EASTERN EUROPEAN JOURNAL OF TRANSNATIONAL RELATIONS

Creating Innovations within the Framework of Scientific and Industrial Consortia and Compliance with Data Protection Obligations

Katarzyna Siemion
Department of Intellectual Property Law,
Faculty of Law, University of Białystok, Poland
k.siemion@uwb.edu.pl
ORCID 0000-0003-4758-5512

Abstract. One of the elements of building a competitive advantage is the development of innovations. With this objective in mind, market players cooperate with other businesses, but also with entities in the science sector, including research institutes and universities. One of the instruments used for this purpose is a consortium agreement, Such cooperation requires defining, first of all, issues related to intellectual property rights. Since personal data may be processed as part of such agreements, it is important to bring these processes in line with legal requirements under data protection laws, particularly the GDPR. The article analyzes first of all what personal data processing processes may be applicable in cooperation between science and business in the field of innovation, what roles in terms of personal data protection are played by the various entities and what obligations they entail, what special obligations in terms of personal data protection arise from the establishment of international consortia, including with entities from countries outside the European Economic Area, and are the rules that govern the responsibility of these entities for the fulfillment of their obligations under personal data protection regulations. Alignment of the collaborations carried out by consortium members with applicable legal requirements not only safeguards them legally, but also affects the economic and commercialization potential of the results generated in the course of such collaboration. These entities are thus seen as socially responsible, which fosters trust among science and business partners, public bodies, as well as customers benefiting from the innovations created.

Keywords: personal data, GDPR, innovation, consortium agreement, science and business cooperation.

JEL Classification: K11, O34.

Citation: Siemion, K. (2024). Creating Innovations within the Framework of Scientific and Industrial Consortia and Compliance with Data Protection Obligations. *Eastern European Journal of Transnational Relations*, *8*(1), 71-82. https://doi.org/10.15290/eejtr.2024.08.01.07.

Academic Editor: Magdalena Rutkowska-Sowa

Publisher's Note:

Copyright: © 2024 Author. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY 4.0.) license (https://creativecommons.org/licenses/by/4.0/).

INTRODUCTION

One of the elements of building a competitive advantage in the market is the development of innovations. With this objective in mind, market players cooperate with other businesses, but also with entities in the science sector, including research institutes and universities. This makes it possible to utilize the research infrastructure, but also the human resources that these entities have. One of the legal instruments that may be used in this regard is a consortium agreement. Within the framework of the cooperation thus established, it is possible to apply for funding for specific research and development objectives, including from European funds, and to implement innovation projects jointly. Increasingly, international consortia are also being formed in this area.

The purpose of this paper is to determine what obligations under data protection laws are associated with the establishment of such cooperation by market players, especially in the framework of cooperation within a scientific and industrial consortium.

The paper aims to answer the following questions: 1) Whether and to what extent can personal data be processed as part of ongoing collaborations to develop innovations? 2) In terms of data protection, what are the roles of the various entities collaborating under research and industry consortium agreements, and what responsibilities do they entail? 3) What special obligations in terms of data protection are associated with the establishment of international consortia, including with entities from countries outside the European Union? 4) How are the responsibilities distributed among the various entities participating in scientific and industrial consortia in the context of obligations under data protection laws?

The research hypothesis of the paper is the assumption that in innovation development processes cooperation may be established between entities from the science and business sectors, including under consortium agreements, which may involve the processing of personal data and the requirement for these entities to meet their obligations under data protection regulations taking into account the unique characteristics of these processes.

In order to verify this hypothesis, I will use the dogmatic-legal method to analyze the existing legislation, in particular the provisions of the GDPR and acts of a non-binding nature related to cooperation in the field of innovation among entities from the science and business sectors, in particular under scientific and industrial consortium agreements, as well as the legal provisions on data protection that may apply in these cases. In addition, the jurisprudence in the field of data protection and decisions of supervisory authorities will be analyzed to allow the identification the roles in personal data processing and the principles of liability for violation of the rights and freedoms of data subjects in the development of innovations. By analyzing documents, guidelines, and opinions issued by entities dealing with data protection, it will be possible to identify good practices and guidelines that can help entities in the science and business sectors ensure legal security and proper fulfillment of their obligations under data protection laws.

