ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XXXIX
2/2020

DATABASES IN THE ELECTRONIC IDENTIFICATION AND AUTHENTICATION SYSTEM: LAWFUL USE OF PERSONAL DATA[1]

Mgr. Petra Žárská, PhD., LL.M.

Comenius University in Bratislava
Institute of Information of Technology Law and Intellectual Property Law
petra.zarska@flaw.uniba.sk

Databázy v elektronickom identifikačnom a autentifikačnom systéme: Zákonné použitie osobných údajov

Členské štáty EÚ vybudovali elektronické systémy pre občanov s cieľom uľahčiť používanie systémov verejnej správy. Členské štáty zhromaždili obrovské množstvo osobných údajov na identifikáciu a autentifikáciu vo fyzickom svete a naďalej zhromažďujú údaje na identifikáciu a autentifikáciu v digitálnom prostredí. Nový právny predpis o ochrane osobných údajov – GDPR však zmenil pravidlá hry. Výsledkom prispôsobenia sa novému digitálnemu svetu prostredníctvom elektronických systémov je existencia neobmedzených databáz obsahujúcich osobné údaje občanov. Aké sú práva občanov a členských štátov k databázam z hľadiska autorských práv? V tomto príspevku sa skúmajú možné problémy, ktorým musia členské štáty a občania čeliť v súvislosti s databázami pozostávajúcimi z osobných údajov v súvislosti s autorským právom.

Datenbanken im elektronischen Identifikations- und Authentifizierungssystem: Rechtmäßige Verwendung personenbezogener Daten

Die EU-Mitgliedstaaten haben elektronische Systeme für die Bürger eingerichtet, um die Nutzung der Systeme der öffentlichen Verwaltung zu vereinfachen. Während die Mitgliedstaaten bereits eine große Menge personenbezogener Daten zur Identifizierung und Authentifizierung

[1] This article is created within the project APVV 17-0403: „Influence of mutual recognition of electronic identification means on public administration electronic services."

in der physischen Welt gesammelt haben, sammeln sie weiterhin Daten zur Identifizierung und Authentifizierung in einer digitalen Umgebung. Der Game Changer ist die neue Gesetzgebung zum Schutz personenbezogener Daten - DSGVO. Das Ergebnis der Anpassung an die neue digitale Welt durch elektronische Systeme ist die Existenz unbegrenzter Datenbanken, die personenbezogene Daten von Bürgern enthalten. Welche Rechte haben Bürger und Mitgliedstaaten in Bezug auf das Urheberrecht an diesen Datenbanken? Der Artikel untersucht mögliche Herausforderungen für Mitgliedstaaten und Bürger in Bezug auf Datenbanken, die aus personenbezogenen Daten bestehen, aus Sicht des Urheberrechts.

Databases in the electronic identification and authentication system: Lawful use of personal data

Member states of EU have built electronic systems for citizens in order to ease the use of public administration systems. While Member states have already collected vast amount of personal data for identification and authentication in the physical world, they continue to collect data for identification and authentication in digital environment. The game changer was the new legislation on the protection of personal data – GDPR. The result of adaptation to the new digital world through electronic systems is the existence of limitless databases containing personal data of citizens. What are the rights of citizens and Member States to these databases in terms of Copyright? The article explores possible challenges to be faced with by Member states and citizens in relation to databases consisting of personal data from perspective of Copyright.

Kľúčové slová: databáza, autorské právo, identifikácia, autentifikácia, elektronický systém, osobné údaje

Schlüsselbegriffe: Datenbank, Urheberrecht, Identifikation, Authentifizierung, elektronisches System, personenbezogene Daten

Keywords: database, copyright, identification, authentication, electronic system, personal data

Introduction

The electronic identification and authentication of people have brought new questions on the use of data capable of identifying and authentifying every person in the digital world. Member states face the important decision on the lawful use of processed personal data of its citizens. While Member states are obliged to process data in the line with biding law, we should also take into account the possibility of financial benefits of such processing. This article offers legal analyses of

the lawful use of personal data in the form of databases for commercial purposes by Member states. The analyses is divided into sections, which enlighten meaning of important provisions of Data Protection Law and Intellectual Protection Law, then following sections focus on related legal issues and in the summary a possible solution for commercial use of databases consisting of personal data is presented.

