Identification Systems and Their Legitimacy in the New Legislation on the Protection of Personal Data

Vlastimil Benes, Karel Neuwirt, and Otto Dostal

***Abstract*—In the new digital environment, citizens have the right to use tools to effectively control the usage of personal information related to them. Data protection is one of the fundamental rights in the EU guaranteed by the Charter of Fundamental Rights of the European Union. The article deals with the requirements that electronic identification system operators will have to take into account to ensure that the system in operation meets the requirements for the protection of personal data.**

***Keywords*—GDPR, identification systems, legal framework, personal data.**

I. Introduction

Existing EU legislation (in particular Directive 95/46/EC on the Protection of Personal Data and Directive 2002/58/EC on Privacy in Electronic Communications) is no longer able to effectively protect the privacy of individuals in connection with the challenges posed by globalization and new technologies. The conditions for the protection of personal data during their collection, use, access, or any other processing, need to be changed. The new EU legislation, the General Data Protection Regulation (GDPR, hereinafter "General Regulation") [1], valid from 25 May 2016, will come into force on 25 May 2018. Before it comes into force, all controllers and processors of personal data must update their existing systems for processing of personal data, and prepare any new ones, so they will comply with the Regulation from May 2018. The new legal framework must be implemented by all legal entities that deal with personal information about individuals and often misinterpret the impact of privacy laws on their activities.

This article cannot describe all of the obligations that electronic identification system [5] operators will have to take into account to ensure that their systems comply with General Regulation requirements. Therefore, we will particularly focus on one of the frequent problems that the operators of systems dealing with personal data (and therefore also of identification systems) are often clueless about: namely, to determine the legitimate basis for processing. As is already known from current data protection legislation, one of the possible reasons for legitimate data processing is the "legitimate interest of the data controller" [4] [in Directive 95/46/EC this is stated in article 7 letter f) and in Act No. 101/2000 Coll. On the protection of personal data it is referred to as "protection of rights and legitimate interests of the controller" in 5 letter e)]. Since this legitimate reason is also stated in the General Regulation [article 6 paragraph 1 letter f)], we would like to draw attention to some problematic points in the use of this reason for processing of data in identification systems and not only such systems.

Manuscript received August 9, 2017; revised November 2, 2017, revised November 12, 2017.

Vlastimil Benes is with IMA s.r.o., Prague, Czech Republic, e-mail: Vlastimil.Benes@ima.cz.

Karel Neuwirt is an independent DP consultant, Czech Republic.

Otto Dostal is with Brno University of Technology, Brno, Czech Republic, e-mail: xdosta48@stud.feec.vutbr.cz

II. Identification system

By identification systems we mean (in this article) systems for the identification of individuals whose common element is the identification of persons based on a physical medium, biometric element or known information. Typical representatives of such identification systems include attendance, access, catering and guard walk systems, production tracking systems, library lending systems, or vehicle usage systems. The General Regulation of course also applies to a number of other systems that process personal data.

It should be noted that we are using the term "identification system" as a different and broader one that the term "electronic identification scheme" used in the Regulation No. 910/2014 [2]. According to that Regulation, electronic identification scheme means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons, while identification means are defined as a unit containing person identification data and which is used for authentication for an online service. While identification systems discussed in this article might utilise such electronic identification scheme, they also might not fall within its definition, as it might not fulfil all the criteria, such as it might not include issuing of any identification means. As an example of this we can mention a CCTV system.

III. Impact of the regulation on data processing in EU

General Regulation establishes a single legal framework for the protection of personal data across the Union as it is a directly applicable regulation that does not require the full transposition procedure necessary for Directive 95/46/EC. The consistency of the legal framework has largely not been ensured by the Directive, since each member state has created its own legislation, which was based on the principles of the

Directive but was by no means the same and uniform in all member states. The fragmentation of national legislation has increased the costs and administrative burdens for businesses, caused uncertainty in a variety of business areas, and reduced the confidence of citizens in their own oversight over the processing of their personal data, in online services and in the digital economy as a whole. A new and uniform regulatory framework should, on the other hand, bring further development of the single market for online services and the related support for economic growth, innovation, employment, etc. By creating a single EU-wide legal framework for the protection of personal data, the need for comparisons between levels of data protection in individual member states and the associated uncertainty of businesses and institutions when carrying out a wide range of activities within the EU member states should also be avoided.

The Regulation provides data subjects with broad rights, whose application may allow them greater control over the processing of personal data that concern them [9], [10]. This is also one of the reasons why the Regulation applies to the processing of personal data of natural persons located in the EU by a controller or a processor, regardless of whether the processing takes place in the EU or the processing entities are located outside of the EU. This scope of the Regulation also applies to activities related to the offering of goods or services to data subjects within the EU, or to the monitoring of their behaviour if such monitoring takes place within the EU.

