SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 144

GENERAL DATA PROTECTION REGULATION GDPR) AND ITS IMPLICATIONS FOR SOFTWARE SUPPORTING AUTOMATION OF PRODUCTION

Elżbieta MILEWSKA

Silesian University of Technology, Faculty of Organization and Management; Elzbieta.Milewska@polsl.pl, ORCID: 0000-0001-8053-4333

Purpose: The purpose of this article is to illustrate how the General Data Protection Regulation GDPR), which came into force in 2018 in Polish legal system, affects protection in the scope of collection, processing, storage and transfer of personal data in IT systems supporting production.
Design/methodology/ approach: Because production control systems are based on the identification and analysis of human and machine resources behaviour, a significant impact of recent legal regulations on automation of manufacturing processes is perceived. However, according to GDPR, the data enabling unambiguous identification are protected.
Findings: Resource recognition is not only important for the scheduling of production activities, but also for event logging.
Research limitations/implications: It should be noted that both the allocation of human resources, taking into account the boundary conditions for the execution of tasks and the substitutability of individual employees, as well as reporting the efficiency and effectiveness of production, requires the unambiguous identification of people. It is carried out by means of one or several factors that physically, mentally, economically or socially describe the resource.
Practical implications: Since the coordination of the company's production activities requires the processing of data describing human resources, taking into account the aspect of their security, it is necessary to create a new business model, which is the subject of research presented in this document.
Originality/value: Ensuring the security of data in the IT system, in addition to user authentication to resources, means also protection against accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed. When making decisions about the application of certain security measures, it is necessary to take into account the value of the data and the effects that the infringement may cause.

Keywords: digital transformation, Industry 4.0, privacy threats, situational awareness, smart factories.

Category of the paper: Viewpoint, General review.

1. Introduction

Undoubtedly, the development of information technology, which is a natural consequence of globalization, posed new challenges in the field of personal data protection. It has transformed both the economy and social and private life, facilitating the exchange of information for individuals, businesses and public institutions. Technological progress caused a significant increase in the scale of the collection and sharing of personal data. It also led to an unprecedented level of its processing. The latest trends in industrial automation, such as Industry 4.0 Gilchrist, 2016), have generated the demand for intelligent devices supporting production activity that are equipped with sensors collecting and processing information from their environment. Use of IIoT Industrial Internet of Things) Gilchrist, 2016) devices, which transmit data from dispersed locations for storage, and further processing and analysis, opens up new challenges for security of personal data and the privacy of employees Gilchrist, 2016; Wurm et al., 2016). Therefore, it should not raise any doubts that with the development of digital economy, public awareness of the possibility of using personal data should increase Cornock, 2018), and should be accompanied by the conviction that it is necessary to guarantee effective protection of personal data. Abuse in this area could cause disastrous consequences, not only for the individual or the enterprise, but also for the entire economy.

As of 25 May 2018, the General Data Protection Regulation 2016/679 GDPR) of the European Parliament and of the Council of 27 April 2016 is in force. In Polish legal system, it was introduced as the "Rozporządzenie o ochronie danych osobowych RODO)". The GDPR repealed the earlier Directive 95/46/EC [95/46/EC] The Official Journal of the European Union L.2016.119.1) and applies to all EU Member States EU). The purpose of this normative act is to simplify and harmonize data protection laws across Europe and to provide citizens an unprecedented control of their personal data. The GDPR defines the rules for storing, accessing and processing personal data of every EU citizen, in any country or territory of the EU, even if the processing takes place outside the EU European Parliament and Council, 2016). One of the significant changes in the law is the inevitability of the penalty in the event of improprieties. The new regulation applies to all entrepreneurs, regardless of the size of the company and the business profile Kościuk, 2018).

The purpose of this article is to illustrate how the General Data Protection Regulation European Parliament and Council, 2016), currently introduced in the Polish legal system, affects protection in the collection, processing, storage and transfer of personal data in IT systems supporting production. The publication describes the requirements for software automating manufacturing operations in a hybrid environment.

2. Legal basis for the processing of personal data

The concept of data processing is defined in art. 4 point 2 of Directive EU) 2016/680 of the European Parliament and of the Council European Parliament and Council, 2016). The legislator stated that such activity means any operation or set of operations performed on personal data or personal data sets in an automated or non-automated way, such as collecting, recording, organizing, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, distribution or other type of sharing, matching or combining, limiting, deleting or destroying. The aforementioned legal act establishes, therefore, the concept of a broad definition of data processing, consisting in the lack of a top-down definition of all activities that fall within the scope of this term.