1. WHAT PERSONAL DATA PROCESSING CAN OCCUR IN THE COOPERATION OF SCIENCE AND BUSINESS IN INNOVATION PROCESSES

The development of innovation is one of the basic aspirations of modern society - innovation helps companies operating in the market and societies develop thanks to the ability to solve major social problems; it also helps individual states succeed, in particular through economic growth and the importance of the states in the international arena. The authorities of the European Union implement the EU's research and technological development policy, which is regulated in Articles 179-189 of the Treaty on the Functioning of the European Union. Currently, the main program implemented in this area is Horizon Europe as part of the new European Research Area. The program is designed to strengthen the importance of research and innovation in supporting and implementing EU policies while addressing global challenges.

Periodic surveys are conducted in Europe on the development of innovation in individual countries. The latest European Innovation Ranking 2024 shows that most EU member states have increased their innovation

performance since 2017, with Denmark, Sweden, Finland, and the Netherlands in the leading positions. However, the most innovative country in Europe is Switzerland (European Innovation Scoreboard, 2024).

Innovation should be understood "a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by the unit (process)" (Guidelines for Collecting, Reporting and Using Data on Innovation).

One of the basic instruments used in the cooperation between science and business in innovation may be a consortium agreement. They allow a consortium to jointly pursue a specific goal (Guarda, 2015, p. 165), specifically research, using the capabilities and technical, organizational, capital, and human resources of the individual consortium members.

Such cooperation makes it possible to implement projects that these entities might not be able to implement on their own. This is particularly important for entities in the science sector, as it is part of the so-called university's third mission, which is to cooperate with the socio-economic environment and develop innovations (see more: Taieb, 2024, p. 147–167; Lavikka at al., 2020, p. 569-586). On the other hand, entities in the business sector can benefit from the professional human resources and research and development infrastructure of scientific institutions. By joining forces, they can obtain more funding to support research and innovation, including from EU programs and funds, by being able to apply for the performance of larger projects.

In consortium agreements, it is fundamental to determine issues relating to intellectual property rights, including the division of rights to intellectual property assets created as a result of the performance of agreement, or licenses to use such rights. It is also important, however, to regulate the principles and scope of the processing of personal data that will be processed as part of such cooperation. Data protection regulations impose certain obligations on data processors. In the case of scientific and industrial consortia, there may be specific processes involved in personal data processing, as well as an impact of other legal obligations imposed on data processors, which affects the roles in which they act in terms of data protection regulations. Conducting innovative processes and carrying out projects and research can also involve greater risks to data protection. Therefore, these entities should pay special attention to the correct design and conduct of the processes under the contracts being carried out, bearing in mind the protection of personal data, because it may be difficult to correctly define the scope of their obligations.

Within the framework of various programs focused on cooperation between the science and business sectors, one can find model consortium agreements that may also include provisions on personal data protection. For example, the Horizon Europe Regulation includes "DESCA - Model Consortium Agreement for Horizon Europe", which provides an example of a consortium agreement and the issues to be addressed in it (DESCA - Model Consortium Agreement for Horizon Europe). In this document, a proposal is made for the regulation of specific data protection responsibilities in the consortium agreement: "where necessary, the Parties shall cooperate in order to enable one another to fulfil legal obligations arising under applicable data protection laws (the 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 relevant national data protection law applicable to said Party) within the scope of the performance and administration of the Project and Consortium Agreement. In particular, the Parties shall, where necessary, conclude a separate data processing, data sharing and/or joint controller agreement before any data processing or data sharing takes place" (DESCA – Model Consortium Agreement for Horizon Europe, p. 16).

The definition of the various roles in personal data processing in scientific and industrial consortia depends on the scope of the cooperation and the extent to which it is carried out, as well as on the activities undertaken by the various entities. As a result, it is difficult to clearly define in advance the data protection issues under the model contracts used for the consortia being formed. It is necessary to determine these issues on a case-by-case basis.

In order to assume that personal data processing will be conducted under a consortium agreement, it is necessary to determine whether the data and information that will be used in the innovation creation and development processes will constitute personal data.

