UDC 341.171
– DOI https://doi.org/10.32782/2524-0374/2021-12/110

UK-EU PERSONAL DATA TRANSFERS: PAST, PRESENT AND THE FUTURE

ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ МІЖ СПОЛУЧЕНИМ КОРОЛІВСТВОМ І ЄС: МИНУЛЕ, ТЕПЕРІШНЄ ТА МАЙБУТНЄ

Tsuvina A.A., 4th year student
Personnel Training Institute for the Bodies of Justice of Ukraine of the Yaroslav Mudryi National Law University

The article is devoted to identifying the past, present and future state of UK-EU personal data transfers. The analysis on the basis of temporal development illustrates the change of the regulatory regime in the course of time. The example of the United Kingdom (UK) was chosen to demonstrate the particularities of personal data transfers between the European Union (EU) and third countries. Importantly, UK-EU cross-border transfers may be compared to Ukraine-EU cross-border transfers as Ukraine is also regarded as a third country in the context of Article 25 (1) of the General Data Protection Regulation (EU GDPR).

The analysis of the state of personal data transfers before the UK left the EU refers to the general process of conducting data transfers within the EU on the basis of regulations that are in force in all the Member States of the EU. In contrast, the analysis of the changed regime after Brexit demonstrates which difficulties arise for third countries while conducting personal data transfers with the EU countries, in particular the absence of adequacy decisions and the loss of profit caused by the usage of other alternative mechanisms which enable cross-border data transfers.

The attention in the article is mainly focused on the recent UK adequacy decisions and their effect on the future of data transfers. The analysis of the UK adequacy decisions demonstrates how the latter may be used to regulate cross-border transfers effectively and efficiently. The particularities of the UK's national data protection framework are analyzed to demonstrate which provisions of domestic law may be seen as obstacles to the adequacy decision for the country. Several ideas are put forward on the future state of UK-EU personal data transfers to predict the future tendencies in the regulation of cross-border transfers with the UK. The attention is also paid to the current situation with Ukraine-EU personal data transfers. The future changes in national legislation concerning personal data protection in the country are also mentioned to demonstrate the transformation process and development of new high-quality regulations.

Key words: EU GDPR, UK GDPR, personal data transfers, cross-border personal data transfers, adequacy decision, level of data protection.

Стаття присвячена визначенню минулого, теперішнього та майбутнього станів передачі персональних даних між Сполученим Королівством Великої Британії та Північної Ірландії (далі – Сполучене Королівство) та Європейським Союзом (далі – ЄС). Аналіз на основі часового розвитку ілюструє зміну режиму регулювання з плином часу. Для демонстрації особливостей передачі персональних даних між ЄС і третіми країнами обрано приклад Сполученого Королівства. Важливо, що транскордонна передача даних між Сполученим Королівством і ЄС може бути порівняна з транскордонною передачею даних між Україною та ЄС, оскільки Україна також розглядається як третя країна в контексті статті 25 (1) Загального регламенту про захист даних.

Аналіз стану передачі персональних даних до виходу Сполученого Королівства з ЄС стосується загального процесу здійснення передачі даних усередині ЄС на основі правил, які діють у всіх країнах-учасницях ЄС. На відміну від цього, аналіз зміненого режиму після Brexit показує, які труднощі виникають у третіх країн під час здійснення передачі персональних даних з країнами ЄС, зокрема відсутність рішень щодо адекватності й утрата прибутку, спричинена використанням інших альтернативних механізмів, що дають змогу транскордонну передачу даних.

У статті увага в основному зосереджена на останніх рішеннях щодо адекватності рівня захисту в Сполученому Королівстві та їх впливу на майбутнє передачі даних. Аналіз рішень щодо адекватності показує, як останні можуть бути використані для ефективного регулювання транскордонних переказів. Проаналізовано особливості національної системи захисту даних Сполученого Королівства, щоб продемонструвати, які положення національного законодавства можуть розглядатися як перешкоди для прийняття рішення щодо адекватності для країни. Висувається кілька ідей щодо майбутнього стану передачі персональних даних між Сполученим Королівством і ЄС, щоб передбачити майбутні тенденції в регулюванні транскордонної передачі даних. Також звертається увага на стан передачі персональних даних між Україною та ЄС, можливі майбутні нововведення в національному законодавстві щодо захисту персональних даних.