Currently, processing is most often carried out using IT systems, including ERP Enterprise Resource Planning) systems. In the area of production management, it is implemented using APS class systems Advanced Planning and Scheduling) and MES Manufacturing Execution System) Milewska, 2011a, 2011b, 2017a). Automated creation of production plans and scheduling orders, taking into account various criteria limiting the course of production processes, must take place on the basis of a description of owned resources, which are also direct-production employees Milewska, 2014a, 2014b, 2016, 2017b).

Although there are no precise technical requirements, GDPR contains many premises from which one can deduce expectations regarding the functionality of IT systems for the needs of the regulation. The requirements can be divided into the following categories, which concern:

- functionality of software for processing personal data,
- backup and archiving software,
- required level of security.

Each of the points will be described below.

2.1 Requirements regarding software functionality

Functionality of the software should mainly ensure implementation of rights of persons whose data is stored and processed, and obligations of the personal data controller. IT systems in which personal data are processed must enable, among others European Parliament and Council, 2016):

- limitation of the data processing period to be compatible with the purpose of processing limitation of storage) Article 5. point 1 e);
- withdrawal of consent on the basis of which data are processed Article 7. point 3),
- implementation of the right of access by the data subject Article 15. point 3),
- implementation of the right to rectify data Article 16),
- implementation of the right to be forgotten article 17),
- implementation of the right to limit processing Article 18),

- implementation of the right to data transfer Article 20),
- exercise of the right to object article 21),
- implementation of the right not to be subject to automated decision-making, including profiling Article 22),
- implementation of the decision of the supervisory authority to temporarily or completely reduce processing, including the prohibition of processing Article 58. point 2 f).

Most of the above points come down to editing, deleting or marking data. The last option is particularly important in systems in which the same set of data is processed for different purposes. It should then be possible to indicate for which purpose the data may or may not be processed.

It is also important to make sure that data is not stored in the systems for longer period than required. Therefore, it should be possible to identify from when the data appears in the system and what processing period was specified for it. It is worth knowing that only in selected cases we have specific provisions that clearly specify the period of data storage and processing. For example, in the light of the Polish Labour Code, the employer is obliged to keep the employee's personal documentation for the entire period of employment and for 50 years from the day of termination of work. However, according to the Accounting Act, employee remuneration cards should be kept for a period of not less than 5 years. Both mentioned cases are explicitly included in the GDPR Article 5 1e)): "Personal data may be stored for a longer period if they are only processed for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, pursuant to art. 89 paragraph 1, provided that appropriate technical and organizational measures required by this Regulation are implemented to protect the rights and freedoms of data subjects."

In most situations, however, there are no specific provisions that specify the date of deletion. In that case, we should answer a simple but key question: do we still need it? For example, after completing the complaint procedure, the store should immediately delete customer’s data. Theoretically, the solution is simple, but in practice we deal with dozens of different consumers, and not with one client. There is therefore a problem of how to control the process of removing unnecessary data in order to avoid oversights. Each company should have a unified procedure. It is recommended to create a retention table, in which we will determine: the type of stored data, their location paper documents, placed on digital media such as USB, electronic documents) and expiration date regulated by these specific provisions or determined individually). It is also worth to indicate persons employees) responsible for regular deletion and review of data.

The last important functionality resulting from the right to data transfer is the ability to export them to a structured, commonly used machine-readable format. The standard will probably be XML and CSV.

2.2. Requirements for backup and archiving systems

The author mentioned earlier the necessity to verify the period of data processing in IT systems and the client's request to be forgotten. These two requirements may prove extremely difficult to meet if the deletion of data cannot be automated, but will be done manually. Administrators point out that an archival copy is often stored on an external medium, sometimes in an external location, and the use of cryptographic mechanisms does not make a task trivial to be implemented. At this point, however, two types of copies should be distinguished: backup not to be confused with technical backup) and archive.

The data controller can overwrite the backup data without any problem, i.e. replace them with newer ones. Backup is usually stored for 72 hours. The archive, however, consists of information that we keep for more than 3 months. The archive is an integral part of the system and one should not remove individual data, because it can lead to a disturbed operation of the whole system. Of course, it is possible to delete individual data records, but this requires: recovering the system from the backup, removing data of a specific person from them, or performing anonymisation or pseudonymisation and re-archiving data. These activities require additional resources, time and availability of the infrastructure used. In view of the above, it is recommended to regularly review unstructured data. In addition, it is worth setting a date for periodically deleting information from a particular category from the database. If the company does not have systems that allow for removal of data from archival copies, processes huge data sets and has complicated backup procedures, it seems necessary to make a decision concerning implementing new solutions. It is worth mentioning the functionality of efficient recovery, modification and re-archiving of data, as well as the necessity to perform additional activities for multi-level, incremental or differential backups.

