IoT technologies.
Artificial platforms intelligence that adapts the level of protection to user behavior.	Machine learning and behavior analysis. ²	Personalized and adaptable protection. Analysis of behavior patterns for early detection of threats.

Although not yet represented in the workforce, these policies and practices will be essential to the future security of Generation Alpha.

In general, the construction of such a differentiated system of policies allows not only to increase organizational cyber resilience, but also to create a culture of trust and responsibility among all age-related groups. This, in turn, contributes to reducing the risk of internal breaches and increases Commitment to information security policies. A successful information security strategy must be flexible and adaptable to meet the diverse needs and expectations of different generations of employees. By carefully planning and implementing appropriate policies and technologies, organizations can ensure a high level of protection and foster a culture of security across all age groups. Such a differentiated system of policies allows not only to increase.

HR management challenges and a transgenerational approach to security

Information security management in the organization cannot be effective without the active human participation of resources, especially in the context of a multigenerational workforce. HR managers face a range of challenges related to ensuring both technological security and organizational inclusion for employees with different digital habits, expectations, and attitudes towards security.

1. Different levels of digital confidence

Generations T and X often struggle with emerging platforms and software updates, which increases the risk of accidental security breaches, for

¹ *Fingerprint scanner fingerprints, facial recognition* are technologies, using biometric identity verification data. The fingerprint scanner Fingerprints are often used in smartphones and laptops, such as the sensors on the Apple iPhone and MacBook. The facial recognition is applied in access control and security systems, such as Face ID on the iPhone, as well as in some video surveillance systems that use facial recognition algorithms to identify people in real time.

² *Machine learning and behavioral analysis* are used to predict and optimize various business processes. An example of this is Amazon Personalize, which uses machine learning to personalize product recommendations based on user behavior. In marketing, companies like Netflix use algorithms to analyze viewer behavior to recommend movies and series that they would like. In healthcare, IBM Watson Health analyzes medical data and helps doctors make more informed decisions patient treatment decisions.

example, opening phishing emails or inappropriately storing sensitive information. Lack of sufficient knowledge and experience in using modern software solutions can make them vulnerable to various types of cyberattacks, highlighting the need for more in-depth training and support in this area. Al-Qudah et al. (2024) point out that although Generation Z is confident and proactive in using digital channels, they may underestimate the risks related to data sharing, which makes perceived security a critical factor for adoption.

2. Language and terminology barrier.

Older employees from Generations T and X often encounter difficulties at cybersecurity training when the language is strong, technical, and abstract. They demonstrate a preference for structured, clear, and logical information presentation formats. This approach allows them to more easily understand and remember key concepts and practices related to cybersecurity, which is essential for their effective protection in the digital environment. On the contrary, researchers (Barrot et al. 2021) clearly emphasize that younger generations prefer short visual formats and adaptive content that engages them actively. Therefore, HR professionals must ensure multi-format resources – seminars, infographics, video lessons, and mobile tests – are adapted to age profiles.

3. Insufficient transgenerational communication

At a lack of targeted efforts for intergenerational exchange, digital fragmentation arises – i.e. the different groups use different channels, do not share knowledge, and do not develop common practices. This creates weak units in the security system. The programs for the reverse mentoring, in which younger employees train older ones in a digital environment, has proven to be an effective mechanism for building trust and reducing these gaps.

4. Ethical dilemmas in automated surveillance.

The use of activity tracking software, email monitoring correspondence and evaluation through algorithms places under question the boundaries between security and privacy inviolability. Older employees from Generations T and X perceive similar systems as a threat to their personal autonomy and are more likely to react with distrust or resistance, especially when missing sufficient transparency about the scope of monitoring.

Tshazi and Civilcharan (2021) observe that younger generations, particularly Millennials, are generally more receptive to digital innovations, including automated systems, provided that such technologies ensure transparency, data control, and user autonomy. Concerns about privacy remain critical for adoption.

Recommendations for HR practices and technological inclusion with a focus on security

Ensuring information and digital security is critically important for every organization; effective strategies for managing these risks often require

a special approach that takes into account the different needs and preferences of employees of different age groups. Table 2 presents six recommendations aimed at improving digital and information security through age-based adapted measures that can significantly increase the level of protection and engagement among employees. It is important to keep in mind that for information security policies to be effective in a multigenerational workforce, HR management must adopt a differentiated, flexible, and ethically oriented approach that not only meets the regulatory requirements but also the psychological and cultural characteristics of different generations. Based on the presented research, several recommendations are derived that can help achieve this goal (Table 2).

Table 2. Recommendations for HR practices and technological inclusion with a focus on security.