In this regard, reference should be made to the legal definition of personal data contained in the wording of Article 4(1) of the GDPR. Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The definition of personal data processing, on the other hand, is provided in the wording of Article 4 (2) of the GDPR, which states that the term means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As part of cooperation between science and business in the field of innovation, processing of personal data is carried out most often. This may primarily be the case if the product, service, or system to be developed as part of the cooperation is to be used to process personal data. This may involve software, equipment such as medical devices that record images during an examination or data on a patient's health status, or a service the performance of which requires the acquisition and processing of personal data, such as data contained in databases. This may also apply to situations where, although the innovation process does not require the use of personal data, it is necessary to conduct market research and analysis or obtain consumer information to assess the commercialization potential, and to conduct activities during the innovation implementation stage. This may also involve the use of artificial intelligence systems, or their creation, as part of the research conducted. In such a situation, it is necessary to determine whether personal data will be used to produce the results generated by the artificial intelligence system. In this regard, it is worth noting the special obligations related to the use of artificial intelligence systems introduced under the so-called AI Act, which is expected to go into effect in 2026. While it is clear from the provisions of this piece of legislation that data protection issues involving the use of artificial intelligence systems are governed by data protection laws, in particular the GDPR, and the AI Act do not regulate these issues, these two pieces of legislation may overlap in practice. Recital 10 of the AI Act indicates that it is not intended to affect the application of existing European Union law governing the processing of personal data, including the tasks and powers of independent supervisory authorities competent to monitor compliance with these instruments. To the extent that the design, development, or use of AI systems involves the processing of personal data, the AI Act also does not affect the obligations under Union or national law in the area of personal data protection incumbent on suppliers and users of AI systems who act as data controllers or processors. It should also be clarified that data subjects retain all rights and guarantees granted to them under such European Union law, including those related to fully automated decision-making in individual cases, including profiling. The harmonized provisions established by the AI Act that concern the marketing, commissioning, and use of AI systems should facilitate the effective implementation and enable the exercise by data subjects of the rights and other remedies guaranteed under European Union law on the protection of personal data and other fundamental rights. Adapting artificial intelligence systems to comply with the obligations set forth in the GDPR poses a particular challenge for those creating and using such systems (The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, 2020).

In addition, the data of persons performing contracts on behalf of individual consortium members will be increasingly processed, and reporting obligations that will involve the transfer of personal data will be fulfilled.

At the same time, it is worth noting that the scope and nature of the non-disclosure agreements concluded most often in the framework of cooperation between science and business to protect trade secrets are different than those of personal data protection regulations. Protection of confidential information and trade secrets can be broader than protection of personal data. This is because not all confidential information must constitute personal

data. On the other hand, if confidential information is personal data, it may be subject to dual protection: contractual protection under a confidentiality agreement and statutory protection under regulations on the protection of trade secrets (Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure), as well as under personal data protection regulations. Importantly, in order for information to be confidential, the disclosing entity must properly mark it as confidential information or a trade secret. In contrast, in the case of personal data, no action is necessary for it to constitute personal data and be subject to the legal protection under the provisions of the GDPR. Therefore, for personal data, it is essential to regulate its processing and transfer. The regulation of the transmission of confidential information that constitutes a trade secret is not sufficient in this regard.

2. WHO IS WHO IN THE SCIENCE-INDUSTRY CONSORTIUM AGREEMENT IN TERMS OF DATA PROTECTION REGULATIONS

One must bear in mind that a consortium is only an agreement, not a separate legal entity. Consequently, legal personality is vested in the individual members of a consortium, not to the consortium itself. This is important for the issues arising from data protection. Indeed, a consortium is not a separate controller of personal data processed in connection with the performance of the consortium's tasks. The data controller may be one of the consortium members or all consortium members, jointly or independently of each other, may be data controllers.

One of the basic issues that are important in the context of starting and establishing cooperation within science-industry consortia is the determination of the roles of individual consortium members in terms of the application of data protection regulations. The obligations of an entity depend on the role it plays. It is important to determine the actual roles played by the various entities in the processing of personal data. This can sometimes be difficult due to the innovative nature of the project. At the time of conclusion of the agreement, it may not yet be known how the research aimed to create a particular intellectual work will actually proceed and what the final result will be. Entities starting cooperation should discuss in depth the assumptions, goals, and objectives they intend to achieve as early as the time of negotiation and conclusion of the agreement. They must also take into account data protection legislation and the obligations arising from them.

In this regard, the following options can be considered regarding the processing of personal data by consortium members: personal data control or joint personal data control.

2.1. Personal data control

It is necessary to decide which entity will define the purposes and means of personal data processing, and thus will be the data controller. At the same time, the data controller can be either a natural or legal person, a public authority, an organizational unit, or any other entity that makes decisions in the relevant area. The purposes and means of data processing may also be specified in European Union law or the law of a Member State, in which case the EU law or the law of that Member State may designate a data controller, or may indicate specific criteria for its designation (Article 4 (7) of the GDPR). Such a situation applies primarily to the processing of personal data by public sector entities performing tasks specified by law that involve the processing of personal data.

