Transposition of transnational requirements relating to the protection of personal data and the security of information communicated in a global space while taking into account the groundswell concept

Adam Madleňák[1,*], *Marek* Švec[2]

[1]University of Ss. Cyril and Methodius in Trnava, Faculty of Mass Media Communication, Department of Marketing Communication, Námestie J. Herdu 2, 917 01 Trnava, Slovakia

[2]Matej Bel University in Banská Bystrica, Faculty of Law, Department of Civil and Labor Law, Komenského 20, 974 01 Banská Bystrica, Slovakia

Abstract

Research background: The adoption of the GDPR Regulation prompted the introduction of a unified regulation on the protection of personal data and highlighted the need to implement security measures relating to information disseminated across businesses operating in several mainly European countries. In practice, the adopted internal standards at the group level are expected to be introduced to the internal environment of individual local subsidiaries. The need to take into account specificities of national legal systems, as well as a specific environment capable of creating a secondary response - a groundswell has also became important. The legal framework of privacy protection in relation to the confidentiality of information disclosed by employers thus represents a fundamental challenge for the interaction between global requirements and local legislation, taking into account the specific assumptions of the business entity concerned.
Purpose of the article: The aim of the paper is to describe the range of problems and solutions regarding the process of introducing internal processes of business entities in terms of data security. Moreover, the paper also pays attention to personal data protection legislation.
Methods: In an effort to achieve the set goal, the authors used analytical, inductive, deductive and comparative research methods in order to identify areas of problems in relation to intrusion into the privacy of individuals in the online environment and internal communication channels. By synthesising knowledge published in domestic and foreign literature it was possible to draw up the key terminology.
Findings & Value added: The experience of the authors in setting up the internal environment of business entities with regard to the issues in question (personal data protection and security of information disclosed in connection

* Corresponding author: adam.madlenak@ucm.sk

with the decision-making power of national regulators) contributes to the knowledge in the given field.

Keywords: *control mechanism; personal data; data security; communication; groundswell*

JEL Classification: *F63; M31; M54*

1 Introduction

The effort to unify approaches in individual legal sectors at the European and non-European level has sparked an interest in unifying the rules within multinational companies, in particular groups and holdings. In practice, this premise is reflected in the efforts of business entities whose (more or less) independent subsidiaries (this dependence/ independence is given by local legislation) operate in individual states to adopt uniform transnational legislation in certain important areas crucial for internal policies and legal frameworks. A typical practical example is the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter "*GDPR*"), as a result of which the effort to enforce unified group regulations governing the protection of personal data in the internal environment of all property-related business entities or those that meet the condition of mutual relationship between the controlled and the controlling person came to the forefront. Fulfilment of this requirement, i.e. the unified approach to personal data protection and data security in general across related enterprises is the basic starting point for obtaining data by central management from subsidiaries and their verification and implementing general supervision in this regard. In this regard, we usually talk about some form of established centralized audit or audit on the level of the group or holding under which information and data, often of a personal data nature relating to the employment, business or civil law relationships, is collected (Kupec and Pisar, 2021). When using the term "group" or "holding", we mainly refer to the German and Austrian legislation, occasionally Czech legislation which follows the two previous semantically and logically. Czech Act no. 90/2012 Coll, the Commercial Code defines group in the provision of Section 66a par. 7, as follows "*If one or more persons are subject to unified management (hereinafter referred to as the "controlled person") by another person (hereinafter referred to as the "controlling person"), these persons form a group (holding) in which the controlling person and its companies, including the managing person, shall constitute members of such group. Unless proven otherwise, the controlling person and the entities controlled by it shall be deemed to form a group. Persons may be subjected to uniform proceedings by contract (hereinafter referred to as the "controlling agreement"). The controlling agreement may also be concluded in relations between the controlling entity and its controlled entities*." German Aktiengesetz comes with the following wording in Section 18 "*If a controlling and one or more controlled enterprises are subject to the common direction of the controlling enterprise, such enterprises shall constitute a group; the individual enterprises shall constitute members of such group. If enterprises are parties to a controlling agreement (...) or if one enterprise has been integrated into the other (...), such enterprises shall be deemed to be subject to common management. A controlled enterprise and its controlling enterprise shall be presumed to constitute a group*".

