DATABASES CONSISTING OF PERSONAL DATA: PROMISING FINANCIAL OPPORTUNITY FOR MEMBER STATES?

Petra Žárská*

Abstract: *In times of economic recession Member states might seek new incomes. Governments of Member states should not overlook the financial potential of electronic databases consisting of personal data. The commercial use of such databases seems controversial, because the EU data protection law does not allow it directly. However, Copyright and the sui generis database right allow governments of Member states financially profit from the authorized use of databases. The aim of this article is to provide a feasible solution on the lawful commercial use of databases consisting of citizens' data for Member states.*

Keywords: *database, sui generis right, copyright*

INTRODUCTION

The digital era has changed the electronic identification and authentication in the public sector. Not only the new data regulation was established, but the digital world also brought new rights for citizens of Member states towards their personal data. Inevitably, the new data protection law represented by General Data Protection Regulation[1] (further only as "GDPR") has been clashing with binding laws. Given to the fact that personal data are used for creation of databases, Copyright and the sui generis right to databases are a significant part of the play. It might seem that the EU data protection law prevents certain authors and makers of electronic databases consisting of personal data (further as "personal database" as well for the purpose of this article) from exercising Copyright and the sui generis right to databases, therefore they do not generate expected profits from databases. Generally, any author or maker of a database is entitled to use it commercially. The object of the article is to analyse the possibility of lawful use of databases consisting of citizens' personal data for commercial purposes by Member states. The methods of research are information collection, systematizing, generalizing, valuation, comparison, analysis of literature, synthesis, and deduction. The article is divided into eight chapters and conclusion, which enlighten meaning of relevant provisions of GDPR and the Database Directive,[2] related legal issues and in conclusion the author of the article (further

* Mgr. Petra Žárská PhD., LL.M., assistant of professor at the Institute of Information Technology Law and Intellectual Property Law, Faculty of Law, Comenius University in Bratislava, Bratislava, Slovak Republic. ORCID: 0000-0002-1574-5609. This article was drafted with the support from a grant awarded by the Slovak Research and Development Agency No. APVV–17–0403 Effects of Mutual Recognition of Electronic Identification Means on Electronic Services of Public Administration and is included in a research task.

[1] EUROPEAN UNION. Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation). Further as "GDPR". In *EUR-Lex* [online]. 27. 4. 2016 [2022-04-04]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

[2] EUROPEAN UNION. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. In *EUR-Lex* [online]. 11. 3. 1996 [2022-04-04]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009>.

only as "the Author") will explain a workable solution for the commercial use of databases consisting of personal data by Member states.

1. THE EU DATABASE LAW

The most important element of the EU database law is undoubtedly the Database Directive (further as "the Directive"). "The Database Directive aims to regulate interests in the information market."[3] The Directive characterises a database in the article 1 sec. 2 as a 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."[4] The definition of the term database is rather wide. According to recital 17 of the Directive, this term should be understood to include literary, artistic, musical or other collections of works or collections of other material such as texts, sound, images, numbers, facts, and data. This term also covers collections of independent works, data or other materials which are systematically or methodically arranged and can be individually accessed. At the same time, the extent of the term is limited by the fact that recording or an audio-visual, cinematographic, literary, or musical work as such does not fall within the scope of the Directive, it also does not cover computer programs[5] and a compilation of musical performances on CD.[6]

Notionally, we might concur that the protection of any database is twofold. The Directive created a non-standard situation, where we can rely on the two kinds of protection. Without hesitation, we might state, that these two protections are useful, because it focuses on different features of a database.

The sui generis database right was invented by the Directive, while Copyright had existed before it. "It is necessary to remember, that legal protection of databases by the Directive does not collide with Copyright protection of respective elements of the database content. On the contrary, the protection by the Directive complements Copyright protection, or reinforce it. Both regimes can exist in parallel or independently."[7]

Copyright is the original protection of databases.[8] According to article 3 sec. 1 of the Directive, databases which, by reason of the selection or arrangement of their contents, con-

[3] GERMANY. Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach? [online]. BANTERLE, F. The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis. Berlin: Springer Nature, 2018, p. 13. In: *Springer Link* [online]. [2022-03-31]. Available at: <https://link.springer.com/content/pdf/10.1007%2F978-3-662-57646-5.pdf>.