When determining which entity is to be the data controller, it is necessary to answer the questions of why and how personal data will be processed. It is the data controller who should decide on the purpose of personal data processing (Hintze, 2018, p. 2). This purpose may be due to the actual influence of that entity in deciding the purposes of data processing, or it may be due to the legal obligations imposed on that entity (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 12). In the context of cooperation between science and business entities in which they enter into consortium agreements, apply for funding, and perform projects using public money, including from EU funds, the purpose of the agreement and the project may be important, which

may also be an activity carried out in the public interest. Certain reporting obligations may be imposed on these entities, which will also involve the requirement to process certain personal data.

The determination of the means of data processing means that it is up to the entity concerned to decide through which channels, with which systems, or in what form personal data will be processed to the extent necessary to achieve the intended purposes.

When only one member of a consortium decides on the purposes and means of data processing, that entity will become the data controller. This may include situations in which consortium members are responsible for carrying out the various stages of innovation creation and implementation, e.g. an entity from the science sector is fully responsible for the creation of an innovative product and an entity from the business sector is responsible for placing the finished product on the market.

On the other hand, if even these stages are independent of each other, but each involves the processing of the same personal data, there are independent controllers that transfer personal data to each other. In such a situation, personal data will be shared. Consequently, it will be necessary to verify whether there is a legal basis for sharing personal data between these entities. Only then will the sharing be legal due to the fact that sharing is one of the operations performed on personal data. On the other hand, personal data processing is only possible if there is a specific legal basis for it according to the GDPR, i.e. one indicated in Article 6 (1) of the GDPR in the case of so-called ordinary data or in Article 9 (2) of the GDPR in the case of so-called special categories of data (special categories of personal data are data indicating racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership, genetic data, biometric data that can be used to uniquely identify a natural person, and data concerning that person's health, sexuality, or sexual orientation). In practice, data sharing agreements are often concluded between individual data controllers. In such an agreement, it is worth regulating whose and what personal data will be shared, for what purposes and how (e.g., through what communication channels), and on what legal basis. It is also possible to point out the obligations of the data controllers in this regard, in particular the obligation to cooperate with each other and to inform each other of all relevant issues related to the processing of such personal. It is therefore reasonable that either the consortium agreement itself or a separate agreement should regulate the principles of mutual sharing of personal data for purposes related to the performance of a joint research and development project under the consortium agreement entered into by the parties.

2.2. Joint personal data control

If consortium members jointly decide on the purposes and means of data processing, they are joint data controllers. This involves joint data control where more than one entity both determines the purposes and means of personal data processing for specific processing operations and has decisive influence in this regard (Judgment of the CJEU of July 29, 2019 in the case C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV, p. 74). At the same time, however, it should be pointed out that the mere use of the same tools, system, or infrastructure does not always entail the emergence of joint data control. This is because if this data processing is conducted in a disconnected and independent manner, then joint data control is not in place (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 24). Only a joint determination of the means and, at the same time, the purposes of data processing will result in joint data processing.

This can be important wherever consortium members jointly decide to pursue some purpose of data processing in a specific way, such as conducting market research to assess the commercialization potential of the results of the intellectual work produced by the collaboration using their chosen tool, or creating a joint design, device, or service that involves the processing of personal data (Van Vell, 2022, p. 5). At the same time, it is not decisive which of the joint data controllers is the owner or licensee of the particular system or platform used for data processing. Even if the owner is one of the joint data controllers, but they have jointly agreed that the research project will be carried out using this platform and the data entered and processed within the platform will serve a common research

purpose, they will be joint data controllers to that extent (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 25). At the same time, it should be pointed out that the adoption of joint data control does not rule out the possibility that, with respect to certain processes and purposes of processing in relation to the same personal data, the joint controllers will be independent controllers when they perform operations on the data for their own purposes and in the manner they determine.

If a joint data control relationship arises between members of a science-industry consortium, it is necessary for the joint data controllers to make joint arrangements, usually in the form of joint data control agreements (art. 26(1) GDPR).