Ключові слова: Сполучене Королівство, ЄС, транскордонна передача персональних даних, рішення щодо адекватності, рівень захисту персональних даних.

Since the UK left the EU in 2020, the process of conducting personal data transfers has changed significantly. In particular, the UK is regarded as a third country in the context of Article 25 (1) of the EU GDPR. UK-EU transfers, which are now regarded as cross-border personal data transfers, may be conducted only if the UK ensures an adequate level of data protection, namely, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU [1]. The adequacy decisions were adopted by the EU Commission to settle the matter and make the transfers possible and simplified after Brexit. At the same time, two important questions may arise. What is the role of these adequacy decisions? What are the future predictions for personal data transfers between the UK and the EU? In this article several ideas are proposed to give the answers to these questions.

The history of UK-EU personal data transfers should be analyzed in the first place to demonstrate the change of the regulatory regime. To begin with, the UK was a part of the EU for almost fifty years, from 1973 to 2020. In this timeline, the problem of trans-border personal data transfers did not arise for the state as it was one of the Member States of the EU and all the transfers fell under the requirements of regulations that were in force for all the Member States. Specifically, the free flow of data was possible under Article 1 (2) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [2]. In addition, the EU GDPR, which also includes the provisions on the free flow of data within the EU, applied in the UK for almost two years, from 25 May 2018 to 31 January 2020. With the goal of implementing the EU GDPR, the UK adopted the Data Protection Act (DPA 2018), which is still one of the main regulations governing the usage of personal data and the flow of information in the state [3]. The DPA 2018 originally referred to the EU GDPR's most important provisions for the protection of personal data and adopted such main definitions used in the EU GDPR as "personal data", "processing", "data subject", "controller", "processor" etc. Therefore, the original provisions of the DPA 2018 demonstrated the clear intention of the national legislator to implement the EU GDPR into the domestic law of the UK.

The next period in the history of UK-EU personal data transfers was connected with the process of separation

of the UK from the EU. On 23 June 2016, the UK held a referendum on the membership of the EU. The historic decision to leave the EU was reached in that referendum. On 31 January 2020 at midnight, when the Withdrawal Agreement entered into force, the UK left the EU [4]. In the context of data protection, the separation led to the situation where the EU GDPR, the main data privacy regulation throughout the EU, could no longer be applied in the UK. Instead, the UK GDPR was adopted to regulate the questions of personal data protection in the UK [5]. The DPA 2018 was amended to be read in conjunction with the new UK GDPR instead of the EU GDPR. Although mentioned regulations have much in common, there is one important distinguishing feature of the UK data protection framework. In particular, according to the UK GDPR and the DPA 2018 the Information Commissioner is the leading supervisor, regulator and enforcer of the UK GDPR [6, p. 1]. The latest suggestions of the UK Government, which concern the Information Commissioner Office's (ICO) restructuring, deserve special attention in that regard. The government proposed to establish an independent board and a chief executive officer at the ICO. The board would be led by a chair with non-executive directors, while the chief executive officer would have responsibility for the running of the organization. The structural improvements were introduced to make the work of the supervisory authority more effective in the long term [7, p. 123–124].

On 1 January 2021 came into force the EU-UK Trade and Cooperation Agreement (TCA), according to Article 201 (1) of which the EU and the UK were committed to ensuring cross-border data flows to facilitate trade in the digital economy [8]. In addition, in Article 525 (1) of the TCA was once again mentioned that onward transfers to a third country are allowed only subject to conditions and safeguards appropriate to the transfer ensuring that the level of protection is not undermined. Under the TCA, the EU and the UK also agreed on the interim solution (bridging mechanism) to ensure the provisional continuation of personal data flow from the EU to the UK. In general, The TCA may be seen as the first step in the regulation of cross-border personal data transfers which was taken before the UK adequacy decisions were adopted in June 2021. The inclusion of the provisions on cross-border data flows helped to cut the loss of profits in the business sector and postpone the question for several months.