1. The database in EU law

What is a database from legal point of view? According to article 1 sec. 2 of Database Directive[2] (further only as "Directive"), a database is collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. "All these conceptual attributes have to be filled at the same time. The protection is provided for electronic and non-electronic databases. The final definition of database is more extensive than the first proposal of Directive asked. By contrast, computer programs are not protected. Directive 96/9 also does not cover computer programs used with creation or during functioning of electronic databases (art. 1 sec. 3 of Directive). Through all this, the question of protection has to be answered in relation to the specific database. We can imagine, that the protection under Directive might cover the computer program, which is inseparably tied to functioning of a database."[3] The definition of the term "database is rather wide. On the other hand, there are limitations to the extent of definition, such as it does not cover computer programs[4] or a compilation of several recordings of musical performances on CD[5].

Regarding the protected matter, Directive set up somehow non-traditional situation. We might say that a database is protected twice, which is partially true. According to Directive, there are two types of protection. Any of these protections is not redundant, because they target different parts of a database. "It is necessary to remember, that legal protection of databases by Directive does not collide with Copyright protection of respective elements of the database content. On the contrary, the protection by Directive complements Copyright

[2] DIRECTIVE 96191EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 1996 on the legal protection of databases.

[3] CONNELLY KOHUTOVÁ R. Databases in the age of information society and its legal protection. p. 48.

[4] Recital No. 23 of Directive.

[5] Recital No. 19 of Directive.

protection, or reinforce it. Both regimes can exist in parallel or independently."[6]

The first type of protection is Copyright. According to article 3 sec. 1 of Directive, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection. According to section 2 of the same article, Copyright protection of databases provided for by Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves. Copyright protection focus on databases designed by an author (or authors) who is a natural person. At the same time, this database has to be the author's own intellectual creation. Also, according to art. 4 sec. 1 where the legislation of the Member States so permits, the legal person can be designated as the rightholder by that legislation. Copyright protection does not extend to the contents of databases and expires 70 years after an author's death.[7]

The second type of protection is the sui generis right to databases enacted by Directive. According to article 7 sec. 1 of the Directive, Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. The sui generis right enables a maker of database - natural or legal person to protect contents of a database. The sui generis right expires 15 years after the database's creation. Both protection allow author and/or maker to transfer, assign or grant rights under contractual licences.

Copyright and the sui generis right might simultaneously protect a database. Based on article 7 of Directive, the sui generis right to database is not affected by Copyright, because article 7 sec. 4 reads, that the sui generis right shall apply irrespective of the eligibility of that database for protection by Copyright or by other rights. "The right applies to databases whether or not their arrangements justifies Copyright and whatever the position may be regarding Copyright to

[6] CONNELLY KOHUTOVÁ R. Databases in the age of information society and its legal protection. p. 50.

[7] In both cases (Copyright and sui generis right), the duration of rights is duration of economic rights.

individual items in its contents."[8] The protection of databases afforded by the sui generis right shall be without prejudice to existing rights related to the contents of such database. Subsequently, we might differ the eligibility for protection of a database based on what legal requirements it fulfils. Databases eligible for protection under the sui generis right are those ones, which are not author's own intellectual creation, or/and consist of contents, which also do not match thresholds for Copyright protection. For example, database protected solely by the sui generis right are those created by a natural person under various types of agreements, resulting in the situation, where the holder of the sui generis right is a maker of database. The content of such database may consist from any kind of data – weather data or from paintings or songs which are protected by Copyright. Similarly, the protection by the sui generis right of such database shall not prejudice rights related to the contents of a database held by third parties, such as songs.

2. The creation of databases in the electronic identification and authentication system

We might recognize several key factors for the existence of databases within public administration systems in EU. According to the recital No. 5 of GDPR, firstly, the economic and social integration resulting from the functioning of the internal market led to a substantial increase in cross-border flows of personal data. Secondly, the exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union increased. Thirdly, national authorities in the Member States were being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State. We might say that as much as cross-border flows, exchange of data and cooperation among Member States contributed to the higher number of databases, the efficacy of public administration weighed in with the same force. All the aforementioned causes resulted in significant growth of databases in the public sector. Building of databases within identification and authentication systems of Member States (further only as "IASs) is vital for the proper functioning of all major public administrative bodies. In the Single Digital Market of EU, Member States adapted to the digital development have started to build