Such agreements should define the relevant scopes of the responsibility of consortium members regarding the fulfillment of their obligations under data protection regulations. This may include who is responsible for enabling the data subjects whose data is processes as part of the joint data control to exercise their rights, in particular with regard to providing information on the processing of personal data under Articles 13 and 14 of the GDPR, maintaining records related to the processing of data as part of the joint data control, and reporting any personal data security breaches that may occur in the processing of data as part of the joint data control. However, one must bear in mind that the arrangements are to properly reflect the respective responsibilities of the joint data controllers and the relationship between them and the data subjects (Colcell, 2019, p. 1037). Consequently, it is necessary to determine as early as the conclusion of the consortium agreement what data will be processed, in what way, for what purposes, on what terms, and who and to what extent will fulfill the various obligations under the data protection regulations on behalf of the joint data controllers. The arrangements may also indicate a point of contact for the data subjects. It may be helpful to allow these persons to submit their demands to the entity that is responsible under the arrangements. Importantly, however, according to the wording of Article 26 (3) of the GDPR, the data subject may exercise his or her rights under the provisions of the GDPR against any of the controllers. It is pointed out that joint controllers have a certain degree of flexibility in dividing among themselves their responsibilities under data protection regulations. However, they must ensure compliance with those regulations. In making this division, it is worth considering first of all who is competent to perform certain duties and who is really able to perform them effectively (Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 25).

The GDPR regulations do not stipulate the form in which joint arrangements should be made. Consequently, they can be made in any form. For accountability purposes, it is a good idea to make them in writing. In addition, the essential content of the arrangements should be made available to the data subjects whose data will be processed as part of joint data control so that they can have a basic understanding of the terms and extent of the processing of their data, and the entity to which they may submit any claims and demands related to such processing. This makes it necessary to provide these arrangements in a form in which these persons can familiarize themselves with them and return to them at any time.

At the same time, it should be recognized that joint data control should be examined in terms of the actual relations between the various entities within a consortium, and not on the basis of whether the legal obligations imposed by the provisions of the GDPR on the joint data controllers have been fulfilled. The absence of joint arrangements for the joint control of personal data should not rule out the assumption that in certain factual circumstances joint data control is actually in place (Judgment in Case C-683/21, NACIONALINIS VISUOMENĖS SVEIKATOS CENTRAS PRIE SVEIKATOS APSAUGOS MINISTERIJOS v. VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA, p. 46).

The provisions of the GDPR impose certain obligations on personal data controllers and joint controllers. First of all, with regard to compliance with the principles of personal data processing (Article 5 GDPR), realization of the rights of data subjects (Articles 12-22 GDPR), ensuring adequate security of processed personal data (Articles 24 and 32 GDPR, Article 35 GDPR), designing personal data processing processes taking into account the provisions in force in this regard (Article 25 GDPR), regulating the principles of access to personal data by other entities, including so-called "processors" (Article 28-29 GDPR), maintaining adequate documentation on personal data

protection (Article 24 and 32 GDPR, Article 30 GDPR, Article 30 GDPR, Article 35 GDPR). processors (Articles 28-29 GDPR), maintaining adequate documentation regarding the protection of personal data (Article 5(2) GDPR, Article 24(2) GDPR, Article 30 GDPR, Article 33(5) GDPR), appointing a data protection officer in certain cases (Article 37 GDPR), or complying with the rules related to the transfer of personal data to third countries or international organizations (Articles 44-49 GDPR), which will be discussed below.

3. DATA FLOW BETWEEN CONSORTIUM MEMBERS IN INTERNATIONAL CONSORTIUM AGREEMENTS

In connection with the development of international cooperation, especially in the field of innovation and technology development, entities from different countries can enter into science-industrial consortium agreements.

As indicated in Recital 6 of the GDPR, rapid technological advances and globalization have brought new challenges to the protection of personal data. The scale of personal data collection and exchange has increased significantly. Technology enables both private companies and public authorities to use personal data in their operations on an unprecedented scale. Individuals increasingly share their personal information publicly and globally. Technology has transformed the economy and social life and should continue to facilitate the free flow of personal data within the European Union and its transfer to third countries and international organizations, but at the same time it should ensure a high level of personal data protection.

In such a situation, the determination of where these entities are based is of essential importance with regard to the personal data. The provisions of the GDPR apply directly in the European Economic Area, which includes the member states of the European Union, as well as Liechtenstein, Norway, and Iceland. Consequently, entities operating there have an obligation to comply with its provisions, thus ensuring an adequate level of privacy protection for the data subjects whose data they process. Accordingly, the transfer of personal data between those entities is not specifically regulated besides the general obligations under the GDPR. On the other hand, if one of the entities is based outside the EEA, the transfer of personal data is allowed only if the prerequisites of Art. 44-49 of the GDPR are met (See more: Phillips, 2018, p. 575-582).

This may be the case if any of the consortium members is based outside the EEA or if the consortium members use the services of entities based outside the EEA for personal data processing (e.g., using cloud solutions to store personal data, email services, or IT tools and systems for market research and analysis, surveys, etc.).