IV. Personal details and identification of a natural person

Identification systems (if their purpose is to identify persons) should be treated as a processing of personal data. The General Regulation defines personal data as ”any information relating to an identified or identifiable natural person (‘data subject’)” [10], [11]. A natural person is considered identifiable if thy can be identified, in particular by reference to a certain identifier (such as a name, identification number, location data, online identifier, etc.) or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The conditions for electronic identification and authentication are laid down in Regulation No. 910/2014 [2], which requires compliance with the principles laid down in Directive 95/46/EC (Article 5) for data processing. This Regulation defines ”electronic identification” as the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. The processing of personal data in electronic identification systems must therefore comply with the principles set out in the General Regulation.

In addition to the principle of legality and transparency of processing, the principle of processing in accordance with the purpose for which personal data were collected or the time limitation of retention of personal data, the principle of data minimization should also be carefully assessed in identification systems. This principle requires that each processing agent must use only such a set of personal data that is appropriate, relevant, and necessary for given purpose. Therefore, identification systems also should not work with personal information about individuals that are not necessary for a given application.

In practice, this requirement may imply the need to modify current identification systems, so that some items will have to be removed from both the databases and the input forms, in order to avoid breaching the principle of minimization, whether intentional or due to a mistake or error. An example might be to cancel the gender entry when registering visits to protected objects. Other technical measures introduced will be automatic deletion of the data after the expiration of the necessary retention period, which will not require any additional intervention by the system administrator. A typical example is the deletion of old video records in CCTV systems.

V. Legitimisation of data processing in identification systems

One of the essential conditions for the deployment of identification systems is the determination of the legitimate reason (legality) of the processing of personal data [3], [8]. The conditions for the lawfulness of the processing of personal data are laid down in Article 6 of the General Regulation. The controller of the identification system must meet at least one of the following conditions:

- The data subject has given consent to the processing.
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary for protection of the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

All six possibilities of legality of the processing are legally equivalent; the General Regulation prefers none of them above the others. The controller of the identification system must therefore assess and evaluate the relevance of these conditions; namely, they must analyse the nature, purpose, scope and context of the processing of the data, and determine the condition which best ensures its legitimacy.

It is clear from the overview of the legitimacy of the processing that any suitable condition (public interest, contractual relationship, legal obligation, etc.) can be used for identification systems. However, it may be presumed that a very frequent condition of legitimacy to ensure the legality of the processing of personal data in identification systems will be the ”legitimate interests of the controller” [6]. Other legitimacy options may be inappropriate, being either too demanding or costly (e.g. the consent of data subjects) or unusable because of inadequacy.

For example, we can point out the processing of personal data in camera systems whose records are stored on storage

media and where the system records identifiable natural persons. In a number of camera system installations (especially large ones), it is virtually impossible to obtain the consent of every individual (data subject) that can be captured by such a system. Consent is also not a usable reason, for example, in attendance systems, since nobody can be forced to consent; the data subject (e.g. an employee) has the right to refuse to give it.

It is clear that in such applications, the legitimization of the processing of personal data on the basis of the consent of the persons concerned is virtually inapplicable. Not only is it not possible for all persons to obtain such consent, which must be free, informed, concrete and unambiguous (article 4 paragraph 11), but more importantly any consent may be revoked by the data subject at any time. Also, the usage of such a right would undoubtedly make any identification system completely ineffective and useless. New conditions for the expression of the consent of the data subjects unambiguously give them the right to withdraw it at any time (article 7 paragraph 3). According to the Regulation, it will no longer be possible for the controller to limit this right in any way. If the controller uses the consent of the data subjects as their legal basis, it must always be prepared for consent to be withdrawn.

Controllers and processors apply the interests of the controller as the only rationally-applicable legal basis in most cases of the operation of identification systems. In many organizations, the identification system is deployed to ensure their own security, to detect security breaches and protect the organization's entire infrastructure, to guard against unauthorized access to protected information, to protect against hacking, industrial espionage, cyber attacks, etc. [7]. A legitimate interest is also the processing of personal data for the purpose of fraud prevention or for ensuring the safety and health of its employees. It is therefore undoubtedly a "legitimate interest" of the organization (the controller) and the processing of personal data in such systems is a necessary process for performing the legitimate activities of the organization. In such cases, the electronic identification system can process (to a reasonable extent) the personal data of employees, customers, sales representatives and others.

VI. Legitimate interest limits, Assessment of the impact on privacy of individuals

The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

The legitimate interest of the controller as a legitimate basis for the processing of personal data in the electronic identification system has, however, some fundamental limitations.