It is of no use to take into consideration other descriptions of a group. Their existence is directly linked to the efforts of the owners of multinational enterprises to retain influence and the right to enter (control) all processes of subsidiaries or companies under the ownership

influence of owners, regardless of the national (local) legal environment in which their subsidiaries operate (Szeiner et al., 2020). However, while the original group control mechanisms focused mainly on the assessment of business relations, production, paperwork and technical issues taking place in local companies, the increasing degree of flexibility of labor relations has paved the way for the implementation and thus significant penetration of the notion of group investigation into the local labor relations concluded in accordance with law (Vavrecka et al., 2021). In many respects, however, the increased interest of groups in employment relations is also the result of the increased number of cases where groups identified actions detrimental to the their own interests, e.g. giving preference to business partners in exchange for additional benefits on the part of senior employees, cooperation with state administration bodies in exchange for preferential treatment in individual administrative proceedings, selection of service companies providing repairs of machines and devices with poor benefit-cost ratio (Fraccastoro et al., 2021). These actions may also entail large-scale property damage which often meets the factual nature of property crimes. However, due to the preservation of the group's good name, the vast majority of investigated cases are not referred to law enforcement authorities and end with the conclusion of an "employment termination agreement", especially for first- or second-line employees (base on the employer's organizational structure). The key paradigm thus becomes the issue of ensuring the confidentiality and security of information disclosed abroad, as the communication flow is almost constant and the possibility of a security incident happening is relatively high.

Taking into account the predominantly local nature of of labor relations and regulations, e.g. in the individual Member States of the European Union, the implementation of transnational requirements into the local internal environments of individual subsidiaries often clashes with local laws due to the absence of the necessary legal basis tackling this issue. The legal relations between the central management of the group and subsidiaries follow a hierarchical principle, which in principle does not take into account individual national regulations, i.e. obtaining information while any sort of checks or verifications are outside any legal framework or directly contrary to the national legal framework (Gaydarenko et al., 2021). This will, of course, call into question the whole group investigation process, as due to the effort to separate local ties from the whole process the process itself does not involve local employer representatives. Subsequently, local employer representatives become passive recipient of the decision on whether the group violated the group regulations or the "*code of conduct*" or not. The decision entails specific employment-related penalties against employees pursuant to the local labor law. Thus, although the local employer of the employee has the right to exercise the authority over the employee pursuant to law, in fact the employer is hierarchically subordinated to the group regulations and institutions established by the group to ensure independent investigation in individual local branches over which this employer has no power (these investigators have even broader powers in some areas than senior employees of the local employer). The group then conducts investigation into a possible breach of duty by the employee, often regardless of the employer's local internal management processes or the local employer's internal environment, resulting in a decision as to whether the charges against the employee will be dropped or pursued. The local employer (usually his HR department) is notified on the outcome of the investigation. In case the employee's guilt is proven, the local employer is obliged to draw the labor consequences against the employee according to national labor law.

At first glance, the outlined process of the group investigation towards employees of local companies seems as a legal construct with several controversial or questionable issues not in compliance with national law and employee rights to legal protection against employers. As a result, significant opportunities to challenge the whole investigation process may arise which could result in the termination of the employment and at the same time understandably

create resistance or inability to transpose transnational data protection or information security requirements into local subsidiaries.

2 Methods

The aim of the paper is to point out, on the basis of a critical analysis, recurring problems related to the processing and storage of information by business entities with regard to established internal regulations and rules. In particular, the authors pay attention to the quality of implemented internal processes aimed at preventing accidental, unauthorized or illegal changes to data, loss of processed personal data and their disclosure to third parties in companies operating on the international market. The authors chose combined methodological approach to ensure a comprehensive and systematic processing of selected issues through selected qualitative and logical-cognitive methods. In addition to the in-depth critical analysis used to describe the current situation, induction, deduction, comparison and synthesis were employed to broaden knowledge, spark discussion and draw up conclusions. Slovak as well as foreign literary sources, monographs and peer-reviewed journal articles in bibliographic databases were also employed. The research results are supplemented by the authors' own opinions based on the experience gained when working on several scientific projects and grants in the researched field.

