doi: 10.36689/uhk/hed/2020-01-090

Implementation of GDPR into Payroll Accounting in the Czech Republic

Jitka ŠIŠKOVÁ and Enikő LŐRINCZOVÁ *

Czech University of Life Sciences, Prague, Czech Republic, siskova@pef.czu.cz; lorinczova@pef.czu.cz
* Correspondence: lorinczova@pef.czu.cz

Abstract: The General Data Protection Regulation (GDPR) 2016/679 which came into effect on 25 May 2018 is a regulation in EU law on data protection and privacy for natural persons - individual citizens. Payroll accounting is one of the most affected by the GDPR as it handles personal information and focuses on the exchange of personal data between employees, employers and authorities like the tax office and the social security and health insurance institutions. Methods for compiling this paper include a desk research and a case study of GDPR implementation into a payroll accounting in a small company in the Czech Republic. The results show that the main obstacles in the implementation of GDPR are related to the physical and personal security of data protection.

Keywords: GDPR; payroll accounting; employees, wages, data protection

JEL Classification: M14; M48; M41

1. Introduction

The General Data Protection Regulation (GDPR) 2016/679 is a regulation of the European Parliament and of the council of European Union on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This regulation is applicable in all EU member states from 25 May 2018 and replaces the previous Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. Rapid technological developments and globalization have brought new challenges for the protection of personal data. As (Rindașu 2017) states, the technological progress brings obvious benefits for the companies and the development of the accounting profession, helping to reduce the costs by increasing the productivity level and enhancing process automation. Personal data protection and new technologies has a common challenge: the security of sensitive data.. According to the GDPR regulation, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". There are some special categories of personal data ('sensitive data') which should not be processed (Article 9, GDPR 2016/679), such as racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Processing data means any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR 2016/679). Data processing is constantly under threat due to a number of challenges, such as the accelerating change of technology, open networks, third-party dependencies, stakeholder involvement and government requirements for stricter regulation through compliance and policies (Chatzipoulidis et al. 2019). A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. (Article 9, GDPR 2016/679).

Processing data is supposed to be lawful for example only if and to the extent that the data subject (the person) has given consent to the processing of his or her personal data, or processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (GDPR 2016/679). Employees are data subjects where data processing is necessary due to statutory requirements regarding their employment contract and to liabilities to the tax office and other authorities, like the Czech Social Security Administration. The GDPR regulation offers the member states a more individual approach as to the employees´ data, in their Article 88 which says that the EU member states may provide more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's property and for the purposes of the exercise and enjoyment of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

In the Czech Republic, Act No. 110/2019 Coll. on personal data processing is the implementation of the EU new legal framework of GDPR. Both GDPR 2016/679 and Act No. 110/2019 adapt to a modern need of data protection to ensure they are effective. (The Czech Office for personal data protection 2019)

2. Methodology

The methods for compiling this paper include a desk research and a case study of GDPR implementation into a payroll accounting in a small company in the Czech Republic. The desk research focused on the legal framework related to GDPR (GDPR 2016/679) and on the data required for calculating the wages in the Czech Republic (mainly related to the calculation of the personal income tax of the employees, determined by the Czech Income Tax Act No 586/1992 as amended up to date). Data for the case study were collected in 2018 by a third party (a student who works there).

3. Results

Every data processor (company) needs to have a legitimate reason as to why they hold an individual's personal details. Data processors can hold employee´s payroll information to complete the payroll (see Table 1), such as the employee´s date of birth. Under the GDPR legislation, this is classified as a valid and legitimate reason to hold a personal data. To understand what type of information is needed to calculate the wages to be paid and the mandatory deductions, it is necessary to know how the wages are calculated in a specific country (see chapter 3.1).

3.1. Personal data required in payroll accounting in the Czech Republic

In the Czech Republic, wages to be paid are calculated as gross wages (recorded wages as a liability to employees based on their performance or fixed base, plus bonuses and/or personal supplements) minus the mandatory deductions (like income tax and social and health insurance contributions) minus individual personal deductions (regarding child support, court-ordered deductions in case of seizures, savings, etc.). The determination of the gross wages are based on records of personal performance and in some cases also on the previous work-related qualifications. The evidence of these personal data is necessary to determine the gross wages. Other personal information is needed to calculate the income tax. In the Czech Republic, the tax base for the personal income tax is calculated as super gross wages (gross wages before any deductions plus 34% of these gross wages, rounded up to full 100 CZK (in case of calculating the monthly advance payments of income tax) to get the tax base. This tax base is then multiplied by 15% (personal income tax rate in the Czech Republic). The calculated income tax amount can be reduced by various tax credits such as the

Table 1. Categories of necessary information of employees for data processing.