Recommendation	Description
1. Conducting internal digital and information security audits by age groups.	The regular assessment of digital competence and security awareness allows identifying gaps and personalizing training strategies. Organizations that map their generations digital readiness, achieve higher degree of security and commitment.
2. Implementation of age-based adapted educational modules.	Video platforms lessons and infographics for generation Z, simulations and gamification for generation Y, and for generations T and X – live seminars, printed manuals and specialized maintenance.
3. Building a culture of technological trust.	HR policies should create a safe environment where employees do not fear sanctions at mistakes, but receive support and the opportunity to learn. The public sharing successes and good practices related to certainly, it is key.
4. Back mentoring and collaborations teams.	Promoting programs where Generation Z members educate their elders colleagues in using new technologies, including data protection systems. This increases security and strengthens intergenerational solidarity.
5. Engaging employees in the technology selection process.	The different ages groups should be included in pilot projects testing and evaluation of new platforms, especially those related with data protection and internal communication. This improves acceptance and decreases the resistance at implementation.
6. Providing psychological support for digital incidents.	The presence of a discrete A channel for reporting incidents (phishing, breaches, data compromise),

	combined with emotional and technical support is crucial for employees of all levels ages.
--	--

Implementing these recommendations can lead to significant improvements in the digital and information security of organizations. Through regular internal audits, age-appropriate training modules, building a culture of technological trust, reverse mentoring, engaging employees in the technology selection process, and providing psychological support in the event of digital incidents, companies can create a more secure and resilient work environment. These measures will not only increase data and system protection but also promote intergenerational cooperation and mutual respect, which is essential for the long-term success of any organization.

Conclusion

In the context of the deepening digital transformation, technology, cybersecurity, and privacy cannot be considered in isolation from the generational characteristics of the workforce. Multigenerational human resource management implies the need for a multidimensional approach that combines regulatory standards, technological solutions, and behavioral sensitivity.

The study confirms that generations differ not only in their level of digital literacy but also in their ethical perceptions, motivation to comply with security policies, and trust in automated systems. This requires a strategic effort on the part of HR management aimed at building a technologically inclusive organizational culture; creating age-specific training and ethical frameworks; and promoting intergenerational dialogue on topics of privacy, security, and digital autonomy.

Organizations that recognize the potential of age diversity not only as a challenge, but as a resource for sustainable digital development, will be able to build informationally responsible, socially engaged, and technologically literate work communities. These organizations will be able to integrate different perspectives and experiences, which will allow them to adapt their strategies and practices to the rapidly changing digital environment. In this way, they will achieve higher efficiency, innovation, and competitiveness on a global scale. It is also important to emphasize the importance of continuous training and professional development, which will help employees stay relevant and adaptable to new technologies and threats.

REFERENCES

- CHOUDRIE, J., PHEERAPHUTTRANGHKOON, S. & DAVARI, S. 2020. The Digital Divide and Older Adult Population Adoption, Use and Diffusion of Mobile Phones: a Quantitative Study. *Inf Syst Front* 22, 673–695. <https://doi.org/10.1007/s10796-018-9875-2> [viewed 2025-04-15].
- BARROT, JS, IA LLORENTE, and LP DEL ROSARIO. 2021. Students' online learning challenges during the pandemic and how they cope. *Education and Information Technologies*, 26(6), 7321–7338. <https://doi.org/10.1007/s10639-021-10589-x> . [viewed 2025-04-15].
- AL-QUDAH, A. A., M. AL-OKAILY, F. S. SHIYYAB, A. A. D. TAHA, D. A. ALMAJALI, R. MASA'DEH & L. H. WARRAD. 2024. Determinants of Digital Payment Adoption Among Generation Z: An Empirical Study. *Journal of Risk and Financial Management*, 17(11), 521. <https://doi.org/10.3390/jrfm17110521>. [viewed 2025-04-15].
- LEE, C. & J. F. COUGHLIN. 2015. Generational Differences in Adoption and Use of Information and Communications Technology. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59(1), 892–896. <https://journals.sagepub.com/doi/10.1177/1541931215591264>. [viewed 2025-04-15].
- TSHAZI, Z. B. & S. CIVILCHARRAN. 2021. Predicting Multi-Generational Technology Adoption Practices in a South African Context: Millennials vs. Generation X. In: *Perspectives on ICT4D and Socio-Economic Growth Opportunities in Developing Countries*. IGI Global, pp. 1–30. <https://doi.org/10.4018/978-1-7998-2983-6.ch001>. [viewed 2025-04-15].
- PRENSKY, M. 2012. *From Digital Natives to Digital Wisdom: Hopeful Essays for 21st Century Learning*. Thousand Oaks, CA: Corwin Press. Available from: <https://www.scribd.com/document/707767043/Marc-R-Prensky-From-Digital-Natives-to-Digital-Wisdom-Hopeful-Essays-for-21st-Century-Learning-SAGE-Publications-2012> [viewed 2025-04-17].

Prof. Mariana Usheva, PhD

ORCID ID: 0000-0001-8626-2762

International Business School

Botevgrad, Bulgaria

E-mail: musheva@ibsedu.bg