3 Results and Discussion

3.1 The essence of transnationality of internal company regulations

The establishment and operation of a group investigation or control mechanism as a manifestation of data security usually depends on internal regulations adopted by the authorized body of the group (for joint stock companies, as a traditional type of company, regulations are adopted by the company's board). The effectiveness and binding nature of the regulation adopted on the group level is ensured by a formal declaration of commitment given by all companies in the group at the beginning of the internal document and a general obligation to include binding regulations in the local employer's own internal regulations (Bencsik et al., 2019). However, the process of transferring these binding regulations to the employer's internal local environment in individual countries is not examined. Nevertheless, given the nature of the group document in question, deviations from its content are generally not allowed, as the purpose and aim of the documentation to be implemented could be undermined. Group regulations governing the position and implementation of the group investigation do not generally define the relationship between the group investigation and an investigated employee or local employment law - they only define their hierarchically superior position to the management of local companies and to the group management itself (Grencikova et al., 2021). Taking into account the predominantly national nature of labor relations, e.g. in the individual Member States of the European Union, however, the implementation of transnational requirements into the local internal environments of individual subsidiaries may become problematic, especially in relation to the absence of the necessary legal basis. The legal relations between the central management of the group and local companies follow a hierarchical principle, which in principle does not presuppose the existence of the specifics of individual national regulations, i.e obtaining such information and subsequent investigation or inspection is outside any legal framework or directly contrary to the national legal framework.

In this respect, however, the group investigation at the local employer may become a problem as the implementation of the notion of group investigation into the internal

environment of the local employer is rather formal (declaratory adoption of the group regulation by local management) as its content is not implemented to local regulation and directives under local labor law. The group's regulation on the group investigation has similar legal position as the group's regulations on the code of conduct or other directive regulating "ethical behavior" – they are also not implemented into the content of the employer's internal management processes. The question arises as to what form this regulation should take to be implemented in the employer's internal environment. As a rule, it should be part of the employer's internal environment only if it is capable of changing the rights and obligations of employees, but only if this is permitted by the relevant labor law (it may also be a law that is related to the work performance of the employees concerned, not necessarily labor law).

Internal regulations (since their issuance constitutes unilateral acts by the employer, although with the possible participation of employee representatives) cannot impose obligations beyond the law, the employee's conditions arising from the employment contract or collective agreement. Employees are bound by internal regulations only if these are in accordance with generally binding legal regulations and if the employees are duly acquainted with them. However, the group regulation on the position and operation of the group investigation does not constitute an internal management act adopted by a local employer, although it may become (to some extent) the internal management act by way of its transposition into the internal environment upon the employer's decision (local employers usually only provide translation of thereof into the employees' mother tongue (state language) and then issue it as an internal management act of the employer in its unaltered form) (Hatzithomas et al., 2016). However, since no one examines the content of this internal company regulation and the possibilities of its inclusion in the internal environment of local employers, the level of its compliance with national legislation is not assessed. In this regard, a conflict with the competence of employees' representatives in relation to the adoption of internal regulations of the employer (especially the work regulations according to Section 84 of the Labour Code) and the competence of negotiations according to Section 13, par. 4 of the Labour Code arises, as even such a form of group investigation may result in the introduction of a control mechanism at the employer and thus invade the privacy of the employee.