Category	Personal data included
Data needed from the employee based on the requirements of the Czech Labour Law No 262/2006 Coll.	Data about the identification of the employee, data about the employee´s work attendance record, data necessary to calculate the income tax, sick-leave, pension contributions, health insurance, contributions to a social care, data necessary for payroll accounting
Data needed for the fulfilment of the employment contract	Contact information, bank account identification, data about work performance, records about absence in the work place including the reasons, other information necessary for calculating the wages and compensations and the payment to the employee´s account
Legitimate interest of the employer due to administrative and operating needs	The use of cameras, GPD tracking of employees´ cars, the use of photos of employees

personal income tax credit (applicable in general for all employees) and other tax credits where additional personal information is necessary. These other tax credits are related to the disability credit (there is a need for medical evidence as to the level of disability), students tax credit (there is a need for confirmation from the school the employee attends), children´s tax credit (there is a need of further information about the children as to their date of birth and personal identification number). The annual tax refund settlings of employees with the tax office include a need for additional personal information, if the employee wants to apply the tax levies available. This information (which can reduce the employees´ annual tax base according to the Czech Income Tax Act and result in refunds) include a necessary evidence about the interest paid of their mortgage (up to 300 000 CZK for a year for a household – note: only the interest paid can be included in the decrease of the tax base, not the total mortgage payments), gifts given for public purposes (the most common public gift is a blood donation, it can reduce the annual personal tax base by 3000 CZK per donation. Other possible reductions of the annual personal tax base include payments of individual life insurance and individual pension contributions. All these deductions has to be evidenced (by providing contracts or confirmations by other parties) and has to be given to the payroll accountant to apply these deductions in the employee´s annual income tax settlement. Other personal data required for tax purposes in the annual tax settlement is the information about the co-habiting spouse with no income (in the Czech Republic the upper limit is an income of 68 000 CZK per year to be considered as a co-habiting spouse with no income – usually spouses who stay at home to provide care for the children). (Czech Income Tax Act No 586/1992 as amended). Table 2 and Table 3 shows examples of personal data necessary for HR purposes and general payroll accounting.

Table 2. Examples of necessary personal information of employees for various purposes.

Categories	Include	Examples of personal data
Data necessary for HR purposes, general payroll accounting, and identification	CV, documents proving education, information necessary for social contributions and health insurance evidence, data required by the national employment office, by the Foreign Police or by other governmental offices	Name, titles, date of birth, bank account, personal identification number

Data related to health condition	Pre-recruitment medical exams to determine if an employee is physically fit to perform his/her work duties, data related to sick-leave, data related to disability	Results of medical exams (in some cases without specification, in some cases with specification)
Data necessary for tax reliefs	Evidence of contracts and payments	Details of life insurance payments, pension contribution payments, savings, interest payments on mortgage, evidence of disability, evidence of gifts given to public (blood donors)

3.2. The implementation process of GDPR

The implementation process of GDPR usually includes:

1. a data protection audit,
2. preparation of the implementation plan,
3. implementation of GDPR and
4. regular check-ups.

The first step of the implementation process of GDPR is a data protection audit. The audit will assess the risk of non-compliance with data protection legislation and highlight any areas of risk to their compliance. (ICO 2018). A data protection audit may identify weaknesses regarding the company's handling of personal data. The data audit of employees includes several steps, such as setting the scope areas and criteria of the audit, review of stored personal data available, analysis of compliance with GDPR, identifying the risk areas and proposing adjustments to achieve compliance with the GDPR regulation.

The implementation plan of GDPR includes a revision of internal processes ensuring the security of personal data, the decisions of whether a company needs a data protection officer, preparation of documentation for the Records of processing activities , plan of risk solutions related to GDPR and staff training. The most important part is the documentation of Records of processing activities (Vodička and Drábková 2019).

Table 3. Information necessary for wages calculation in the Czech Republic.

Wages to be paid and deductions	Mandatory and voluntary deductions	Information needed
Gross wages	Base of calculation	Work attendance sheet, evidence of absences and holidays, performance evaluation data, previous education and work experience data
Social and health insurance contribution	Mandatory deduction of 11 % of gross wages (6,5 % for social contribution, 4,5 % for health insurance)	Evidence of personal tax reliefs applied either monthly or annually (medical proof of disability, date of birth of children, confirmation of school, dependent spouse´s information, interest on mortgage payments, payments of individual life insurance or pension, public gifts confirmation (blood donation), etc.