2.3. Safety level requirements

An employer, being an entity processing personal data of employees, becomes the controller of these data, that is, the entity deciding about the purposes and means of processing personal data Article 7 point 4 of the Act). When processing personal data, the employer is obliged to apply the rules determined in the Act on personal data protection, which are used to process personal data in files, indexes, books, lists and other records and information systems, also when personal data are processed outside a set Article 2 1) of the Act). This provision applies to both personal data processed manually e.g. personal files of employees) and automatically in the computer systems).

The employer's primary duty as a data controller is to adequately safeguard the data being processed, i.e. the obligation to apply technical and organizational measures that ensure protection of the data processed, appropriate to the threats and categories of data to be protected. The security of personal data processing is described in Article 32. It comprises, among others, the following:

- anonymisation, pseudonymisation and encryption of personal data,
- the ability to continually ensure the confidentiality, integrity, availability and resilience of processing systems and services,
- the ability to quickly restore the accessibility of personal data and access to them in the event of a physical or technical incident,
- regular testing, measuring and evaluation of the effectiveness of technical and organizational measures to ensure the security of processing.

When determining the degree of security, particularly, the risks associated with accidental or illegal removal, loss, modification, unauthorized disclosure or access to personal data should be taken into account.

Moreover, the resolution emphasizes the requirement of accountability, that is verification of the level of security, in a significant way. The basic control and configuration activities that are recommended to be carried out are for sure:

- verification of firewall rules in terms of the possibility of obtaining unauthorized access to services,
- sealing outgoing communication to reduce data leakage,
- configuration of rules for monitoring and reporting calls initiated from internal and external networks,
- verification of the configuration of smtp/pop3/imap, FTP, WWW services for the transmission of credentials using unencrypted channels,
- implementation of solutions for automatic updates of the system and application software,
- implementing solutions for centralized authorization management,
- implementation of solutions for managing and monitoring remote sessions e.g. established by external service companies),
- implementation of backup systems allowing for automatic verification of tasks and reporting.

The lack of any of the above-mentioned activities may consequently lead to serious incidents related to the violation of the security of personal data. The above-mentioned requirements are unfortunately not easy to verify. Their fulfilment depends on many factors, including:

- applied technical solutions Wirth, and Kolain, 2018),
- the course of the processing of personal data Pandit at al., 2018),
- business environment and organization context Lindgren, 2016),
- values and quantities of data processed Preuveneers at al., 2016; Tikkinen-Piri at al., 2018).

Determining the risk requires a careful inventory of systems, learning how they work and interact with each other, learning methods of managing them and finally comparing them with a catalogue of possible threats and vulnerabilities. In order to finally assess the security of the systems, not only technical knowledge but also experience in the design and management of information systems is necessary Olkiewicz, 2016).

To protect both data stored in the system and the entire IT infrastructure, the necessary steps must be taken. First of all, one needs to secure access to both the network and the system itself by verifying access authentication, authorization, login) and the ability to check who, how, where and when viewed/downloaded/printed what data. It is worth noting here that storing data in the cloud does not guarantee the total security of their storage.

It is also necessary to introduce configuration changes in the system already used so that the default settings of the system are assigned personal data protection. If the type of personal data processing especially in connection with the use of new technologies) involves a high risk of violating the rights or freedoms of individuals, the data controller must assess the impact of these operations.

The system should also store all necessary information about the authorizations granted to access personal data provided by the controller of this data. The software should, therefore, store scans of relevant documents, a list of authorized persons, as well as the scope and time frame of the authorization, separately for each authorized person.

The generally applicable accountability principle in the context of having data access rights is understood as providing information on who entered, changed or deleted data. It does not include, for example, data browsing operations that the system user is authorized to process. In relation to medical documentation, the duty of accountability was also extended in the scope regarding access to information.

3. Software supporting production automation

Technological progress in the field of automation, including data processing which includes sound and image, allows for a broad interpretation and analysis of the development process. This mainly applies to the hybrid environment in which there is close cooperation between machine resources and human resources. The functionality of information systems supporting production processes, ensuring the participation of human resources in production events, uses the processing of personal data. An example of new applications for data processing is, among others:

- records of employees' working time,
- e-mail,
- monitoring the employee's activity at the workplace,
- data exchange with external entities.