If we take into account the obligation of employees to participate in such a form of group investigation, i.e. employees are notified via the employer's communication platform the date of the meeting or they are requested directly by the group investigators to provide documents on a certain issue, group investigators obviously act on behalf of the local employer without such an instruction being issued to the employee by the authorized persons of the local employer. To explain, it is necessary to add that this is not an obligation stipulated e.g. in the employment regulations or other internal regulations of the local employer, but the request made by the group investigation body is considered to be an instruction issued by the local employer within the internal environment of the employer. Due to the nature of the group investigation (independent of local processes), the representative of the local employer may not even know about this instruction to participate in the investigation or to submit documents. Even though information is occasionally provided to the immediate superior of the employee or department in charge of local auditing or monitoring, this is not usually the case given the nature of their involvement in the investigation and the existence of local links (Vlahou et al., 2021). In practice, it may happen that none of the representatives of the local employer (senior employees or the relevant department of the local employer) know that the group investigation is taking place.

Although the employee’s obligation to participate and cooperate in the group investigation is undisputable, the obligation formulated in this way is not included in any internal regulation of the employer, regardless of possible participation of employee representatives under local employment law (Kupec et al., 2021). Therefore, if we take into

account provision of Section 84 of the Labor Code on the adoption of work regulations by the employer and take into account the fact that group's regulations may introduce a new set of employee-related obligations, these should be introduced in line with work regulations (and become their inherent parts). The enforcement of such internal regulations of the employer without taking into account employee representatives clearly contradicts the process of adopting internal employee-related regulations (code of conduct/ employment discipline), in particular in relation to the provision of Section 84 of the Labor Code. Moreover, refusal to participate in the group investigation is considered a breach of employment discipline, although such an obligation (but also its breach), is not actually set and regulated in any internal regulations of the employer. Thus, if we perceive the implementation of group regulations at local employers as a tool to extend the powers of the employer through internal company regulations (the status of adopted codes of ethics/ conduct, as well as the above-described case of the regulation governing group investigations), which clearly violates employees' right to privacy, the procedure according to the internal company regulations may be questioned if it demonstrably circumvents the local labor law regulating adoption and implementation of certain types of internal company regulations regulating the obligations of employees (their employment discipline) without taking into account the right of employee representatives to take part in the process. The above is possible when the employer concludes that such a process is in fact implementation of a control mechanism (as discussed below in more detail).

However, the group investigation or investigation at the local employer (as a tool to ensure compliance) may be perceived as a form of invasion into privacy of the employee. Thus, the investigation may fall within the legal framework of the control mechanism at the employer with reference to Section 13, par. 4 of the Labour Code. Before provisions of Section 13, par. 4 of the Labour Code are implemented in the assessment of the proceedings against the employee, various forms of employer's control mechanisms must be identified. These sometimes do not meet particulars set out in personal data protection legislation, especially the GDPR. The concept of control activities in terms of the provisions of Section 13, par. 4 of the Labor Code may thus acquire much broader meaning and scope of use in practical situations than protection of personal data of employees. According to Section 13, par. 4, first sentence of the Labor Code, invasion of employee's privacy include, inter alia monitoring, recording telephone calls, inspection of e-mails sent from the work e-mail address and delivered to this e-mail address without notifying the employee, as well as introduction of a control mechanism aimed at monitoring the employee with the secondary consequence of obtaining the employee's personal data (the legislation on personal data protection applies). The activity of the employer which could be perceived as intrusive may fall within the legal framework of the provisions of Section 13, par. 4 of the Labour Code, yet is not necessarily labelled as a control mechanism. According to Section 13, par. 4, first sentence of the Labor Code, the employee's privacy may be invaded in this way (an objective reason is defined - the obligation on the part of employer is fulfilled), but such action by the employer will not necessarily result in introduction of a control mechanism as it does not meet the requirement of regularity (duration of the control mechanism, etc). The implementation of control activities will be triggered by a subjective or objective reason on the part of the employer ad hoc without being subject to any kind of employment liability. Another argument regarding the broader concept of invasion of employee privacy through monitoring activities tackles the ambiguous interpretation of the term "monitoring", pursuant to provision of Section 13, par. 4 Labour Code. The term in question should not be identified exclusively with CCTV, as the linguistic and legal interpretation of the provision of Section 13, par. 4 Labour Code gives room to several possible interpretations. If we take into account the conventional interpretation, the term "monitoring" can be interpreted as supervision or oversight (Hitka et al., 2021; Syroid et al., 2021). However, monitoring does not necessarily

