Stoilova, Veronika

Article

Regulation of international data transfers under EU data protection law

CES Working Papers

Provided in Cooperation with:
Centre for European Studies, Alexandru Ioan Cuza University

Suggested Citation: Stoilova, Veronika (2021) : Regulation of international data transfers under EU data protection law, CES Working Papers, ISSN 2067-7693, Alexandru Ioan Cuza University of Iasi, Centre for European Studies, Iasi, Vol. 13, Iss. 1, pp. 1-16

Regulation of international data transfers under EU data protection law

Veronika STOILOVA*

Abstract

This study seeks to identify the specifics of personal data protection in the context of EU legislation. The focus is on the personal data transferred outside the Union. It is described how the EU data protection law provides specific measures in order to ensure the protection of individuals and legal persons from malicious acts. The article also highlights the reform of the EU data protection legislation in the context of the reliability of the data transfer mechanisms to third countries. The legal regulation in this matter goes through various stages of development, and the latter one includes the implementation of rules with a focus on ensuring greater data sharing between institutions and companies. The analysis of the international data flows as a priority topic in relations between the EU and countries outside its borders, including international organizations, also find its place in the study. In this sense, transfers to specific sectors based on specific international agreements will be considered in connection with the improvement and strengthening of the existing procedures for international data transfer.

Keywords: international data transfer, data protection, European Union, legislation reform

Introduction

We live in an age dominated by technology and innovation. The development of digital technologies and their penetration into all spheres of economic and social life necessitates a global need to rethink the approach to the sharing, dissemination and protection of personal data. On the one hand, with the growing number of digital services and risk levels, strengthening trust and security in the use of information and communication technologies is the basis for economic growth and prosperity. On the other hand, protecting the interests of the individual from the use of their data is another important point that should not be overlooked.

In today's digital reality, the collection and storage of personal data have its significance (European Commission, 2020a). Companies in all areas of social and professional real and virtual life - for example, utilities, banks, insurance companies, Internet pages, internet trade stores, social networks, digital media, computer programs, mobile applications and more, use digital personal data.

*Veronika STOILOVA is PhD is Chief Assist Professor at South-West University "Neofit Rilski" – Blagoevgrad, Bulgaria, e-mail: veronikabg@gmail.com.

Data transfer has never been easier because the digital space knows no boundaries. This could also be considered as one of the reasons for the search for and introduction of regulatory mechanisms to ensure the protection of individuals and legal entities from malicious actions. In the context of globalization, the transfer of data to third countries is gradually becoming part of everyday life and leads to the consideration of additional measures to protect European citizens from violating their rights. This requires compliance with certain principles such as legality, fairness, transparency, confidentiality of access and storage of personal data.

The processing of personal data acquires new dimensions in connection with the deepening of integration processes worldwide. An example in this respect are the international companies, for the smooth operation and development of which the exchange of data, including that of personal data, is of particular importance. In today's world, the place and role of multinational companies and corporations are undoubtedly key. It is they who initiate the search for the most favorable places in the world, where the legislation on data storage and processing, including personal data, is most advantageous from the point of view of the interests of the respective companies. In this sense, despite the numerous debates "for" and "against" free data transfers within international companies, the process could be defined as normal and even daily, as it is regulated and subject to control under current legislation in the field of personal data in different countries around the world.

Despite the conflicting opinions of various human rights experts on the protection of the interests of the individual against the use of their data, international companies are controllers of personal data and should align their data processing activities with each of the different national legislation of the countries in which they operate. Within the EU, the Union legislation guarantees the free movement of data and harmonization of rules in each of the Member States. Under these rules, there is at least one independent data protection authority in each EU country that oversees the lawful processing of personal data in respect of international companies.