[4] CONNELLY KOHUTOVÁ, R. *Databases in the age of information society and its legal protection.* Prague: C. H. Beck, 2013, p. 48.

[5] Recital No. 23 of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. In *EUR-Lex* [online]. 11. 3. 1996 [2022-04-04]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009>.

[6] Recital No. 19 of the Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. In *EUR-Lex* [online]. 11. 3. 1996 [2022-04-04]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009>.

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

[8] The Commission proposal for a Council Directive on the legal protection of databases (COM(92) 24 of 15.4.1992) aimed to provide copyright protection in each Member State for databases as collections within the meaning of Article 2(5) of the Berne Convention for the Protection of Literary and Artistic Works (text of the Paris Act of 1971).

stitute 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 this article, Copyright protection of databases provided for by the Directive shall not extend to their contents and shall be without prejudice to any rights subsisting in those contents themselves. Copyright protection aims to protect databases created by a natural person – the author[9] and the database must be the author's own intellectual creation. As general time rule, Copyright protection of databases expires 70 years after an author's death.[10] To differentiate Copyright from the sui generis right conceptually, we must stress that Copyright protection of databases provided for by the Directive shall not extend to their contents, while the sui generis right does. "Copyright does not protect the contents but only the database's structure. So, taking the contents without the structure would not infringe. An additional protection was necessary to protect the contents."[11] This lack of protection resulted into the enaction of sui generis database right. 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 overwhelming majority of commentators classify it as an intellectual property right and many Member States have classified it as a neighbouring right in their national laws. It is also clear that the sui generis right is not (part of) Copyright."[12] Without doubts the sui generis right, which enables a maker of database protects its contents has a special character in terms of extent and subject of protection. The protection expires 15 years after the database's creation. Both protections enable authors and/or makers to transfer, assign or grant rights under contractual licences.

Some databases can be simultaneously protected by Copyright and the sui generis right. The overlapping protection was assumed by the article 7 sec. 4 of Directive, which reads, that the sui generis right shall apply irrespective of the eligibility of that database for protection by Copyright or by other rights. "The (sui generis) right applies to databases whether or not their arrangements justifies Copyright and whatever the position may be regarding Copyright to individual items in its contents."[13] The protection by sui generis right shall be without prejudice to rights existing in respect of their contents of a database, therefore rights of citizens as data subjects under GDPR have to be taken into account in the process of authorisation for the usage of databases.

[9] Art. 4 sec. 1 of the Directive 96/9/EC says where the legislation of the Member States so permits, the legal person can be designated as the rightsholder by that legislation, therefore not only natural persons can become holders of copyright to databases.

[10] According to art. 1 subsection 1 of the Directive 2006/116/EC of the European parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights. Also, in both cases (Copyright and sui generis right), the duration of rights is duration of economic rights.

[11] UNITED KINGDOM. *EU Copyright Law: A Commentary*. DERCLAYE, E. *Database Directive*. Cheltenham: Edward Elgar Publishing, 2014, p. 320. In: *Elgaronline* [online]. [2022-03-31]. Available at: <https://www.elgaronline.com/view/edcoll/9781786437792/9781786437792.xml>.

[12] Ibid.

[13] CORNISCH, W., LLEWELYN, D., APLIN, T. *Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights*. London: Sweet & Maxwell, 2010, p. 875.

2. GOVERNMENTAL DATABASES IN THE ELECTRONIC IDENTIFICATION AND AUTHENTICATION SYSTEM

Why do we have governmental electronic databases consisting of personal data? The elevated number of personal databases has been caused by moving the public sector into the electronic form[14] and by the evident importance of personal data in the new Digital Single Market of EU. EU responded to it by higher level of protection of its citizens, by establishing the new data protection legislation – GDPR.