mean the employer's obligation to introduce a control mechanism or to carry out this monitoring exclusively by technical means. The said term may also include the performance of monitoring activities by the employer which may take place e.g. only in the form of physical monitoring by the manager or the employer or the introduction a control mechanism through technical means. However, the term may also cover situations where the control mechanism of the employer has been introduced but is not carried out through the technical means – it is carried out in another way, e.g. in the form of an observation method to determine the employee 's alcohol consumption (breath test without the use of a measuring device).

In this respect, the interpretation of the term "monitoring" that narrows it down to the use of technical means, e.g. CCTV is plainly wrong. Assuming that we would come to the conclusion that the group investigation is a monitoring activity under which the employer does not introduce control mechanism pursuant to Section 13, par. 4 of the Labor Code, it is not necessary (although not common in practice) to inform employees on the existence of such internal regulation or to acquaint them with its content. In this regard, the employer is not obliged to inform employees on the performance of monitoring activities aimed at, for example, detecting breaches of employees' employment discipline or unsatisfactory performance of work tasks. To confirm the premise in question, reference may be made to the judgement of the Supreme Court of the Czech Republic of 7 August 2014, file no. 21 Cdo 747/2013 ("*The employer is authorized to monitor the use of work equipment which is provided to employees to perform their work and to check whether it has not been misused*"). However, if the nature of the monitoring activity fulfills (fulfilled) the substantive preconditions stated in the provision of Section 13, par. 4 of the Labour Code (i.e. the control mechanism should be introduced and negotiations with the employees' representatives should take place and the employees should be informed), the employer's conduct can be assessed as being in conflict with the relevant provisions of the Labor Code and thus questioned on the basis of the internal company regulation in question (including any imposed labor sanctions).

The whole situation was complicated even further by the activity of the Slovak supervisory authority at the time of the adoption of the GDPR Regulation. Introduction of a control mechanism according to Section 13, par. 4 of the Labor Code from the point of view of personal data protection is from the position of supervisory body (Office for Personal Data Protection of the Slovak Republic), but also from the point of view of employers themselves was perceived as the introduction of monitoring, i.e. activities aimed at monitoring the fulfillment of duties by employees at the workplace using technical aids - personal data are processed through information systems with as little human interference as possible. Even at present, the Office for Personal Data Protection of the Slovak Republic perceives the provision of Section 13, par. 4 of the Labor Code as monitoring and not as an intrusion into privacy. This is also evidenced by the list of processing activities issued by the Office for Personal Data Protection of the Slovak Republic in accordance with Article 35, par. 4 of the GDPR Regulation for which an impact assessment must be carried out (Švec and Valentová, 2021). The list in question was subject to review by the Data Protection Committee. Point 9 of that list mentions the processing operation *'Monitoring the employee's work for serious reasons arising from the specific nature of the employer's activity'*, under which the employer is obliged to carry out an impact assessment whenever the employer monitors the employee for serious reasons. Although the list of the Office for Personal Data Protection is not explicitly based on Section 13, par. 4 of the Labor Code, it was clear inspired by it. In the Methodological Guidelines concerning the lawfulness of personal data processing, the Office for Personal Data Protection of the Slovak Republic mentions a control mechanism as a lawfull reason for personal data processing. It also recommends using the public interest or the legitimate interest of the operator (depending on the type of operator and its activities) as

a legal basis for personal data processing (Žuľová, 2021). However, it is not clear whether data protection should also cover the issue of transnationality (cross-border transmission of data) because if the employer fails to introduce a sanction system in the internal company regulation, it will not consitute a legal framework falling under the control mechanism according to the Labour Code. Consequently, the employer could significantly weaken the system of set transnational requirements for the security of communicated data, thus significantly simplifying the whole process.