First of all, there must be an interest of the controller and this interest must be legitimate. "The legitimate interest of the controller" here is the purpose of the processing. As already stated in the current legislation, the purpose of the processing must be specific, expressly stated and also acceptable under domestic law. Such an interest must be genuine, lasting, and related to the legitimate activities of the controller. The purpose must be known to the data subjects and must be communicated to them (in any reasonable form).

The second essential condition is to balance the interests of the controller with the protection of the interests and fundamental rights and freedoms of the data subjects who could be identified or authenticated by the identification system. The processing of personal data is legal if it is necessary for the purpose of the legitimate interest of the controller and at the same time the legitimate interests of the controller are not outweighed by the interests or fundamental rights and freedoms of the data subjects [article 6 paragraph 1 letter f)].

Legitimate interest limits	
An interest	Is the broader stake that a controller may have in the processing, or the benefit that the controller derives (or that society might derive) from necessity the processing. A legitimate interest must be acceptable under the law'.
Necessary	This 'necessity' requirement applies to ensure that processing of data based on legitimate interests will not lead to an unduly broad interpretation of the necessity to process data. This means that it should be considered whether other less invasive means are available to serve the same end. The processing of personal data is allowed only to the extent strictly necessary and proportionate for the purposes.
Overriding	The existence of a legitimate interest needs careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller when personal data are processed in circumstances where data subjects do not reasonably expect further processing.

When deciding on the implementation of an identification system in an organization, an analysis of the impact of such a system on the privacy of the individuals should first be performed. Any impacts identified by the analysis should be dealt with in such a way that the systems operation interferes as little as possible with the rights of natural persons. The impact assessment should be done with consideration of the broader context and the context of the relationship between the data controller and the data subjects. For example they should evaluate if the persons concerned can expect or assume that the identification system will record them, whether identification or authentication is not deliberately hidden, whether the data subjects are appropriately informed of such a system and also about the possibilities of exercising their rights under the

Regulation. An assessment of the balance between the interests of the controller and the interests and rights of the data subjects must be an integral part of the decision-making process on the establishment and operation of identification systems.

VII. Conclusion

Undoubtedly, in many cases the controller's "legitimate interest" as a condition for the processing of personal data in identification systems will be invoked by the controllers or operators of these systems when assessing the compatibility of their processing with the General Regulation. However, they must be aware that this reason for the legitimatization of the processing of personal data has certain limits. Above all, it must hold water when balanced against the rights of the data subjects. The General Regulation provision is relatively flexible in this aspect, but this does not mean that it can be used as an "open door" for the legitimacy of processing of personal data in all cases where other conditions for the lawfulness of processing could not be used. Undoubtedly, it will not be possible to hide under "legitimate interest" cases of extensive on-line or off-line monitoring of employees, customers, or clients using a large amount of data about them from different sources that were originally collected in other contexts and for other purposes and the creation of complex profiles of personalities, preferences or behaviours of such persons (under Article 22 of General Regulation profiling as a basis for decision-making about data subjects is forbidden). The legitimate interests of a collector must always be balanced against the interests and fundamental rights and freedoms of the data subjects, which are guaranteed to them not only by Regulation itself, but also by the Charter of Fundamental Rights of the European Union and by the national regulations on fundamental rights and freedoms. The results of a check-up on this balance will show to a large extent whether the controller can, regarding the lawfulness of the processing of personal data, refer to the condition of his legitimate interest. It should also be kept in mind that the setting of the legitimacy of such processing is only one of the obligations that the General Regulation imposes on controllers and processors.

References

[1] Regulation (EU) 2016/679 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).

[2] Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[3] *The Guide to Privacy and Electronic Communications*, Information Communications Office, U.K., London, May 2016.

[4] *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, Article 29 data protection working party (WP 29), document WP 217, Brussels, 9 April 2014.

[5] *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*, Article 29 data protection working party (WP 29), document WP 247, Brussels, April 2017.

[6] *CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data (Discussion Draft)*, Centre for Information Policy Leadership, Hunton & Williams LLP, Brussels, March 2017.

[7] *Standardisation in the field of Electronic Identities and Trust Service Providers*, Inventory of activities, European Union Agency for Network and Information Security (ENISA), 2014.

[8] P. Woolfson and D. Terruso, "Data portability under EU GDPR: A financial services perspective," *Privacy Laws & Business International Report*, pp. 12-14, 2016.

[9] *EDPS Opinion 9/2016 on Personal Information Management Systems, Towards more user empowerment in managing and processing personal data*, European Data Protection Supervisor, Brussels, 2016.

[10] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of Personally Identifiable Information," *New York University Law Review*, vol. 86, 2011, pp. 1814-1894.

[11] S. Stalla-Bourdillon and A. Knight, "Anonymous Data V. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data," *Wisconsin International Law Journal*, pp. 284-322, 2017, [Online] Available: https://eprints.soton.ac.uk/400388/