The recital No. 5 of GDPR recognises several important reasons for creating the new legislation on data, which preserve rights of citizens to personal data in the identification and authentication systems of Member states.[15] 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 to be able to perform their duties or carry out tasks on behalf of an authority in another Member state. Subsequently, the efficacy of national public administrations would by troubled if governments would not adapt to the digital transformation resulting from functioning of the Digital Single Market of EU. The digital transformation of services for citizens requires efficient data storage system of processed data. The adaptation to effective data storage requirement came in the form of vast national electronic personal databases. Building personal databases in identification and authentication systems is essential for appropriate functioning of all EU governmental bodies. Generally, governments approach processing of personal data and information as the collection, usage, and storage of it necessary for performing its legal 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 open 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. "[16] EU governments construct personal

[14] The overall performance on eGovernment in the EU is moving in the right direction. Today 58% of EU citizens choose to get in touch with their public administration online and the overall online availability of public services is 82 %. Digital solutions can greatly contribute to strengthening the trust of citizens in governments. Europe will make a big leap in this direction on 29 September when the eIDAS Regulation rules on cross border recognition of electronic identification means enter into force. In: *European Commission* [online]. 24. 9. 2018 [2022-03-31]. Available at: <https://digital-strategy.ec.europa.eu/en/news/moving-forward-digital-public-services-europe>.

[15] More on issues of identification and authentication through the use of personal data find in the article: ANDRAŠKO, J. Mutual recognition of electronic identification means under the eIDAS Regulation and its application issues. *AD ALTA.* 2017, Vol. 7, No. 2, pp. 9–13.

[16] BROWN, D. Electronic government and public administration. *International Review of Administrative Sciences.* 2005, Vol. 71, No. 2, [2022-03-31]. Available at: <https://journals.sagepub.com/doi/pdf/10.1177/0020852305053883>.

data into databases, because then the use of it can be efficient. Before the existence of electronic personal database, processed personal data identified citizens in the physical world only, citizens identified themselves by ID cards or certifications of birth. In the digital era, EU governments use personal data for the identification and authentication of citizens in digital world[17] – electronic systems.[18] While electronic personal databases are the most vital source of governmental information, its existence also brought new interesting legal issues in relation to Copyright and the sui generis database right.

3. THE RIGHTSHOLDER OF COPYRIGHT AND/OR MAKER OF A DATABASE

When defining the position of EU governments in terms of creating databases, we need to differentiate whether the database is protected by Copyright or the sui generis right. The reason is the different set of rights available within each protection and duration of rights.

The object of protection by Copyright is the database which is the author's own intellectual creation. According to the article 4 sec. 1 of the Directive, the author of database shall be the natural person or group of natural persons who created the base or, where the legislation of the Member states so permits, the legal person designated as the rightsholder by that legislation. According to binding law, EU governments and its institutions are legal persons, therefore they can be rightsholders of Copyright, but they are not authors. By whom are databases created when the rightsholder is an EU government? In this scenario, personal databases are created in two regimes. The first regime presents a situation, where an employee under the employment contract designs a database based on requirements laid down by an employer, the government. Based on national laws, EU governments than exercise the author's rights in the position of rightsholders, which means that governments are legally allowed to exercise economic rights towards to the database. The right to use the work and the right authorise the use of work belong to the author, in this case in the regime of employee's work, this right belongs to the rightsholder, the government.

Second regime of creating databases by governments, which are also the author's own intellectual creations, is the commissioned work. EU governments enter contracts with third parties (natural or legal persons) with the aim to create databases. These contracts stipulate the rights of a government to the database, usually the right to use and to authorise the use of work (database) is reserved to the commissioner – the government.

Under the article 5 of the Directive, which details the right to use and to authorize the use of databases, governments as rightsholders have the same exclusive rights as authors to carry out or to authorize temporary or permanent reproduction, to translate, adapt, arrange or alter database. They can decide about any form of distribution to the public of the database or of copies thereof. EU governments have the right to communicate, display or perform the database to the public.