The specificity of the above-described situation manifests itself when information obtained unofficially, i. e. as a manifestation of the groundswell concept, becomes the basis for the start of monitoring (Neznamova et al., 2020). In practice, the employer obtains information about the employee, e.g. about their health or privacy (and this information constitutes a breach of the employee's duty) from the active or passive action of third parties (e.g other employees of the employer) who pass this information to the employer or manager (gossips, talks behind one's back, slander or submission to a group-wide anonymous compliance system). On the basis of the information thus obtained, a process of monitoring activities is subsequently initiated, with the group investigation representatives investigating and verifying this information in the local subsidiary - information found during the investigation is transferred cross-border (often with transfer to third countries), thus giving rise to the possibility of a security incident and the need to take additional security measures in the framework of transnational security requirements. At the same time, however, such conduct of the employer may be classified as contrary to the data security requirement set out by the GDPR. In such cases, data in question may fall under Art. 11, the Basic Principles of the Labour Code and be seen as relevant to the employer with regard to the agreed type of work (i.e. the employer learns that their employee is pregnant, although the employee themselves did not notify the employee and the employer sends the employee for a special medical check-up). However, such data and information have been obtained in a "non-standard" way. In this case, it is possible to apply provisions of Art. 6, par. 1, letter (c) of the GDPR Regulation as the legal basis for the processing of personal data. However, from the point of view of the GDPR Regulation, it is necessary to take into account the fact that information obtained from informal sources cannot be considered as lawfully obtained and cannot be processed, i.e. they cannot be formally processed in the personal records of the employee (Ntouvas, 2019; Žuľová et al., 2018). If, on the basis of unofficial information, the employer decides to arrange a medical check-up, he cannot use the information obtained based on gossips. It is then questionable on what grounds and for what reasons the employer arranges medical check-up for the employee. Even though such conduct is standard in practice, however, from the point of view of the GDPR Regulation, such processing of personal data is perceived as illegal as data has not been obtained in accordance with the law. The employer should look for other sources to base their reasonable concern on, such as a decrease in the employee's work performance, frequent sick leaves and the like.

4 Conclusion

Looking for ways to improve the process of transposition of transnational data security and data protection requirements into local legislation is, basically, unnecessary. Although it is understandable that companies strive to implement unified group-wide regulation in this area, there is simply no legislation that would simplify the transposition process even if the local regulation and specifics were taken into account (groundswell penetrations). The group directives, regulations and the requirements contained therein (including personal data security regulation or security in general) are in many cases formulated in a way so as to be applicable in different legal, political, cultural and social conditions of countries in which individual companies belonging to the group operate. Limited direct applicability of

regulations, vagueness of the provisions of the group directives and their direct conflict with national laws and the subsequent application of the *ordre public* principle are a direct result of the group's pursuit of group-wide applicability of regulations. The effort to have a widely applicable unified text of group directives and regulations often results in a text that has the nature of general principles or guideline rather than a normative act outlining specific rights and obligations of employees (Gustafsson and Polynczuk-Alenius, 2018). Some groups prefer to issue group-wide guidelines in accordance with the law of the country in which the group's management center is located. The individual companies of the group are then obliged to adopt these group directives with no or only minimal changes, i.e. translate the original text of the group directive. Terminology linked to a specific legal system, differences in the same or comparable legal institutes in individual legal systems and, last but not least, different local mandatory norms of local labor law do not allow for smooth transposition of group directives and regulations without alternations (pursuant to local law).

The future transposition of transnational requirements may only go two ways - either transnational documents which are to be implemented on the national level and in the employer's internal system will become more vague, or these transnational documents will become more flexible and be based on special internal regulations of the employer and will take into account the group requirements, e.g. implementation of monitoring activities or group security-related investigation, thus conforming to the local legislation (the law of the Slovak Republic).

Acknowledgements

The research was supported by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences (VEGA, No. 1/0458/21) under the project entitled "Management of the "groundswell" concept by business entities in promotion of environmentally-friendly products in times of technology interference".