The general condition that must be met for data transfer to third countries to be permissible is that the transfer of personal data that are being processed or are to be processed after the transfer to a third country may only take place if the controller and the processor (i.e., the entity that processes personal data on behalf of and for the benefit of the personal data controller) meet the conditions set forth in Art. 45-49 of the GDPR, including the conditions for further transfer of data from a third country or by an international organization to another third country or another international organization. This regulation is intended to ensure that the degree of protection for individuals guaranteed by the provisions of the GDPR (Article 44 of the GDPR) is not compromised.

In principle, it is possible to transfer personal data to entities based in countries for which the European Commission determines by decision that the third country, territory, or specific sector within that country ensures an adequate level of protection, taking into account the criteria indicated in Article 45(2) of the GDPR (A list of decisions issued by the European Commission establishing an adequate level of data protection is published at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). In the context of the use of technological tools and solutions, of particular importance is the European Commission's decision regarding the possibility of transferring personal data to entities based in the United States (Juliussen et al., 2023, p. 229) - commercial organizations participating in the EU-US Data Privacy Framework (Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation

(EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework).

In the absence of such a decision, the transfer of personal data is allowed only if adequate safeguards have been put in place and if the rights of data subjects are enforced and effective legal remedies are provided. According to Art. 46 (2) of the GDPR, adequate safeguards can be provided by: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules (personal data protection policies applied by a controller or processor who has an organizational unit in the territory of an EU member state, with a single or multiple transfers of personal data to a controller or processor in one or more third countries within a group of companies or a group of joint ventures, which have been approved by the competent supervisory authority); standard data protection clauses adopted or approved by the European Commission in accordance with the examination procedure referred to in Article 93 (2) of the GDPR (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council); an approved code of conduct pursuant to Article 40 of the GDPR; an approved certification mechanism pursuant to Article 42 of the GDPR; or other legal instruments allowed by the competent supervisory body in accordance with Art. 46 (3) of the GDPR.

On the other hand, in the absence of decisions establishing an adequate level of data protection or in the event of a lack of adequate safeguards, the transfer of personal data to a third country may take place only if one of the prerequisites set forth in Art. 49 of the GDPR is met. This can apply to both one-time and multiple transfers of data, but it is important that these must be exceptions indicated in specific situations and must be interpreted narrowly as an exception to the rule prohibiting transfers to such a third country.

4. RESPONSIBILITY OF CONSORTIUM MEMBERS FOR COMPLIANCE WITH DATA PROTECTION REGULATIONS

The extent of the responsibility for compliance with data protection regulations is primarily depends on the roles each entity plays in the processing of personal data. If one or each of the entities is a separate data controller, they are independently liable to the supervisory authority for non-compliance with data protection regulations and data subjects for violations of their rights and freedoms (see more: Detlev & Hickman, 2019).

The supervisory authority has certain powers, including remedial powers in relation to data controllers and joint data controllers, as set forth in Article 58 of the GDPR. In this regard, special attention should be paid to possibility of imposing administrative fines as specified in Article 83 of the GDPR. They may be imposed on a case-by-case basis, in addition to or instead of the measures mentioned above.

Joint data controllers bear administrative liability for failing to comply with the obligations arising from joint data control, as indicated in Article 26 of the GDPR (Fajgielski, 2022).

In terms of the liability to the data subject, the provisions of the GDPR also allow for asserting the right to compensation by those who have suffered financial or non-financial damage as a result of a data controller's violation of these provisions. It is indicated that this is a special type of non-contractual liability for damages, the emergence of which is subject to the following circumstances: the emergence of damage on the part of the data subject; the violation of the provisions of the GDPR as a harmful event; the occurrence of fault in the violation of the provisions of the GDPR; and the existence of a causal link between the damage and the violation (Zawadzka, 2018).

A harmful event is the processing of personal data in violation of the provisions of the GDPR (Article 82(2) of the GDPR). At the same time, it is presumed that the personal data controller or joint personal data controller acted culpably. This entity is not held liable if it proves that it is not at fault for the event that led to the damage (Judgment of the CJEU of December 21, 2023 in the case ZQ v. MEDIZINISCHER DIENST DER KRANKENVERSICHERUNG NORDRHEIN, KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS). This right has a compensatory function and, as monetary compensation, should make it possible to fully compensate the

damage suffered by the data subject (Judgment of the CJEU of June 20, 2024 in the case JU I SU v. SCALABLE CAPITAL GMBH). However, only establishing a violation of the provisions of the GDPR by the data controller or joint controllers is not in itself sufficient to justify the right to compensation. The data subject must prove the occurrence of a damage caused by this violation, and the damage does not have to reach a certain degree of severity (Judgment of the CJEU of June 20, 2024 in the case AT I BT AGAINST PS GBR AND IN). As pointed out in case law, the mere fact that the data subject fears that some future misuse of his or her personal data or identity theft will occur as a result of the breach is not tantamount to non-financial damage. This damage must be of a real nature (Judgment of the CJEU of January 25, 2024 in the case BL v. MEDIAMARKTSATURN HAGEN-ISERLOHN GMBH, ANCIENNEMENT SATURN ELECTRO-HANDELSGESELLSCHAFT MBH HAGEN).