[17] SLOVAKIA. Electronic identification: theory and practice. SOPÚCHOVÁ, S. On the problems of identification and authentication of foreign persons electronic identity in electronic communication with public authorities of the Slovak Republic. Bratislava: Comenius University, 2020, pp. 78–85. In: *ResearchGate* [online]. [2022-03-31]. Available at: <https://www.researchgate.net/publication/349028106_ELEKTRONICKA_IDENTIFIKACIA_TEORIA_A_PRAX>.

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

Under the sui generis right, the object of protection is not author's own creation and instead of the author, the maker of database possesses all rights towards to databases. The Directive does not contain the definition of a maker in provisions, this definition was left to recital No. 41. The maker is a person who takes the initiative and the risk of investing, the definition excludes subcontractors. Recital No. 39 of the Directive explains meaning of investment made by a maker, it says that whereas, in addition to aiming to protect 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 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."[19] The Directive requires a natural or legal person to become a maker of database to be initiative and make a substantial investment into creation of the database. When one determines the substance of investment, one must conclude that 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."[20] If a maker invests quantitatively (such as financial investment) and/or qualitatively (such as person's own intellectual contribution), a maker must invest "correctly"." 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. "[21]

Undoubtedly, Member states creates databases in the line with the Directive because they respect legal requirements of the Directive. Member states invest in databases quantitatively, for example by subsidize buildings and employees' wages and qualitatively as well by employee's intellectual contribution. Member states track down, obtain, and verify[22] existing independent materials – personal data of their citizens, therefore, we can safely state that, it is the "correct" investment under the Directive. This correct investment and fulfilling other necessary legal conditions asked by the Directive and nationals laws result in the creation of databases with considerable financial potential, where Member states are makers of these databases.

[19] CONNELLY KOHUTOVÁ R. *Databases in the age of information society and its legal protection*. p. 53.
[20] C-444/02, Fixtures Marketing Ltd. v. Organismos prognostikon agonon Podosfairou AE (OPAP), point 44.
[21] C-444/02, Fixtures Marketing Ltd. v. Organismos prognostikon agonon Podosfairou AE (OPAP), point 40.
[22] 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. THE SPECIAL CONTENT OF DATABASES

Personal databases produced by Member states are "special" due to its contents. As we approached the digital era, personal data have become "commercial assets",[23] whether we saw it coming or not. The digital revolution[24] happened fast, the law caught up latter. Before the digital age and personal data becoming commodity, the idea of using collected personal data of citizens by EU governments for commercial purposes was too distant. This idea may still seem farfetched from the original purpose of data processing mainly due to the sensitive character of personal data and possible negative effects on citizens if data would be misused. At the same time, private entities collect personal data of all kinds on citizens and sell it to other private entities predominantly for marketing purposes.[25] This data trading[26] is happening now whether we realize it or have clear laws on it.[27] Should not EU governments have a certain chance, as private companies have, to pick up profits from this trade already happening?

From legal point of view, GDPR and the Directive left the open door for creation of databases consisting of personal data. "Indeed, the definition of a database set out by the Database Directive embraces any type of data. Recital 48 states that the database protection is without prejudice to data protection law thus recognizing the possibility of databases including personal data."[28] GDPR prescribes legal bases for processing personal data for all entities including Member states. Art. 6 of GDPR enlists bases for lawful processing of personal data. Member states may employ all bases, but from the character of their official duties we can derive that the most used bases for processing are sec. 1 sub. c), d) and e) of article 6 of GDPR. Subsection c) allows a member state as a controller[29] to process personal data for compliance with a legal obligation to which the con-

[23] See more in UNITED STATES. *Assetization: Turning Things into Assets*. BEAUVISAGE, T., MELLET, K. Datassets: Assetizing and Marketizing Personal Data. Cambridge MA: MIT Press, 2020, pp. 75–95. In: *MIT Press Direct* [online]. [2022-04-04]. Available at: <https://direct.mit.edu/books/book/4848/AssetizationTurning-Things-into-Assets-in>.

[24] HELBING, D. Societal, Economic, Ethical and Legal Challenges of the Digital Revolution: From Big Data to Deep Learning, Artificial Intelligence, and Manipulative Technologies. *Justletter IT*. 2019, Vol. 16, No. 2, [2022-03-31]. Available at: <https://www.researchgate.net/publication/335748286_Datassets_Assetizing_and_Marketizing_Personal_Data, p>.

