NEW APPROACHES TO THE PROTECTION OF PERSONAL DATA IN TRANSPORT SERVICES

Margita Majerčáková[1], Peter Jucha[2]

Abstract: In order to protect the rights and freedoms of individuals in the processing of personal data, each company had to take technical and organizational measures as of 25 May 2018 to meet the legislative requirements on the protection of personal data. This obligation also applies to transport services undertakings. At the same time, the company must regularly assess the security of the processing from the point of view of the nature of the processed personal data after the implementation of the measures. The periodic assessment should also ensure that the personal data processing undertaking in company is able to demonstrate that it has taken all reasonable and effective technical measures necessary in view of the nature, scale and purpose of the processing of the personal data it processes as well as the risks to rights and freedom of data subjects.

Keywords: Privacy, GDPR, Personal Data Act, processing of personal data

1. Introduction

Privacy is a frequently discussed topic at present. The privacy is addressed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / ES (General Data Protection Regulation) [1], Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or movement of such data and repealing Council Framework Decision 2008/977 / JHA [2] and Act 18/2018 Coll. on the protection of personal data and on amendments to certain acts [3].

The Regulation, the Directive as well as the Personal Data Protection Act impose an obligation on both the controller and the intermediary to take action in the light of the latest knowledge that each undertaking should monitor with developments in possible technical and security measures. Depending on the nature, extent and purpose of the processing of personal data as well as the potential risks, the company must decide on appropriate measures (e.g. more effective antivirus programs, firewall, employee training, etc.).

[1] doc. Dr. Ing. Margita Majerčáková, University of Zilina, Faculty of Operation and Economics of Transport and Communications, Department of Communications, Univerzitna 8215/1, 01026 Zilina, Slovakia
e-mail: margita.majercakova@fpedas.uniza.sk
[2] Ing. Peter Jucha, University of Zilina, Faculty of Operation and Economics of Transport and Communications, Department of Communications, Univerzitna 8215/1, 01026 Zilina, Slovakia
e-mail: peter.jucha@fpedas.uniza.sk

2. GDPR Regulation

The Regulation lays down rules on the protection of individuals with regard to the processing of personal data and rules on the free movement of personal data. The Regulation protects the fundamental rights and freedoms of individuals. The free movement of personal data within the EU cannot be restricted or prohibited, while preserving their protection.

The GDPR Regulation (as well as the law in Slovakia) obliges both operators and intermediaries to keep records of processing activities, a sample of which was also published by the Office for Personal Data Protection of the Slovak Republic itself on its website [4]. This document needs to be constantly updated and brought into line with the actual processing operations in the particular enterprise, which the operator respective intermediary performed. It should not be forgotten that in addition to processing activities aimed at clients or business partners, companies also process the personal data of their employees.

GDPR concerns anyone who collects and processes the personal data of Europeans, including companies and institutions outside the EU, which operate in our market. The regulation is applicable to companies, institutions, individuals - employees, customers, clients and suppliers across all sectors. It also applies to those who analyze the behavior of users of websites and applications [5].

The most important obligations for an enterprise with the validity of the GDPR Regulation:

- the appointment of a responsible person in cases provided for in the new legislation,
- processing of relevant documentation according to the new legislation,
- change of approval to the processing of personal data according to the new legislation.

3. Data Protection Act

Valid act No. 18/2018 on the protection of personal data defines several principles of personal data processing [3]:

- *Principle of legality*
  Personal data can only be processed lawfully and in a way that does not violate the data subject's fundamental rights.
- *Principle of purpose limitation*
  Personal data may only be collected for a specific, explicit and legitimate purpose and may not be further processed in a way incompatible with that purpose; further processing of personal data for archiving purposes, for scientific purposes, for historical research purposes or for statistical purposes, if it complies with a special regulation.
- *Principle of minimizing personal data*
  The processed personal data must be appropriate, relevant and limited to the extent necessary for the purpose for which they are processed.
- *Principle of accuracy*
  The processed personal data must be correct and updated as necessary; appropriate and effective measures must be taken to ensure that personal data which are inaccurate for the purposes for which they are processed are deleted or corrected without undue delay.
- *Principle of minimization of retention*
  Personal data must be stored in a form which allows the data subject to be identified at the latest until it is necessary for the purpose for which the personal data are processed; personal data may be kept for a longer period if they are to be processed solely for archiving purpose, scientific purpose, historical research or statistical

purpose on the basis of a specific regulation and if appropriate safeguards for the protection of the data subject's rights are respected.

- *Principle of integrity and confidentiality*
  Personal data must be processed in a manner that, through appropriate technical and organizational measures, ensures appropriate security of personal data, including protection against unauthorized processing of personal data, unlawful processing of personal data, accidental loss of personal data, deletion of personal data or damage to personal data.
- *Principle of responsibility*
  The controller is responsible for adherence to the basic principles of processing of personal data, for compliance of the processing of personal data with the principles of processing of personal data and is obliged to prove this compliance with the principles of processing of personal data at the Office's request.