In the case of joint data controllers, the liability of the entities, as a rule, is joint and several. This is because, according to the wording of Art. 82 (4-5) of the GDPR, if more than one controller is involved in the same processing and the controllers are responsible for the damage caused by the processing, they are jointly and severally liable for the entire damage, so as to ensure that the data subject is actually compensated. On the other hand, if one of the controllers has paid compensation for the entire damage caused, it has the right to demand that the other controllers who participated in the same processing reimburse the portion of the compensation corresponding to the portion of the damage for which they are liable.

It should be emphasized that, as the CJEU pointed out in the judgment in the case C-210/16, the existence of joint liability does not necessarily translate into equal liability for the various entities involved in the processing of personal data. On the contrary, these entities may be involved at different stages of this processing and to different degrees, so that the level of liability of each entity should be assessed taking into account all the relevant circumstances of the case (Judgment of the CJEU of June 5, 2018 in the case C-210/16, UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN v. WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH).

CONCLUSION

The performance of scientific and industrial consortium agreements may involve the processing of personal data, particularly in the creation of products, systems, or services for processing such data, as well as in activities relating to the implementation of innovations, including the study of the commercialization potential. The new challenges also involve the use of artificial intelligence systems in the performance of processes that use personal data. Therefore, it is important to determine what roles consortium members will play in personal data processing. In this regard, the key role is personal data control, when one of the consortium members decides on the purposes and methods of personal data processing. There may also be situations where each consortium member processes personal data on its own, i.e., decides on the purposes and methods of the processing independently of the other members. This constitutes separate personal data control. Transfers of personal data among separate data controllers involve sharing of personal data, which must be done in accordance with the provisions of the GDPR, in particularly with regard to the need to indicate the legal basis for such sharing. If consortium members jointly decide on the purposes and methods of personal data processing, they act as joint data controllers. The role assigned to each entity depends on the need to meet certain obligations under the data protection law.

Attention should be paid to the special obligations that may apply to the formation of international consortia. If such formation involves the transfer of personal data to third countries, it is necessary to regulate the principles and grounds for such transfer of personal data, in accordance with the provisions of Articles 44-49 of the GDPR.

If data processors acting under consortium agreements fail to comply with the obligations imposed on them by the provisions of the GDPR, they are held legally liable. The scope and basis of the liability depends on the roles of the data processors. If only one of them is considered a data controller or each of them is a separate data

controller, they are independently liable to the supervisory authority and to the data subject. On the other hand, if they are joint data controllers, their liability to the supervisory authority depends on the actual distribution of their obligations and their failure to fulfill them, while their liability to the data subject is, in principle, joint and several.

Entities should establish and properly regulate issues related to the protection of personal data as early as at the start of their cooperation and in its course. This is required by applicable laws, but it also contributes to fostering the principles and enhancing the protection of individuals' privacy, which is particularly important in the context of the continuous development of technology and innovation. It is also related to the increasing role of market players in both the public and private sectors in terms of social responsibility and compliance. It can also influence the growth of trust among science and business partners and stakeholders in the processes of the commercialization and development of technologies. As Sheryl Sandberg said, the technology we have makes our lives easier, but what makes our lives meaningful is what we do with that technology (Sandberg, 2018).

ACKNOWLEDGMENS

Publication co-financed by the state budget under the program of the Minister of Education and Science entitled 'Science for Society', project no. nds/548731/2022; amount of co-financing: 425,615 PLN. Total value of the project: 425,615 PLN.

REFERENCES

Colcell, V. (2019). Joint Controller Agreement under GDPR. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 3, 1030-1047. https://doi.org/10.25234/eclic/9043.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), C/2021/3972 (OJ L 199, 7.6.2021), p. 31–61.

Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (notified under document C(2023)4745) (Text with EEA relevance), C/2023/4745 (OJ L 231, 20.9.2023), p. 118–229.

DESCA – Model Consortium Agreement for Horizon Europe, ver. 2.0, February 2024. Accessed August 2, 2024: https://www.desca-agreement.eu/desca-model-consortium-agreement/.