[25] ESTEVE, A. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law*. 2017, Vol. 7, No. 1, [2022-03-31]. Available at: <https://academic.oup.com/idpl/article/7/1/36/3097625?login=true>.

[26] OH, H., PARK, S., LEE, G. M., HEO, H., CHOI, J. K. Personal Data Trading Scheme for Data Brokers in IoT Data Marketplaces. *IEEE Access*. 2019, Vol. 7, No. 1, [2021-01-25]. Available at: <https://ieeexplore.ieee.org/document/8664564>.

[27] Apart from data trading, how personal databases created by internet companies can be misused in PLAVČAN, P., FUNTA, R. Some economic characteristics of internet platforms. *DANUBE: Law, Economics and Social Issues Review*. 2020, Vol. 11, No. 2, [2022-03-31]. Available at: <https://sciendo.com/article/10.2478/danb-2020-0009>.

[28] GERMANY. *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* BANTERLE, F. The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis.

[29] 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.

troller is subject, subsection d) enables processing when it is necessary to protect the vital interests of the data subject[30] 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.

First specific trait of personal databases is the character of its content – personal data. We must not forget the second specific trait in relation to databases. It is the volume of data in personal databases. We assume that given to the ongoing processing of personal data in all Member states on all their citizens, EU may have at its disposal the second biggest database of personal data in the world, the biggest personal database should be probably attributed to China. The potential of such database is endless. We might use it in a different way, for example for health research or generating financial gain. Whichever aim might be pursued by EU governments in the quest of fair and balance usage of this data bank, the usage must be in the line with law. The biggest fear hovering over such usage is the safety of personal data.

In terms of the inner character of data, we distinguish[31] between databases consisting of original data provided by data subject and databases consisting of derived data.[32] The first type of data is untouched data processed in the provided form and the data will not be changed or transformed in the future by the controller. On the contrary, derived data are result of combination of data and after the combination of different type of data, the controller invents absolutely distinctive data from the data used at processing. Exercising of Copyright and the sui generis right towards to personal databases consisting of personal data might differ based on whether original or derived data are the content of databases. For purposes of this article only the original data will be analysed, the derived data will be the topic of separate research by the Author. Within the original data, we can identify various categories of it under GDPR. GDPR recognises basic personal data (for example name, address, the number of ID card), data concerning health,[33] biometric data,[34] genetic data,[35] data on sexual preferences and political opinions.[36]

The rare nature of personal databases brings great challenges for its lawful use by Member states. Member states should be interested into establishing legal limitations

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

[31] Literature recognises many data categories based on various qualities of data, such as the type of data based on the method of acquiring data, on data subjects and many others.

[32] If you are interested into derived data, you can read more in MESARČÍK, M. Am I really afraid of the darkness? Some considerations about technological determinism in the context of personal data protection. *Acta Facultatis Iuridicae Universitatis Comenianae.* 2017, Vol 36, No. 2, pp. 204–217.

[33] According to 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.

[34] According to 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.

[35] 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 from an analysis of a biological sample from the natural person in question.

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

of lawful use of these databases. When the legislation on lawful use of personal database by Member states is missing, it is necessary to take into account existing legislations concerning such usage, which are GDPR and Copyright and/or the sui generis right to databases.

5. LICENCING DATABASES

The Intellectual Property rights to databases available for EU governments depend on the character of databases, whether Member states are rightsholders of Copyright or makers with the sui generis right. For example, Member states may become rightsholders of Copyright when databases are created in the regime of employee's works or commissioned works.

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 not matching legal requirements for Copyright protection. Databases protected only by the sui generis right can be designed by natural persons under various agreements. Such agreements are for example commission agreements, where exercising of the sui generis right is preserved contractually for the maker of database.

The contents of both types of databases can be various data – traffic data or information on paintings/songs/novels protected by Copyright. If there is chance that these data can be related somehow to third parties, the rule of no prejudice to rights of third parties applies here if contents of databases are subjects of Copyright protection or other rights of third parties.