3.1. Working time registration

Proper registration of employees' working time is the responsibility of the employer. The Labour Code does not impose a method of confirming attendance at work, it leaves the employer a lot of freedom in this area, but also introduces requirements. One of them is a strict prohibition of use of biometric data for the purposes of working time records. Technological progress makes methods based on the use of biometric data of employees Article 29) more popular, like in the case of image of the face, fingerprint, iris, retina, vascular system, voice or the shape of the pinna. These elements are characteristic for each person and enable their unambiguous identification. In order to record the progress of works, however, their use is forbidden. The employer cannot scan or retrieve biometric data of employees in order to register the time of entering and leaving the facility, even with the consent of such an employee. They may, however, use it in limiting access to places for which the employer requires special rights due to business secrets or a limited range of people with professional skills able to get to a protected area. Biometric data belong to the data of a particular category and can be processed only in situations listed in art. 22 European Parliament and Council, 2016).

3.2. Employee email monitoring

New technologies also allow the employer to use internal telecommunications resources to monitor employees. Nevertheless, one must remember that they have no right to violate the privacy of the employee in the workplace without a serious reason related to the nature of their work. An example of violations is eavesdropping on telephone conversations, tracking e-mail correspondence or checking shipments addressed to an employee. The employer's right to monitor the e-mail of employees only applies to business accounts. According to art. 22 3) of the Labour Code, the employer is entitled, if it is necessary, to ensure effective organization of work enabling full use of working time and the use of work tools provided to the employee Vojkovic, 2018). The employer cannot control the private correspondence of employees, it is even forbidden. Such behaviour would violate the constitutional right to privacy. Monitoring e-mail cannot violate the confidentiality of correspondence and other personal rights of an employee.

The employer can also control the activity of employees during their work by checking the websites they use, and which do not serve their duties or belong to sites prohibited by the employer. However, the control is to ensure that the employee is not overly burdened with work and uses the tools entrusted to them for professional purposes.

The employer is obliged to inform the employee about the use of devices monitoring their behaviour before the employee starts working or two weeks before starting the monitoring. The information should be provided to the employee in writing and contain the purpose, scope and method of monitoring and the rules for the collection and use of data. It must be reliable and transparent and available to the employee.

3.3. Monitoring employee activity at the workplace

Processing of personal data in production support systems is mainly used to increase the efficiency and effectiveness of the hybrid manufacturing operations. First of all, it concerns ensuring safe working conditions and allocating resources, that is, assigning an employee to a workplace in order to implement a designated technological operation at a specific time using the selected material.

It should be noted that the allocation of resources taking place in an autonomous manner requires prior definition of competency matrices. They may include physical predispositions, acquired qualifications or limitations of the employee's temporary availability, which regulate the performance of manufacturing activities. It should be noted that the standardization of the duration of technological operations, except for a small number of cases, does not directly refer to personal data, but indirectly regulates the issue of allocation. The competency matrix is one of the instruments supporting the management of human resources of an enterprise and can be a tool for planning the training needs of direct production employees as well as a tool used in scheduling production activities. As the competence matrices contain information describing the skills of each of the direct production employees, taking into account the tasks and organizational roles adopted at selected company workplaces, they are also useful in searching for solutions that take into account the boundary conditions of the manufacturing tasks and employees' substitutability.

In addition to the above-mentioned example of the use of scheduling algorithms in creating production schedules, identification of people as production resources also occurs when the work reports are completed, as well as the technical documentation is made available. Reports submitted by the employee may concern not only reporting of a discrepancies in the quality of the product or quantitative material, but also may be a signal indicating the end of the technological operation. They enable the recording of operating activities of direct production employees and analysis of their behaviour Milewska, and Gembalska-Kwiecień, 2018; Milewska, and Skowron, 2018a, 2018b; Skowron, and Milewska, 2018).

Translating the scope of the term of personal data processing into the niveau of production automation, it should be recognized that all activities undertaken as part of the process of identifying people as production resources, which have personal information as a subject, are qualified as personal data processing. The way of controlling employee activity is of fundamental importance to the presented problem. Technological progress caused a significant increase in the use of IIoT devices equipped with sensors that collect and process information from the environment. Despite the enormous opportunities offered by the digital economy, there is an evident need to guarantee employees effective protection of personal data. According to GDPR and the amendment to the Labour Code, which was introduced by the Act of 10 May 2018 on the protection of personal data Journal of Laws of 2018, item 1000) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych), in the field of monitoring employee activity

in the workplace, under certain conditions, devices that locate GPS, RFID and others are allowed to be used. The employer must remember that the purpose stated in the documentation must be the same as the purpose of using industrial automation devices and data obtained through them. It does not change the fact that the goals, scope and manner of registering process events and tracking the production activities of direct production workers must be set in the collective work arrangement or in the work regulations, or in a notice, if the employer is not covered by either of the two.