Detlev, G., & Hickman, T. (2019). *Obligations of controllers - Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection* law. https://www.whitecase.com/insight-our-thinking/chapter-10-obligations-controllers-unlocking-eu-general-data-protection.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance) (OJ L 157, 15.6.2016), p. 1–18.

European Commission (2024). *European Innovation Scoreboard.* https://op.europa.eu/en/publication-detail/-/publication/8a4a4a1f-3e68-11ef-ab8f-01aa75ed71a1/language-en/format-PDF/source-search.

European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR adopted on 07.07.2021 r., v. 2.1. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en.

European Parliament (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.* https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530.

European Research Area. https://www.consilium.europa.eu/en/policies/european-research-area/.

Fajgielski, P. (2022). Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [A commentary to Regulation 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). In: *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Komentarz* (2nd ed., art. 26) Warsaw: Lex.pl.

Guarda, P. (2015). Consortium Agreement and Intellectual Property Rights within the European Union Research and Innovation Programme. *European Intellectual Property Review*, 37, 161-171.

Hintze, M. (2018). Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR. *Journal of Internet Law (Wolters Kluwer)*, 1-21. http://dx.doi.org/10.2139/ssrn.3192721.

Horizon Europe Programme. https://www.consilium.europa.eu/en/policies/horizon-europe/.

Judgment in Case C-683/21, NACIONALINIS VISUOMENĖS SVEIKATOS CENTRAS PRIE SVEIKATOS APSAUGOS MINISTERIJOS v. VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA, ECLI:EU:2024:914.

Judgment of the CJEU of December 21, 2023 in the case ZQ v. MEDIZINISCHER DIENST DER KRANKENVERSICHERUNG NORDRHEIN, KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS, C-667/21, www.eur-lex.europa.eu (accessed on August 4, 2024).

Judgment of the CJEU of January 25, 2024 in the case BL v. MEDIAMARKTSATURN HAGEN-ISERLOHN GMBH, ANCIENNEMENT SATURN ELECTRO-HANDELSGESELLSCHAFT MBH HAGEN, C-687/21, www.eur-lex.europa.eu (accessed on August 4, 2024).

Judgment of the CJEU of July 29, 2019 in the case C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV, ECLI:EU:2018:1039.

Judgment of the CJEU of June 20, 2024 in the case AT I BT AGAINST PS GBR AND IN., C-590/22, www.eur-lex.europa.eu (accessed on August 4, 2024).

Judgment of the CJEU of June 20, 2024 in the case JU I SU v. SCALABLE CAPITAL GMBH, C-182/22, www.eur-lex.europa.eu (accessed on August 4, 2024).

Judgment of the CJEU of June 5, 2018 in the case C-210/16, UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN v. WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH, CLI:EU:C:2018:388.

Juliussen, B.A., Kozyri, E., Johansen D., & Rui, J.P. (2023). The third country problem under the GDPR: enhancing protection of data transfers with technology. *International Data Privacy Law*, 13, 225-243. https://doi.org/10.1093/idpl/ipad013.

Lavikka, R., Seppänen, O., Peltokorpi, Lehtovaara, J. (2020). Fostering process innovations in construction through industry–university consortium. *Construction Innovation*, 20(4), 569-586. https://doi.org/10.1108/CI-08-2019-0081.

List of decisions issued by the European Commission establishing an adequate level of data protection. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed on August 3, 2024).

Organisation for Economic Co-operation and Development (2018). Oslo Manual. Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition. https://www.oecd.org/en/publications/oslo-manual-2018_9789264304604-en.html.

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Open access*, 137, 575-582.

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) (OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024, p. 1689.

Sheryl Sandberg at MIT Commencement 2018. https://news.mit.edu/2018/sheryl-sandberg-commencement-address-0608.

Taieb, S.H. (2024). Measuring the third mission of European Universities: A systematic literature review. *Society and Economy*, 2, 147–167. https://doi.org/10.1556/204.2023.00030.

Treaty of March 25, 1957 on the Functioning of the European Union (consolidated Version), OJ C 326/47, 26.10.2012, p. 47-390.

Treaty of March 25, 1957 on the Functioning of the European Union (consolidated Version), OJ C 326/47, 26.10.2012, p. 47-390.

Zawadzka, N. (2018). In: E. Bielak-Jomaa & D. Lubasz (Eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz* (art. 82) [GDPR. General Data Protection Regulation. A commentary]. Warsaw: Lex.pl.