According to biding law, Member states can hold Copyright or the sui generis right to databases. According to art. 7 sec. 1 of the Directive, makers have the right to prevent unlawful use of database in the form of extraction and/or re-utilization. According to art. 7 sec. 2 of the Directive, extraction means the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form. Re-utilization means any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The same article also covers the exhaustion of the right to the first sale of a copy of a database in EU. Through this right under art. 7 of the Directive makers can exercise their power over the use of databases. Makers are entitled to use databases and decide who and how can use these databases with the consent. According to art.7 sec. 3 this right may be transferred, assigned or granted under contractual licence. The use through licences represents a standard tool to financially profit from databases. Licencing databases consisting of data such as weather or traffic data, data on average wages, data publicly accessible and not personal, is standard process with less issues, because there are no rights of third parties to data involved.

Licensing rights to personal databases gets bit trickier because data subjects which provided data to the controller and maker at the same time, hold special rights to their personal data in databases produced by Member states. Within such databases, Member states are rightsholders of Copyright and/or makers of databases under the Directive and controllers under GDPR, therefore they must abide two different legislations.

The same subject must abide two different rules that may conflict. Member states can process personal data of citizens for specific lawful bases in article 6 of GDPR. The specific lawful bases used by Member states[37] do not contain licencing of personal data for any reason. Therefore, if Member states would like to licence personal databases, they can license it only under different lawful bases, which do exist at the moment, not under the original lawful basis used for processing personal data. On the contrary, Member states can licence databases without personal data, consisting of data where no rights of third parties are involved (for example weather/traffic data or other type of publicly accessible data for free use), freely without consents of third parties.

6. RIGHTS OF CITIZENS TO PERSONAL DATABASES

EU citizens as data subjects possess rights under GDPR over their data in databases. Citizens do not hold Copyright and/or the sui generis to personal databases, because they did not participate on creation of it in the sense of legal requirements by Copyright or the sui generis right in order to be qualified as authors/rightsholders or makers.

Even though, data subjects are not entitled to Intellectual Property rights to databases, they hold different rights – rights of third parties on contents of databases. These contents are personal data of citizens. Citizens provide personal data to Member states in the positions of data subjects, therefore they can exercise data subject's rights towards their personal data. GDPR recognises wide set of rights in the chapter III of GDPR.[38] The wide set of rights can be exercised by data subjects whether data are organized in database or not.[39] The organisation of data in the form of databases do not create any barrier for data subjects to assert their rights under GDPR. The fact that data are organised into databases do not influence exercising of data subject's rights. When a member state builds personal databases and data were processed on the legal base 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), data subjects who provided data are entitled to exercise rights. A data subject can ask the controller to access data in database or rectify it.

[37] See chapter 4. of this article.

[38] The 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. Alongside these rights, data subjects have the right to withdraw a consent to processing at 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.

[39] How to exercise the right to be forgotten is explained in ANDRAŠKO, J., DAŇKO, M. Right to be forgotten. In: L. Piechowiczová – L. Madleňáková (eds.). *Autonomie jednotlivce*. Praha: Leges, 2014, pp. 282–290. In: *https://pf2016.upol.cz* [2022-03-31]. Available at: <https://pf2016.upol.cz/fileadmin/userdata/PF/Veda_a_vyzkum/konference/odmp/ODMP_2014.pdf>.

7. WILL PSEUDONYMIZATION AND ANONYMIZATION ALLOW MEMBER STATES TO REAP FINANCIAL GAINS FROM PERSONAL DATABASES?

GDPR prescribes Member states to process personal data only on the legal bases for which data were originally processed. We assume that these bases are mainly legal obligations, protection of vital interests, the performance of a task carried out in the public interest, or the exercise of official authority vested in the controller. The consent of a data subject seems to be available as well, the following chapter is analysing the position of consent within the commercial use of personal databases.