Of interest are those companies that have organized their activities not only in the EU but also in third countries. It is wrong to assume that there are no rules for the processing of personal data in such an international environment. On the contrary, efforts are being made to continuously improve them so that they can follow the rapidly evolving processes of globalization. In carrying out its activities, an international company inevitably reaches the exchange of information containing personal data in one form or another. The reasons and mechanisms for this exchange can be of different nature. Data transfer is usually done either within multinational companies (between headquarters and branches) or between different international companies in order to globalize data flows, reduce costs or under an outsourcing contract. Under an outsourcing contract, the transfer of

data from an entirely European company as a controller of personal data to a processor of personal data in a third country is not excluded.

In the context of European legislation, personal data and their protection take on a specific dimension. The legal regulation in this matter goes through various stages of development, and the latter one includes the implementation of a reform with a focus on ensuring greater data sharing between institutions and companies. In this context, it should be noted that EU regulatory mechanisms outline stronger European and weaker national jurisdiction over data generated by users of member states to ensure that the privacy, dignity and fundamental rights of individuals are respected (Official Journal, 2012), such as the right to privacy.

1. Personal data protection in the context of EU legislation

The protection of personal data and respect for the right to privacy are part of the fundamental rights that everyone is born with. In this context, it is important to emphasize the need to strike a balance between the digitalization of everyday life, the security of the individual and the protection of human rights by preserving the inviolability of personal data and privacy. EU rules for the legal regulation of this fragile issue entered into force in May 2018 (European Council, Council of the European Union, 2020). After that date, the introduced legislative restrictions set a clear line between the technologically possible and the legally and morally correct.

Legal regulation concerning the protection of personal data at the EU level is contained in Article 16 of the Treaty on the Functioning of the European Union and Articles 7 and 8 of the EU Charter of Fundamental Rights (European Parliament, 2020). This is the basis on which the EU stands to ensure that the personal data of European citizens will be protected in the implementation of European policies, including law enforcement and crime prevention (Belova and Georgieva, 2017, pp. 144 – 149), as well as in international relations.

The development of technology provides many benefits to people and society, as it improves the quality of life, efficiency, and productivity. On the other hand, there is no denying that progress and the opportunities that come with it create new risks to individual rights. Due to the emerging need for the introduction of special rules to regulate the collection and processing of personal data, a new concept of "personal information privacy", also known as the "right to information self-determination", has emerged.

The protection of personal data in Europe began in the 1970s when some countries (such as France, Germany, the Netherlands, and the United Kingdom) enacted laws at a national level to

control personal data collection processes. Later, various data protection instruments were adopted at the EU level, the most important of which is Directive 95/46 / EC (European Parliament and The Council of European Union, 1995). In this way, the idea of personal data protection has become a legal norm.

In addition, it is important to emphasize that the right to protection of personal data, defined in Art. 8 of the EU Charter of Fundamental Rights should not be seen as an absolute right "but must be seen in relation to its function in society" (CJEU, 2010). Moreover, Art. 52 (1) of the Charter clearly states that:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (Official Journal, 2012).

Given that the protection of personal data is a separate and independent fundamental right in the EU legal order, it should be concluded that any processing of personal data in itself constitutes an interference with that right. In this sense, in order to be defined as lawful, the intervention must explicitly comply with all the conditions listed in Article 52 (1) of the Charter.

Furthermore, in January 2012, the EU initiated its data protection reform. The goal was clearly stated - to prepare Europe for the challenges of the new digital age (European Commission, 2012). The results were there - on 15 December 2015, the European Parliament, the Council and the Commission agreed that new data protection rules are needed and that the attention of the whole of European society should be focused on establishing a modern and harmonized data protection framework across the EU. Thus, following the successful approval of the texts by the three institutions, Regulation (EU) 2016/679 (European Parliament and The Council of European Union, 2016a) entered into force on 24 May 2016 (applicable from 25 May 2018), and Directive (EU) 2016/680 (European Parliament and The Council of European Union, 2016b) entered into force on 5 May 2016 (applicable from 6 May 2018 after EU countries have taken steps to transpose it into their national legislation).

Subsequently, Regulation (EU) 2018/1725 (European Parliament and The Council of European Union, 2018) was adopted, and entered into force on 11 December 2018. It provides opportunities for assessment and management of risks to data protection, privacy and other fundamental rights of individuals in the event of violation found. This can be seen as a step forward in the direction of better protection of the individual and their freedom to decide which personal data to share.