[8] CORNISCH, W., LLEWELYN, D., APLIN, T. Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights, p. 875.

predominantly electronic databases of personal data of their citizens. Public administrations of Member states approach the collection of personal data as collection of information needed for performing its fundamental duties. "The stages of the government's information holdings begin with its collection and production and include use, storage, retrieval, dissemination, protection, disposal and longer-term retention. Information collected for one purpose can be re-used for other purposes, and storage of information in electronic databases opens up significant possibilities — and related issues — for sharing information and creating new information and knowledge. Such information can be retained as individual data elements, as combinations of data to support decision-making and, with the application of judgement, as accumulated knowledge and wisdom."[9] Public administrations (further only as PAs) collect and process all kind of information including personal data on its citizens. PAs organize all information into databases that allows them to use information efficiently. Personal data are also organized into databases for quick data search on a specific person or for separation of certain data from other data. Before creation of electronic IASs, collected personal data were used for identification in the physical world only, for example for issuing ID card or certification of birth/marriage. Nowadays, PAs use personal data also for the identification and authentication of citizens in digital world – electronic systems[10]. Electronic databases in IASs are endless source of information and its use brought new interesting issues.

3. Who is the maker of a database and why?

The maker of a database is not defined directly in Directive, this definition was left to recitals. Recital No. 41 of Directive defines maker as the person who takes the initiative and the risk of investing; whereas this excludes subcontractors in particular from the definition of maker. Recital No. 39 shed some light on meaning of investment made by a maker, it says that whereas, in addition to aiming to protect the copyright in the original selection or arrangement of the contents of a database, this Directive seeks to safeguard the position of makers of databases against misappropriation of the results of the financial

[9] BROWN, D. Electronic government and public administration. In: International Review of Administrative Sciences. p. 249.

[10] In Slovakia, citizens use the electronic system called „slovensko.sk". It is the central system of public administration.

and professional investment made in obtaining and collection the contents by protecting the whole or substantial parts of a database against certain acts by a user or competitor. "The database has to be the product of substantial investment. It cannot, for instance, consist merely of different works collected together on an ordinary music CD."[11] Directive requires a natural or legal person in order to become a maker of database to be initiative and make a substantial investment into creation of a database. When assessing the substance of investment, the investment has to be substantial quantitatively or qualitatively. "Investment in the creation of a database may consist in the deployment of human, financial or technical resources but it must be substantial in quantitative or qualitative terms. The quantitative assessment refers to quantifiable resources and the qualitative assessment to efforts which cannot be quantified, such as intellectual effort or energy, according to the 7th, 39th and 40th recitals of the preamble to the Directive."[12] At the same time when a maker invests quantitatively (for example financial investment) or qualitatively (a person's intellectual contribution), a maker has to make the "right" kind of investment. "The expression ‚investment' in ... the obtaining ... of the contents' of a database must be understood to refer to the resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent materials. The purpose of the protection by the sui generis right provided for by the Directive is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database."[13]

Member states are makers of databases, because they fulfil all legal requirements asked by Directive. Member states as makers undoubtedly invest into creation of databases quantitatively by financing governmental buildings and employees' salaries and qualitatively as well by employee's intellectual efforts to create databases. Member states seek out, obtain and verify[14] existing independent materials – personal data of citizens, therefore, it is also the "right" investment.

---

[11] See 5. – to connely

[12] C-444/02, Fixtures Marketing Ltd. v. Organismos prognostikon agonon Podosfairou AE (OPAP), point 44.

[13] C-444/02, Fixtures Marketing Ltd. v. Organismos prognostikon agonon Podosfairou AE (OPAP), point 40.

[14] Member states usually obtain personal data directly from data subjects, verify it with the data subjects, but they do not present these databases publicly due the confidential character of data and its legal obligation to protect safety of personal data.

4. Personal data in databases

Databases compiled by Member states as result of its legal obligations are unique due to its content. Member states are allowed to process data thanks to art. 6 of GDPR which lists reason for lawful processing of personal data. Member states use for processing mainly sec. 1 sub. c), d) and e) of article 6 of GDPR. Subsection c) allows a Member state as a controller[15] to process personal data for compliance with a legal obligation to which the controller is subject, subsection d) allows processing when it is necessary in order to protect the vital interests of the data subject[16] or of another natural person. Subsection e) allows processing when it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, which is probably the most used legal basis by PAs for data processing. Where it suits the purpose, Member states are allowed to use all legal basis stated in art. 6 of GDPR. Given to the fact, that PAs process data predominantly when they follow certain legal obligations, protecting vital interest of citizens, carry out tasks of public interest or exercise official authorities, we may say that the use of other legal basis can be minimal.