As anyone can notice, the commercial use of databases by its nature simply cannot be subsumed as a part of legal obligations that Member states are bound to undergo in relation to citizens or other Member states. The legal obligation of commercial database use sounds under actual legal conditions very controversial or can be harmful to fundamental freedoms and rights of data subjects. Only the profound legal change would help to implement such obligation into legal system of EU. We can safely conclude that implementation of legal obligation of commercial database use[40] is very distant at the moment. At the same time, it is not possible to include the commercial use of databases in public interest. The reason is safety of data. The data are confidential by its virtue and were provided by data subjects under the presumed safety measures applied by Member states. Moreover, Member states are legally required to protect data from any danger or harm, therefore we can imply that, it is not in the public interest to share personal data with third parties for purposes of financial profit of Member states. Apart from lacking legal legitimacy of such use by third parties, there are practical reasons for outlawing sharing personal data with third parties. The reasons disqualifying such use are missing appropriate safeguards from third parties against the abuse of personal data and dubious guarantee of adherence to safeguards by third parties. Finally, we may only imagine the creation of an official authority for monetization of databases at this time because no state recognises such official body for commercialization of databases consisting of personal data. These hypothetical solutions for lawful use of personal data (the legal obligation of commercial database use, the commercial use of databases is in public interest and official authority for commercial database use) for financial benefit of Member states, therefore for financial benefit of us, citizens, cannot be absolutely overlooked. Member states might consider such possibilities in the future within the Digital Single Market.

Presently, we are forced to abandon the commercial use of personal databases based on legal bases under GDPR. When Member states are not allowed to use personal data in databases commercially under existing legal bases in art. 6 of GDPR, we tend to conclude that there is no possibility of such use. Surprisingly, there may be viable solutions. These solutions may be data anonymization and pseudonymization. According to recital No. 28 of GDPR, the application of pseudonymization[41] to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-pro-

[40] The commercial use of database consisting of personal data only.

[41] More on pseudonymised data in HINTZE, M. Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*. 2017, Vol. 7, No. 1, pp. 86–101.

tection obligations. If Member states would pseudonymize data in personal databases, licencing of such databases to third parties while adhering GDPR provisions might be possible. At the same time, Member states would only reduce the risks for rights and freedoms of data subjects, because the real threat of unauthorised reversal of pseudonymization[42] is present.

Due to the danger of unauthorised reversal of pseudonymization, the most attainable solving for commercial use of personal databases seems anonymization[43]. Recital No. 26 of GDPR gives us way out from this almost impossible situation of the commercial use of personal databases. The recital reads that 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. Hence, GDPR does not concern the processing and any use of anonymous data, including for statistical or research purposes. Clearly, anonymized personal databases might be licenced by Member states to countless private companies. The result of such wide licencing might reflect in better public services across EU due to higher financial resources stemming from it. In times of Covid-19 and financial struggles in the whole world, additional source in Member state's budgets is welcomed. While the use of anonymised personal databases seems easy, we must not forget to mention risks. When for example, data related to health of citizens of certain region are being processed, these citizens might be identifiable even through anonymised data. Hypothetically, when you have a small village with few dozens of citizens and enough data such as gender, age, ethnicity, and health information, one can identify these persons.[44] It brings not only safety risk for these persons, it also could mean that that information become personal, therefore GDPR is applicable here. The possibility of such situation exists, but it could be avoided by Member states not providing personal databases focusing on small portion of citizens, groups, or specific regions.

8. THE CONSENT

The consent of data subject might come across as the most convenient solution for commercial use of personal databases by Member states. According to recital 43 of GDPR, to ensure that consent is freely given, consent should not provide a valid legal ground for

[42] 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 process is offered in the guidelines produced by The European Union Agency for Cybersecurity from November 2019 with the title „Pseudonymisation techniques and best practices". In: *European Union Agency for Cybersecurity* [online]. 2022 [2022-03-31]. Available at: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.

[43] More on anonymization in FINCK, M., PALLAS, F. They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law.* 2020, Vol. 10, No.1, pp. 11–36.