In addition, the biometric data of the employee are subject to particular control. Although unambiguous identification of people could accelerate implementation of manufacturing processes, overcome mistakes occurring in the registration of events and increase the efficiency of works due to the precise adaptation of the environment to the needs of the worker, processing of sensitive data is legally permissible only under certain conditions. Pursuant to the provisions of the Act, this is a permissible solution when it is necessary to fulfil the employer's obligation imposed by the law, or when providing sensitive data is necessary due to the control of access to particularly sensitive information, the disclosure of which may expose the employer to damage, or access to rooms requiring special protection. It is not required in this respect to obtain separate consent of the employee to process this data. Only persons who have a written authorization to process such data assigned by the employer will be allowed to process these personal data, and persons authorized to process personal data will be bound by secrecy. The provisions of the Act Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych) also apply to the monitoring of the workplace and adjacent areas. In connection with the arguments mentioned above, it seems obvious that there is a conflict between privacy and the efficiency of production processes in the digital work environment.

3.4. Providing employee data to external entities

During the employment period, the employer is often forced to disclose employees' data to other business entities in order to perform the tasks entrusted to them or in connection with the services offered to the employer or employees. In this situation, the external company must enter into an agreement with the employer to entrust the processing of personal data. The scope of personal data provided by the employer should be limited and closely related to the subject of service provided by the entity. It must therefore be necessary to render given service. It should be emphasized that if the data provided include the specific categories of data referred to in Article 9 par. 1 GDPR it is necessary to obtain a separate employee's consent Article 9 paragraph 2 point and GDPR). The situation described above concerns the transfer of execution documentation by subcontractors in the form of certificates or declarations containing, for example, contractor IDs of individual manufacturing activities. They are often necessary to certify the performance of warranty, service or repair services that are undertaken by authorized service points throughout the entire life cycle of the product.

4. Summary

In practice, organizations that process personal data are required to implement two types of protection: organizational and technical. Ensuring the security of data in the IT system, in addition to user authorisation to resources, means also protection against accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data sent, stored or otherwise processed. In addition, in a situation where it is necessary, the implementation of appropriate data protection policies should be considered.

When making decisions about the application of certain security measures, it is necessary to take into account the value of the data and the effects that the infringement may cause, i.e. unauthorized disclosure, modification, unavailability or loss. An example would be the risk of losing continuity of access to data.

Acknowledgements

This article was created as part of statutory work 13/010/BK_19/0034 conducted at the Institute of Economics and Informatics at the Faculty of Organisation and Management of the Silesian University of Technology.

References

1. Cornock, M. 2018). General Data Protection Regulation GDPR) and implications for research. *Maturitas, 111*, pp. A1-A2. doi: 10.1016/j.maturitas.2018.01.017.
2. European Parliament and Council, *General Data Protection Regulation, EU) 2016/679* 2016). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32-016R0679, November 21, 2018.
3. European Parliament and of the Council 2017). *Data Protection Directive Directive 95/46/EC)*. Retrieved from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%-3A31995L0046, December 21, 2018.
4. Gilchrist, A. 2016). *Industry 4.0: The Industrial Internet of Things*. Berkely, CA: Apress.
5. Kościuk, D. 2018). General Data Protection Regulation GDPR) – The EU Law Strengthening the Information Society in Poland. *Białostockie Studia Prawnicze, 2 23)*, pp. 139-148. doi: 10.15290/bsp.2018.23.02.10.