Personal income tax	Mandatory deduction of 15 % income tax rate of the tax base (tax base equals to gross wages plus 34% of gross wages) after tax credits	Contracts and bank account specifics, proof of payments
Other deductions from wages	Mandatory or voluntary deductions (alimonies, child support and other court-ordered deductions, voluntary savings, contributions to individual life insurances, payments of mortgages	

[1] Own processing based on the Czech legal requirements

The implementation of European data protection is a challenge for businesses and has imposed legal, technical and organizational changes for companies. (Poritskiy et al. 2019)

The implementation of GDPR requires an implementation of technical and operating measures ensuring data protection and preventing unauthorized access includes (based on Vodička and Drábková 2019):

1. Physical security of data protection – data in printed or written form includes hard copies of electronic documents, hand written documents or notes, access to workspaces, printers, fax machines and trash receptacles.
2. IT security of data protection – include data encryption, complex passwords, technical security and monitoring measures like the history of data changes in files (time and the user), data backup.
3. Personal security of data protection – include the access authorization of employees to the file system and removing the access to an account when employees leave the company.

3.3. . Case study of implementing the GDPR into the payroll accounting

The company is a small manufacturing limited liability company, a legal entity registered in the Czech Commercial Register for entrepreneurs. The company has around 40 employees. It uses the Czech economic software Pohoda for processing necessary general and payroll accounting. Personal data are saved in this economic software and in a form of physical (hard-copy) personal employee records.

Table 4. Examples of personal data processed by the payroll accountant.

User of personal data	Purpose of processing	Examples of personal data processed
Payroll accountant	Calculation of wages, social and health insurance contributions, income tax calculation	Name of the employees (first name, family name), date of birth, personal identification number, address, data about ability to work, work performance and attendance sheets, data about the health insurance company, phone number, email, bank account number, data about children and spouses (including their date of birth and personal identification number), disability claims medical records

[1] Own processing based on the company´s information

Table 3 shows the necessary information which is generally required in the Czech Republic for calculating the wages. Table 4 shows examples of the extent of personal data the payroll accountant has to use for fulfilling the statutory requirements. The personal data audit focused on the type of data stored, the necessity of these data, the physical, IT and personal security of data protection. Examples of non-compliance with GDPR in some areas are shown in Table 5.

Physical security of the employees´ hard-copy records was not ensured sufficiently. Unauthorized access was possible, as the records were stored in open shelfs albeit in an office which could be locked. The company invested in new filing cabinets which can be locked.

IT security of data protection – the company uses a very common Czech economic software. The supplier of this software gave free updates of the software to increase the compliance with GDPR. This update included a new feature in the Directory (Personal address book), which focus on the „Description of personal data" where all the information about the employees is stored and is ready to print it out and provide it to the employee (as one of the requirements of GDPR is to provide employees with the summary of their personal data if they wish so). Another sub feature of the updated Directory is the possibility to assign for every personal information the legal reason why it is stored (like for tax purposes). There is a feature enabling to manage and change the access rights to specific information or databases.

The company can send official documents to the data box of the authorities or to the application of financial administration (tax purposes) and the Czech Social Security Administration directly from this software. This helps the company to ensure the security of electronic submission of data to the authorities, which is possible to invoke through the command under the menu for the declaration, respectively overview. Data sent by electronic submission is encrypted and provided with an electronic signature. There is also a possibility of upgrade offered by the software supplier to a more advanced version of the economic software, but it was rejected by the company as not necessary.

Table 5. Issues related to the Implementation of GDPR in the company.

Criteria	Assessment	Reasons/Remedy
Designation of a data protection officer	No necessary impact assessment	no **high** risk of unauthorised interference with the rights and freedoms of the data subject
	Not necessary	the processing is not carried out by a public authority (the company is not a public authority), there is no need for a constant monitoring of data subjects, no special categories of personal data
Personal data stored	Copies of identity cards (IDs) and health insurance cards and, former job applicants CVs found	necessity to dispose of these documents
Physical security of data protection	Hard-copy employee records filed in a book-shelf	Filing cabinet for the records with a lock
Personal security of data protection	Access to most files in the economic software by various employees	Authorizations for access
IT security of data protection	Encrypted data, complex passwords	Sufficient

Special categories of personal data	No special categories of personal data	Only health related non-specific documents (as an evidence for tax reliefs for disability)

Personal security of data protection was not sufficient enough as the access to information was not strictly determined. All database systems are now password protected and access is terminated to people with a legitimate reason for doing so. All user names must have a password which has to be changed reasonable frequently and also to have a level of complexity. The document „Records of processing activities" were created where it was determined in a written form what is the purpose of data processing (like employees data for internal administration and labour law related content), who is the data subject (employees), categories of personal data (like information related to the fulfilment of work contract), duration of processing (how long these personal data are available for processing), etc.