[44] New study found that any database containing 15 pieces of demographic data could be used to identify individuals. LEMOS, R. Companies Anonymized Data May Violate GDPR, Privacy Regs. In: *Dark reading* [online]. 26. 7. 2019 [2022-03-31]. Available at: <https://www.darkreading.com/endpoint/privacy/companies-anonymized-data-may-violate-gdpr-privacy-regs/d/d-id/1335361>.

the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority, and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. According to the European Data Protection Board (further as "EDPB" only),[45] "recital 43 clearly indicates that it is unlikely that public authorities can rely on consent for processing as whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities.[46] Without prejudice to these general considerations, the use of consent as a lawful basis for data processing by public authorities is not totally excluded under the legal framework of the GDPR."[47] In Guidelines 05/2020 on consent under Regulation 2016/679,[48] the EDPB presents three examples of the consent given to a public authority, but any of them is the commercial use of database. Those examples cover processing of data based on citizens' consent in cases such as road maintenance works to receive updates on the progress of the works or students' consent to use their photographs in a printed student's magazine. Although there is a one example of merging data of citizens into a shared database used by two public bodies,[49] the merger of two databases is to avoid duplicate procedures and correspondence, therefore for the improvement of public services, not for the financial gain of Member states.

CONCLUSION

Proposing the commercial usage of personal data processed by EU governments is undoubtedly uncharted territory. There is no confusion about the fact, that GDPR does not provide legal basis of processing personal data for commercial purposes in the form of databases created by EU governments. "On the other hand, EU Privacy Laws allow data

[45] The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities.

[46] See Article 6 GDPR, notably paragraphs (1c) and (1e).

[47] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020. In: *European Data Protection Board* [online]. 2022 [2022-03-31]. Available at: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

[48] Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020. In: *European Data Protection Board* [online]. 2022 [2022-03-31]. Available at: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>.

[49] An individual who owns land needs certain permits from both her local municipality and from the provincial government under which the municipality resides. Both public bodies require the same information for issuing their permit but are not accessing each other's databases. Therefore, both ask for the same information and the landowner sends out her details to both public bodies. The municipality and the provincial authority ask for her consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies ensure that this is optional and that the permit requests will still be processed separately if she decides not to consent to the merger of her data. The landowner is able to give consent to the authorities for the purpose of merging the files freely.

controllers to exploit personal data for commercial purposes. If all data protection requirements are met (and subject to an accountability principle), data controllers have exploitation rights in those data."[50] Making use of personal data for commercial purposes by controllers is not frowned upon when controllers are private companies conducting business activities and can rely on legal bases. These legal bases can be processing for the purposes of the legitimate interests pursued by the controller or by a third party[51] (such as direct marketing according to recital 47 of GDPR) and the consent of data subjects.[52] Private companies are allowed to process personal data for marketing purposes, form it into personal databases and licence it to a third party. Member states are not legally equipped to do it the same way due to safety reasons and original purpose of processing, for example the performance of a task carried out in the public interest. Also, the consent of a data subject is not the ideal legal base for commercial use of personal databases by Member states. Therefore, only feasible way of financially benefiting from personal databases created by Member states through licencing while maintaining safety requirements and binding EU data protection law requirements is to anonymise personal databases. Anonymization would render some financial benefits and would keep fundamental rights and freedoms untouched. Anonymization techniques give private companies enormous advantages in commercializing personal data,[53] while Member states lack behind. Underlying question is whether Member states should leave this opportunity solely in hands of big technology companies already using personal databases for marketing purposes or anonymized databases. The answer is that Member states might attempt to licence certain anonymized personal databases for welfare of society such as vaccine research by private companies. The question of setting appropriate legislative for the commercial use of personal databases by Member states is still open.

[50] GERMANY. *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* [online]. BANTERLE, F. *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis.* p.19.

[51] Art. 6 sec. 1 sub. f) of GDPR.

[52] Art. 6 sec. 1 sub. a) of GDPR.

[53] There is flourishing market for anonymization companies. 5 Top Emerging Data Anonymization Startups. In: *StartUs Insights.* [online]. 2022 [2022-03-31]. Available at: <https://www.startus-insights.com/innovators-guide/5-top-emerging-data-anonymization-startups/>.