References

1. Bencsik, A., Juhasz, T., Mura, L., & Csanadi, A. (2019). Formal and informal knowledge sharing in organisations from Slovakia and Hungary. *Entrepreneurial Business and Economics Review*, 7(3), 25-42.
2. Fraccastoro, S., Gabrielsson, M., & Pullins, E. B. (2021). The integrated use of social media, digital, and traditional communication tools in the B2B sales process of international SMEs. *International Business Review*, 30(4), Art. No. 101776.
3. Gaydarenko, V. A., Arutyunian, V. S., Belogash, M. A., Rabotnikova, N. A., & Sharonin, P. N. (2021). Development potentials of international marketing in modern environment. *Laplage em Revista*, 7, 360-366.
4. Grencikova, A., Navickas, V., Kordos, M., & Huzevka, M. (2021). Slovak business environment development under the industry 4.0 and global pandemic outbreak issues. *Entrepreneurship and Sustainability Issues*, 8(4), 164-179.
5. Gustafsson, J., & Polynczuk-Alenius, K. (2018). Media and communication between the local and the global. *Media and Communication*, 6(2), 145-148.
6. Hatzithomas, L., Fotiadis, T. A., & Coudounaris, D. N. (2016). Standardization, adaptation, and personalization of international corporate social media communications. *Psychology & Marketing*, 33(12), 1098-1105.

7. Hitka, M., Schmidtova, J., Lorincova, S., Starchon, P., Weberova, D., & Kampf, R. (2021). Sustainability of human resource management processes through employee motivation and job satisfaction. *Acta Polytechnica Hungarica*, 18(2), 7-26.
8. Kupec, V., & Pisar, P. (2021). Auditing and controlling as a tool for SME marketing risk management. *Marketing and Management of Innovations*, 12(1), 225-235.
9. Kupec, V., Pisar, P., Lukac, M., & Bartakova, G. P. (2021). Conceptual comparison of internal audit and internal control in the marketing environment. *Sustainability*, 13(12), Art. No. 6691.
10. Lorincova, S., Cambal, M., Miklosik, A., Balazova, B., Babel'ova, Z. G., & Hitka, M. (2020). Sustainability in business process management as an important strategic challenge in human resource management. *Sustainability*, 12(15), Art. No. 5941.
11. Neznamova, A. A., Kuleshov, G. N., & Turkin, M. M. (2020). International experience in personal data protection. *Jurídicas CUC*, 16(1), 391-406.
12. Ntouvas, I. (2019). Exporting personal data to EU-based international organizations under the GDPR. *International Data Privacy Law*, 9(4), 272-284.
13. Syroid, T. L., Kaganoyska, T. Y., Shamraieya, V. M., Perederii, O. S., Titov, I. B., & Varunts, L. D. (2021). The personal data protection mechanism in the European Union. *International Journal of Computer Science and Network Security*, 21(5), 113-120.
14. Szeiner, Z., Mura, L., Horbulak, Z., Roberson, M., & Poor, J. (2020). Management consulting trends in Slovakia in the light of global and regional tendencies. *Journal of Eastern European and Central Asian Research*, 7(2), 191-204.
15. Švec, M., & Valentová, T. (2021). *Prevencia negatívneho zásahu do súkromia zamestnanca*. Wolters Kluwer.
16. Vavrecka, V., Zauskova, A., Privara, A., Civelek, M., & Gajdka, K. (2021). The propensity of SMEs regarding the usage of technology enabled marketing channels: evidence from the Czech, Slovak and Hungarian SMEs. *Transformations in Business & Economics*, 20(2), 223-240.
17. Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., Bischoff, R., Black, P. C., Boehm, F., & Ceraline, J. (2021). Data sharing under the general data protection regulation time to harmonize law and research ethics? *Hypertension*, 77(4), 1029-1035.
18. Žuľová, J. (2021). *Výber zamestnancov – právne úskalia obsadzovania pracovných miest*. Wolters Kluwer.
19. Žuľová, J., Barinková, M., Dolobáč, M., & Varga, V. (2018). *Spracúvanie osobných údajov zamestnanca podľa GDPR*. Pavol Jozef Šafárik University in Košice.