6. Lindgren, P. 2016). GDPR Regulation Impact on Different Business Models and Businesses. *Journal of Multi Business Model Innovation and Technology, 4 3)*, pp. 241-254, doi: 10.13052/jmbmit2245-456X.434.
7. Milewska, E. 2011a). Wykorzystanie narzędzi informatycznych w procesie sterowania strumieniem przepływu materiałowego. *Mechanik, 7 84),* CD. pp. 575-582.
8. Milewska, E. 2011b). Zintegrowane systemy informatyczne wspomagające zarządzanie zdolnościami produkcyjnymi. *Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedzą, 40,* pp. 263-271.
9. Milewska, E. 2014a). Aspekty techniczne i organizacyjne wdrożenia systemu informatycznego wspomagającego planowanie produkcji. *Systemy Wspomagania w Inżynierii Produkcji, 2 8)/2014/13,* pp. 142-152.
10. Milewska, E. 2014b). Wykorzystanie wiedzy technologicznej w procesie sterowania przepływem produkcji. In: R. Knosala ed.), *Innowacje w zarządzaniu i inżynierii produkcji. T. 1* (pp. 604-613). Opole: Oficyna Wydaw. Polskiego Towarzystwa Zarządzania Produkcją.
11. Milewska, E. (2016). Wdrożenie hybrydowej metody sterowania produkcją dyskretną. In: R. Knosala (ed.), *Innowacje w zarządzaniu i inżynierii produkcji. T. 1* (pp. 759-767). Opole: Oficyna Wydaw. Polskiego Towarzystwa Zarządzania Produkcją.
12. Milewska, E. (2017a). IT systems supporting the management of production capacity introduction. *Management Systems in Production Engineering, 1(25),* pp 60-67, doi: 10.1515/mspe-2017-0009.
13. Milewska, E. (2017b). Zdolność adaptacyjna przedsiębiorstw produkcyjnych. *Systemy Wspomagania w Inżynierii Produkcji, 6(6)*, pp. 159-166.
14. Milewska, E., and Gembalska-Kwiecień, A. (2018). *Selected aspects of human resources management based on competence matrix.* 5th International Multidisciplinary Scientific Conference on Social Sciences and Arts. SGEM 2018 Conference proceedings. Book 1, Vol. 5, pp. 861-866, doi: 10.5593/sgemsocial2018/1.5/S05.107.
15. Milewska, E., and Skowron, B. (2018a). Use of IT technologies in the calculation of the technological production cost conducted – a case study. In: A. Albrychiewicz-Słocińska, A. Czarnecka, A. Dunay (Eds.), *Challenges of management in modern organizations* (pp. 188-196). Gödöllő.
16. Milewska, E., and Skowron, B. (2018b). *Use of IT technologies in the management of production process quality*. MATEC Web of Conferences, 183, 03012 2018, doi: 10.1051/matecconf/201818303012.
17. Olkiewicz, M. (2016). System zarządzania determinantą bezpieczeństwa informacji w działalności gospodarczej. *Studia nad Bezpieczeństwem, 1*, pp. 85-112.
18. Pandit, H.J., O'Sullivan, D., and Lewis, D. (2018). *GDPR Data Interoperability Model*, 23rd EURAS Annual Standardisation Conference, Dublin, Ireland. http://purl.org/ADAPT/pub/E18EURAS.

19. Preuveneers, D., Joosen, W., and Ilie-Zudor, E. (2016). *Data Protection Compliance Regulations and Implications for Smart Factories of the Future*. 12th International Conference on Intelligent Environments IE, London, pp. 40-47. doi: 10.1109/IE.2016.15.
20. Skowron, B., and Milewska, E. (2018). *Use of IT technologies in the management of production process quality – a case study.* Book of proceedings – ICoM 2018. F. Bylok, A. Albrychiewicz-Słocińska, L. Cichobłaziński, p. 575-579.
21. Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34(1)*, pp. 134-153, doi: 10.1016/j.clsr.2017.05.015.
22. Ustawa z dnia 26 czerwca 1974 r. *Kodeks pracy.* Dz.U. 1974, Nr 24, poz. 141 z póz. zm.).
23. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. z 2016 r., poz. 922).
24. Vojkovic, G. (2018). *Will the GDPR slow down development of smart cities?* 41st International Convention on Information and Communication Technology, Electronics and Microelectronics MIPRO, Opatija, pp. 1295-1297. doi: 10.23919/MIPRO.2018. 8400234.
25. Wirth, C., Kolain, M. (2018). *Privacy by blockchain design: a blockchainenabled GDPR-compliant approach for handling personal data*. Reports of the European Society for Socially Embedded Technologies, 2(6), doi: 10.18420/blockchain2018_03.
26. Wurm, J., Hoang, K., Arias, O., Sadeghi, A.R., and Jin, Y. (2016). *Security analysis on consumer and industrial IoT devices*. 21st Asia and South Pacific Design Automation Conference ASP-DAC, Macau, pp. 519-524. doi: 10.1109/ASPDAC.2016.7428064.