The processing of personal data of enterprise that provides transport services may be [3]:

- **Lawful**, if carried out base of at least one of these legal basis:
  - The data subject has approval to the processing of his personal data for at least one specific purpose.
  - The processing of personal data is necessary for the performance of the contract to which the data subject is a part or to take action before the contract is concluded at the request of the data subject.
  - The processing of personal data is necessary under a special regulation or an international agreement by which the Slovak Republic is bound.
  - The processing of personal data is necessary to protect the life, health or property of the data subject or of another individual.
  - The processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of public authority entrusted to the operator.
  - The processing of personal data is necessary for the purposes of the legitimate interests of the operator or of a third party, unless those interests are outweighed by the interests or rights of the data subject requiring the protection of personal data, in particular where the data subject is a child; this legal basis shall not apply to the processing of personal data by public authorities in the performance of their tasks.
- **By approval** to the processing of personal data [3]:
  - If the processing of personal data is based on the approval of the data subject, the operator shall at any time be able to demonstrate that the data subject has given his approval to the processing of his personal data.
  - If the operator applies for the approval of the data subject to the processing of his personal data, this approval must be distinguished from other facts and must be expressed in a clear and comprehensible and easily accessible form.
  - The data subject has the right to withdraw the approval to the processing of personal data which concerning him or her at any time. Revocation of approval shall not affect the lawfulness of the processing of personal data based on approval prior to its withdrawal; the person concerned must be informed of this fact before giving his or her approval. The data subject may withdraw the approval in the same manner as the approval.
  - When assessing whether approval has been given freely, account shall be taken in particular of whether the performance of the contract, including the

provision of the service, is subject to the approval to the processing of personal data which is not necessary for the performance of the contract.

4. Obligations arising from the processing of personal data in an enterprise providing transport services

The enterprise is mandatory:

- Keep records of processing activities
- Establish appropriate technical and organizational measures
- Conclude mediatory contracts
- Elaborate joint operator agreements
- Elaborate an impact assessment
- Register a responsible person if the type of personal data processing so requires

If the data subject provides personal data by consent, the enterprise must comply with the following:

- providing of personal data must be voluntary,
- providing of personal data cannot be a condition.

At the same time the individuals have the right:

- to access to personal data,
- to correct inaccurate or false personal data,
- the right to request clarification if personal data is suspected of processing privacy, or if personal data are being processed in violation of law,
- the right to demand remedy of a situation that is contrary to legal regulations, in particular by stopping the handling, correction, supplementing or deletion of personal data,
- the right to the deletion of personal data if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed, or where it has been established that they have been processed unlawfully,
- the right to limit the processing of personal data,
- the right to data portability,
- the right to object after which the processing of personal data will be terminated unless it is established that there are serious legitimate reasons for the processing that outweigh the interests or rights or freedoms of the data subjects, in particular if it is possible to enforce legal claims.

These obligations apply to companies providing transport services within the Slovak Republic. Special agreements have been concluded for flows of personal data to third countries outside the EU. These agreements concern two types of data transfer, namely Passenger Name Record and Financial Reporting Data.

When booking tickets, airlines collect personal passenger records (data: name, address, credit card and seat number). Under US law, airlines are required to make this data available to the Department of Homeland Security before the aircraft is departed. This provision applies to flights to and from the United States. The first EU-US data sharing and management agreement was signed in 2012, its shortcomings being replaced by a new agreement in the same year. An updated agreement on the processing and transfer of EU Passenger Name Record (PNR) data between EU and Australia was also concluded in December 2011. An EU-Canada agreement was concluded in 2006.

On 21 April 2016, the EU Council accepted a Directive on the use of Passenger Name Record (PNR) data for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime. The Directive aims to regulate the provision by Member States of PNR data relating to passengers on international routes and the processing of such data by the competent authorities. The Directive provides that PNR data collected may only be processed for the purpose of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime [6].

Under the new Directive, air carriers will be obliged to provide PNR data to Member States authorities on flights to or from the EU. Member States will also have the possibility, but not the obligation, to collect PNR data for selected flights within the EU.

5. Conclusion

The legislation itself lays down obligations to undertake regular testing, assessment and evaluation of their effectiveness in taking appropriate technical and organizational measures. The audit of personal data processed helps to verify the correct processing of personal data. However, there are still mistakes made by entrepreneurs who underestimate this area and do not pay enough attention to it.

References

[1] NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) Available online: *https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32016R0679*

[2] SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVVJ Available online: *https://eur-lex.europa.eu/legal-content/sk/TXT/?uri=CELEX:32016L0680*

[3] Zákon z 29. novembra 2017 - 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov Available online: *https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20180525*

[4] Vzor Záznamov o spracovateľských činnostiach, Úrad na ochranu osobných údajov Slovenskej republiky Available online: *https://dataprotection.gov.sk/uoou/sk/content/vzor-zaznamov-o-spracovatelskych-cinnostiach*

[5] Čo je GDPR, GDPR-SLOVENSKO.SK, Available online: *https://gdpr-slovensko.sk/co-je-gdpr/*

[6] Smernica EÚ o záznamoch o cestujúcich (PNR) Available online: https://www.consilium.europa.eu/sk/press/press-releases/2016/04/21/council-adopts-eu-pnr-directive/

Grant support

VEGA 1/0152/18 Business models and platforms in digital space