The current state of UK-EU personal data transfers is connected with the decisions of the EU Commission on the UK's adequacy under the EU GDPR and Law Enforcement Directive (LED) [9]. In both decisions, the EU Commission stated that the UK ensures an adequate level of protection in the context of Article 25 (1) of the EU GDPR. This means that most data can continue to flow from the EU without the need for additional safeguards. At the same time, the so-called "sunset clause", which means that the UK adequacy decisions are limited to four years and will not be automatically renewed, was developed by the EU Commission. The new adequacy process will be required to determine whether the UK still ensures the essentially equivalent level of data protection in June 2025. In addition, during the four-year period the EU Commission can amend, suspend, or repeal the adopted decisions if issues related to the data protection that call into question the level of protection arise. There is also a possibility for the Court of Justice of the European Union to decide on the data protection level in the case an EU data subject or an EU data protection authority challenges these decisions.

In fact, although the value of positive adequacy decisions in allowing personal data to be transferred without any additional safeguards between the UK and the EU cannot be denied, they are just one of mechanisms to enable such cross-border data transfers. To support trusted data flows across the world such alternative mechanisms as Standard Contractual Clauses (SCCs) are readily available, flexible and straightforward to implement [10]. However, a recent study estimated the costs of the absence of the UK adequacy decisions at around GB £1-1.6 billion (€1.116–1.7856 billion) for UK firms, stemming largely from companies reverting to alternative transfer mechanisms under the EU GDPR [11, p. 1]. Therefore, the adequacy decisions may be considered in practice as one of the most effective tools to regulate cross-border data transfers compared to other alternatives. This explains the desire of the UK national authorities to get the positive adequacy decision despite all the doubts concerning the UK's relevant legislation, including those concerning public security, defence, national security, criminal law and the access of public authorities to personal data.

Specifically, according to some studies, UK surveillance activities do not fully comply with EU data protection and privacy standards. For instance, the UK Government Communications Headquarters (GCHQ) intercepts, retains and analyses masses of personal data by collaborating with or compelling private actors to provide access points. As Hendrik Mildebrath mentioned in the recent in-depth analysis for the European Parliamentary Research Service, the algorithmic detection used in the UK causes three main problems, namely the mathematically unavoidable fact of a large number of false positives or false negatives when searching for rare instances in large data sets ("base-rate fallacy"), built-in biases and opaque processing ("black box phenomenon") [11, p. 15–17]. In addition, the Investigatory Powers Act does not require the Investigatory Powers Commissioner to disclose intrusive data processing to the data subject, even where it would not jeopardize intelligence activities. So, these examples demonstrate the drawbacks in the regulation which confirm that the level of data protection in the UK may be seen as not essentially equivalent to that within the EU. Nevertheless, these particularities did not preclude the adoption of the adequacy decisions for the UK which include, inter alia, some rules on the usage of personal data by public authorities, notably for national security reasons. Furthermore, the adequacy decisions seem to be adopted on the basis of trustworthy relationships between the UK and the EU, taking into account their common historical background. As it was said in one of the recent official documents of the UK government, new arrangements to govern the continued free flow of personal data between the EU and the UK were needed as "part of the new, deep and special partnership" [12, p. 2].

In the context of the future of UK-EU data flows several ideas should be highlighted. Firstly, the adequacy decisions seem to be an interim arrangement designed to make cross-border data transfers possible in the short term. As it was already mentioned, they may be amended, suspended and repealed. Secondly, the new adequacy decisions are highly questionable. It is still possible that the EU Commission will not adopt a new adequacy decision unless already mentioned issues of national security and surveillance regime will not be addressed by the government. Another challenge in this context is the intention of the UK government to allow free cross-border data transfers with other states all over the world. Such a decision of the UK government may cause harm to the EU data protection system as the majority of mentioned states do not have the adequacy decisions. This may be seen as a gap in the closed system which is constructed within the countries that have the adequacy decisions and aims at the highest possible level of data protection among these third countries.