Expenses related to the implementation of GDPR in the company (economic impact) were around 45 000 CZK (around 1 800 €, if 1 € = 25 CZK). Most of the expenses were related to the overtime wages of the accountants (the accountant of the company spent approximately 15 hours and the payroll accountant around 28 hours with the preparation of the implementation of GDPR). Other expenses were related to the purchase of the filing cabinets with a lock, staff training, IT consultations, lawyer consultations, website alteration and literature.

4. Discussion

The positive points about the GDPR regulation are that employees have greater rights to be informed about how long their information will be stored and how it will be used. Employees can also request access to the personal information that is held on them and they can request to have it rectified and in some cases where there are no compelling reasons to retain the data, they can request for it to be deleted (erasure).

Employees now

have the right to increased transparency to ensure their data is being managed correctly. As (Poritskiy et al. 2019) states, the main benefits identified by the application of European data protection include increased confidence and legal clarification.

In the case study, the SME company relied on the economic software provider to update the software they use for the compliance with GDPR to ensure IT security of data protection. Even if the software provider offers updates, data protection depends also on the human factor as IT security is only one part of the technical and organizational measures a company has to take. This issue is pointed out for example in the findings of (Kapoor et al. 2018), where research showed an over-emphasis on technical measures.

A company can recruit an external firm to provide the GDPR implementation, but even though it may appear as cheaper, it is not always the best way as the external firm cannot provide sufficiently the necessary internal data audit.

5. Conclusions

GDPR requires an implementation of technical and operating measures ensuring data protection and preventing unauthorized access. Physical, IT and personal security of data protection has to be implemented. In payroll accounting, a large amount of personal data need to be processed due to statutory requirements regarding information for the calculation of wages and mandatory deductions from wages such as the income tax and the social and health insurance. Physical records of the employees has to be stored in a safe place with a lock and limited access. Internal data audit has to ensure that a company does not have any personal data which is not necessary or not legal, i.e. copies of identity cards or health insurance cards or personal data of former employees.

References

Chatzipoulidis Aristeidis, Kargidis Theodoros, Tsiakis Theodosios. 2019. A readiness assessment tool for GDPR compliance certification. *Computer Fraud & Security*: Vol. 2019, Issue 8, 14-19. https://doi.org/10.1016/S1361-3723(19)30086-7

Council of the European Union. 2016. General Data Protection Regulation (GDPR) 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. Official Journal of the European Union L 119/1.

Czech Income Tax Act No 586/1992, as amended (Zákon o daních z příjmů). Available online: https://www.zakonyprolidi.cz/cs/1992-586 (accessed on 3 January 2020)

Information Commissioner´s Office ICO.2018. A guide to ICO audits. Available online : https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf (accessed on 4 January 2020)

Kapoor Keshav, Renaud Karen, Archibald Jacqueline (2018). Preparing for GDPR: helping EU SMEs to manage data breaches. Paper presented at the Symposium on Digital Behaviour Interventions for Cyber Security, April 5, pp. 13-20. Available online: http://aisb2018.csc.liv.ac.uk/PROCEEDINGS%20AISB2018/Digital%20Behaviour%20Interventions%20for%20CyberSecurity%20-%20AISB2018.pdf (accessed on 3 January 2020)

Poritskiy Nazar, Oliveira Flávio, Almeida Fernando. 2019. The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*: Vol. 21, No 5, 510-524. https://doi.org/10.1108/DPRG-05-2019-0039

Rîndașua Sînziana-Maria. 2017. Emerging information technologies in accounting and related security risks –what is the impact on the Romanian accounting profession. Accounting and Management Information Systems: Vol. 16, No. 4, 581-609. http://dx.doi.org/10.24818/jamis.2017.04008

The Office for Personal Data Protection (Úřad pro ochranu osobních údajů), available online: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1001&p1=1001 (accessed on 3 January 2020)

Vodička Milan, Drábková Tereza. 2019. GDPR Praktický průvodce pro účetní. Metodické aktuality Svazu úèetních: 7/2019. 4-51. ISBN 978-80-87367-99-5