The contents of databases are personal data of all citizens. The extent and amount of such data is hard to measure. The data are piling up and so types and figures of databases. We distinguish[17] between databases consisting of collected data and databases consisting of derived data[18]. Within collected data, we find different categories of data, such as basic personal data (name, address, the number of ID card), data concerning

[15] Art. 4 sec. 7 of GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[16] Art. 4 sec. 1 of GDPR: data subject is an identified or identifiable natural person.

[17] There are many categories of distinguishing data based on different approaches, such as differentiation based on the method of acquiring data, on types of data subjects and lots of others.

[18] More on definition of derived data and related issues in MESARČÍK, M. Am I really afraid of the darkness? Some considerations about technological determinism in the context of personal data protection. In: Acta Facultatis Iuridicae Universitatis Comenianae. Volume 36, No. 2 (2017), pages. 204-217.

health[19], biometric data[20], genetic data[21], data on sexual preferences and political opinions[22]. By combining databases with content consisting of collected data, Member states might create derived data. Derived data kept in the form of databases might be of great commercial value for makers, in this instance Member states.

The unique character of the content of databases consisting of personal data can possess challenging questions towards to the lawful use of databases by Member states when we take into account GDPR requirements on processing of data and the sui generis right to databases.

5. Rights of Member states to databases

Member states possess rights towards databases, because Member states are makers of it. In the line with art. 7 sec. 1 of Directive, a maker of database is entitled to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of the database. Apart from the right to prevent unlawful use, Member states can exercise their right to licence the use of databases through licences. Licences are standard tools for makers to financially benefit from the creation of databases. Licencing the use of databases with contents such weather information, information on minimal wage, therefore information publicly accessible and not being personal, shall be seamless due to the non-existence of rights of third parties related to the information. The same cannot be applied to personal data, because data subjects which provided data to PAs, holds specific rights to their personal data in databases create by Member states. Member states as makers produce databases consisting of personal data of citizens for specific lawful purposes in article 6 of

[19] According art. 4 sec. 15 of GDPR, '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.

[20] According art. 4 sec. 14 of GDPR, '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.

[21] According to art. 4 sec. 13 of GDPR, 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

[22] According art. 9 of GDPR these data are special categories of data. Proccessing of such data is generally prohibited, unless processing falls under exemptions in art. 9 sec. 2 of GDPR.

GDPR. These specific lawful purposes mostly used by Member states[23] do not cover licencing of data for any reason. By comparison, when a Member state wish to licence the databases without personal data consisting of data where no related rights of third parties exist (such weather data or any kind of publicly accessible data for free use), a Member state is free to do it without consents of any third parties.

6. Rights of data subjects to personal data in databases

According to chapter III of GDPR, data subjects are entitled to specific rights to their own personal data. Citizens provide personal data to Member states in the positions of data subjects, therefore they can exercised data subjects' rights towards their personal data. These rights are listed in Chapter III of GDPR. Those rights are the right to be informed under art. 13 and 14, the right of access under art. 15, the right to rectification under art. 16, the right to erasure under art. 17, the right to restriction of processing under art. 18, the right to notification obligation regarding rectification or erasure of personal data or restriction of processing under art. 19, the right to data portability under art. 20, the right to object in case of automated individual decision-making including profiling and other rights under art. 21 and 22. Apart from these rights, a data subject has the right to withdraw a consent to processing any time under art. 7 sec. 3, the right to lodge a complaint with a supervisory authority under art. 77, the right to an effective judicial remedy against a supervisory authority under art. 78, and the right to an effective judicial remedy against a controller or processor under art. 79.