The current situation with UK-EU personal data transfers may be compared to the situation with Ukraine-EU personal data transfers. Although Ukraine has signed the Association Agreement with the EU and its Member States, it is still on the way to the membership in the EU. As a result, Ukraine as well as the UK is regarded as a third country in the context of Article 25 (1) of the EU GDPR. However, unlike in the UK, the cross-border transfers with the EU are now possible for Ukraine only based on the mechanisms that are alternative to

adequacy decisions. This means that the range of tools which are available for Ukraine is quite wide. At the same time, one of the most effective tools – the adequacy decision – is still not available for the country. In this context the perspective changes in the data protection framework of Ukraine should be mentioned to demonstrate the intention of the national legislator to reach in Ukraine the level of data protection which is essentially equivalent to that guaranteed within the EU. For instance, under Article 15 of the above-mentioned Association Agreement Ukraine and the EU agreed to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards [13]. To bring the data protection system in Ukraine closer to the EU GDPR standards, a draft law "On Personal Data Protection" was registered in the Parliament in June 2021 [14]. In addition, a draft law on the establishment of a new data protection authority in Ukraine, the National Commission on Personal Data Protection and Access to Public Information, was registered in the Parliament in October 2021 [15]. Thus, the development of new domestic regulations as part of the data protection reform shows that Ukraine is getting closer to the European standards of data protection. At the same time, much has to be done to reach an adequate level of data protection which may be observed today in some third countries, in the UK in particular.

So, the history of UK-EU data transfers demonstrates that for a long time the regulatory regime stayed unchanged. As a Member State of the EU, the UK could count on the provisions on the free flow of data within the EU. After the separation from the EU, the TCA was adopted to make the transfers possible before the adoption of the adequacy decisions. Although the adequacy decisions were finally adopted by the EU Commission, the fact that some issues in the UK data protection framework are still visible today may not be neglected. This leads to uncertainty with regard to both already adopted and future adequacy decisions. However, the government still has four years to find the solution to the problem and improve the national strategy on how to keep the level of data protection in the state at the necessary level, namely, at the level that is essentially equivalent to that guaranteed within the EU.

REFERENCES

1. 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) / EUR-Lex. *Official Journal of the European Union*. L 119/1. 04.05.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed: 12.12.2021).
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data/ EUR-Lex. *Official Journal of the European Union*. L 281. 23.11.1995. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046 (accessed: 12.12.2021).
3. Data Protection Act 2018 / UK Legislation. The National Archives on behalf of HM Government. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed: 12.12.2021).
4. Brexit: EU-UK relationship / The official website of the European Union. URL: https://eur-lex.europa.eu/content/news/Brexit-UK-withdrawal-from-the-eu.html (accessed: 12.12.2021).
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 / UK Legislation. The National Archives on behalf of HM Government. URL: https://www.legislation.gov.uk/eur/2016/679/contents (accessed: 12.12.2021).
6. Data Protection Act 2018 Factsheet – The Information Commissioner and Enforcement / The Government of the United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). 2018. 4 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711238/2018-05-23_Factsheet_5_-_Information_Commissioner.pdf (accessed: 12.12.2021).
7. Data: a new direction / The Government of the United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). 2021. 146 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf (accessed: 12.12.2021).
8. Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part / EUR-Lex. *Official Journal of the European Union*. L 149/10. 30.04.2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22021A0430(01)&from=EN (accessed: 12.12.2021).
9. Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Unite Kingdom / The official website of the European Commission. URL: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en (accessed: 12.12.2021).
10. UK Business Data Survey 2020 / The Government of the United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). URL: https://www.gov.uk/government/statistics/uk-business-data-survey-2020/uk-business-data-survey-2020#chap6 (accessed: 12.12.2021).
11. Hendrik Mildebrath. European Parliamentary Research Service (EPRS). EU-UK private-sector data flows after Brexit. Settling on adequacy. April 2021. 34 p. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690536/EPRS_IDA(2021)690536_EN.pdf (accessed: 12.12.2021).
12. The exchange and protection of personal data: a future partnership paper / The Government of the United Kingdom. 13 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf (accessed: 12.12.2021).
13. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part / EUR-Lex. *Official Journal of the European Union*. L 161/3. 29.05.2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22014A0529(01)&from=EN (accessed: 12.12.2021).
14. Про захист персональних даних : Проект Закону України від 7 червня 2021 р. № 5628 / *Верховна Рада України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 (дата звернення: 12.12.2021).
15. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації : Проект Закону України від 18 жовтня 2021 р. № 6177 / *Верховна Рада України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992 (дата звернення: 12.12.2021).