This broad set of rights can by exercised by data subject in connection to their personal data whether data are organized in database or not. We should stressed at this point the fact, that personal data are organized into databases purely for the efficacy of data usage by controller. From the point of GDPR, the fact that data are organised into databases has no bearing on exercising of data subjects' rights. In hypothetical situation, where Member states build a databases consisting of personal data while data were processed for purpose of art. 6 sec. 1 subsection e) (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority), any data

[23] Look at par. 4 of this article, where main legal basis for processing data by Member states are mentioned.

subject can employ aforementioned rights, for example a data subject can access data in database, erase data or rectify data.

Summary

According to recital No. 10 of GDPR, regarding the processing of personal data for the compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. Where Member States did not introduce specific provision on the use of database consisting of personal data processed for purposes of aforementioned legal basis[24], we assume, that binding law shall be applied. Binding law – GDPR allows Member states to authorize use of databases only for purposes for which data were processed. These purposes are mainly legal obligations, the performance of a task carried out in the public interest or the exercise of official authority vested in the controller. The commercial use of databases by its virtue cannot be classifies as part of legal obligations that Member states are obliged to fulfil towards to citizens or other Member states. At this point such legal obligations are at least controversial or seen as harmful to fundamental freedoms and rights of data subjects. Also we cannot subsume such commercial use of databases under public interest, because majority of these data are of confidential character and Member states are legally required to protect it from misuse, therefore it is not in the public interest to present it publicly and commercialize it publicly too. Finally, it is very brave to imagine any official authority for monetization of databases at this time, where no such official body for commercialization of databases consisting of personal data exists. When we rule out the commercial use of databases consisting of personal data processed on specific legal basis as Member states do it, we might think that there is no way out of it. The opposite seems to be true. The solution might be the use of databases in the anonymised or pseudonymised form. According recital No. 28 of GDPR, the application of pseudonymisation[25] to personal data

[24] For example The Slovak republic, as many other Member States, did not introduce any specific national provisions towards the use of personal data in the case of data processing based on the compliance with legal obligations, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[25] More on pseudonymised data in Hintze, M. Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency.

can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. If Member states would use pseudonymisation of data in all databases consisting of personal data, there might be a way of licencing such databases to third parties while adhering to biding law on data protection. At the same time, Member states would only reduce the risks for rights and freedoms of data subjects, because there possibility of unauthorised reversal of pseudonymisation[26] exists.

The most feasible solution for commercial use of databases might be the anonymization[27]. According to recital No. 26 of GDPR, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. As result, GDPR does not therefore concern the processing of such anonymous information, including for statistical or research purposes. With the anonymization of data in databases, Member states might licence it and thrive on financial sources acquired from licencing without breaking EU data protection law.

References

1. APLIN, T., DAVIS, J.: *Intellectual Property Law, Text, Cases, and Materials*. 2th edition. Oxford: Oxford University Press, 2013. 932 pages. ISBN 978-0-19-874354-5.
2. BROWN, D.: *Electronic government and public administration.* In: International Review of Administrative Sciences. Volume: 71 issue: 2, pages 241-254.
3. CONNELLY KOHUTOVÁ R.: *Databases in the age of information society and its legal protection.* First edition. Praha: C.H.Beck, 2013, 221 pages.
4. CORNISCH, W. LLEWELYN, D., APLIN, T.: *Intellectual property: Patents, Copyright, Trade Marks and Allied Rights.* 7th edition. London: Sweet & Maxwell, 2010. 974 pages. ISBN 978 1847039231.
5. Finck, M., PALLAS, F.: *They who must not be identified – distinguishing personal from non-personal data under the GDPR.*

[26] The reversal of pseudonymisation is a technique which allows the linking of one or more pseudonyms back to the identity of the pseudonym holders. Detailed explanation of the whole proces is offered in the guidelines produced by The European Union Agency for Cybersecurity from November 2019 with the title „Pseudonimisation techniques and best practices“ available at https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

[27] More on anonymisation in Finck, M., Pallas, F. They who must not be identified – distinguishing personal from non-personal data under the GDPR.

In: International Data Privacy Law. 2020. Volume 10, No. 1, pages 11-36.
6. Hintze, M.: *Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency.* In: International Data Privacy Law, Volume 8, Issue 1, February 2018, Pages 86-101.
7. MESARČÍK, M.: *Am I really afraid of the darkness? Some considerations about technological determinism in the context of personal data protection.* In: Acta Facultatis Iuridicae Universitatis Comenianae. Volume 36, No. 2 (2017), pages. 204-217.