Of course, the introduction of such legislative restrictions at EU level provokes debate in support of or against how personal data is shared, stored and disseminated. For example, large companies, social platforms and service providers argue that real-time data collection, processing and analysis should be controlled by more liberal legislation with fewer restrictions on data transfer, as through greater freedom. Moreover, in terms of access to data, users are offered more advantages such as: 1) quick detection of errors or threats of fraud in the digital space; 2) protection of consumers from abuse (the more information is provided, the more protected it is); 3) creation by the business of effective strategies oriented to the needs of the consumers; 4) better customer service.

Further controversy, especially in the context of the COVID-19 pandemic, is the abuse of privacy and the vast amount of personal data that could be collected by healthcare organizations and disseminated not only in the EU but also worldwide. In support of the free collection of data on the health of individuals, for example, the fact that this prevents catastrophic accidents and saves lives is emphasized.

All these arguments are logical and well founded, but individuals cannot be convinced and reassured about how well the collection and processing of their personal data is handled or presented. In this sense, it can be summarized that at EU level, the security and integrity of personal information and data prevail over the wishes of companies, social platforms and service providers.

The protection of personal data is a cause for great concern among individuals. Their trust in the digital environment remains relatively low precisely because of the uncertain nature of the way and reasons personal information is been collected and disseminated. In this sense, it should be pointed out that the Court of Justice of the European Union 's decisions on providing the permanent protection of personal data are evidence of that the case law in this area is getting better and is being created every day. Governments, corporations and other data-hungry stakeholders need to find solutions that align with the theoretical framework for strong data protection and confidentiality proposed by the Court on the basis of relevant EU legislation (Christakis, 2020). An example of the partial regulation of international transfers of European personal data to third countries, as well as how to avoid further circumvention of GDPR standards, is the judgment of the Court of Justice in Case C 311/18 of 16 July 2020 (CJEU, 2020a). Practice in the application of EU law in the context of privacy and data protection shows the importance of concerted action and, in particular, the introduction of uniform rules for national enforcement and regulation at the EU level.

It should be summarized that today the topic of the development of EU case law is more relevant than ever in the context of the eventful process of reforming European legislation on personal data protection and the growing globalization of this vital resource. Due to the fact that personal data is

increasingly seen as a new type of currency (Angwin and Steel, 2011), the following few questions logically arise: 1) will it be illegal in the near future to use such widespread centralized international databases and human resource management systems, or for management and customer service, which are widely implemented in international corporations; 2) how European companies will be able to use the cloud, hosting or other technology services provided by companies outside the EU, or this will be taboo; 3) will the provision on the European market of some of the most popular online services and platforms among Europeans, such as Facebook, Amazon, LinkedIn, etc., be hindered? These and countless other questions are currently awaiting an answer.

Despite its many benefits, the digital age also poses many challenges to privacy and data protection as vast amounts of personal information are collected and processed in increasingly complex and opaque ways (Belova *et al*., 2017). The development of technology has led to the development of massive data sets that can be easily compared and further analysed in order to search for models or make decisions based on algorithms that can provide an unprecedented view of human behaviour and privacy.

New technologies are powerful tools and can be especially dangerous if they fall into the wrong hands. In 2013, Edward Snowden's revelations about the use of large-scale programs for monitoring the Internet and telephone conversations by intelligence services in some countries raised serious concerns about the dangers of privacy surveillance activities, democratic governance and freedom of expression. Mass surveillance and technologies that enable the global storage and processing of personal information and access to all data at the same time may affect the very nature of the right to privacy (ECHR, 2020). In addition, they can have a negative impact on political culture and have a deterrent effect on democracy, creativity, and innovation. The very fears that the state may constantly monitor and analyse the behaviour and actions of citizens may discourage them from expressing their views on certain issues and lead to mistrust and caution (European Data Protection Supervisor, 2015). These challenges have led a number of public bodies, research centres, and civil society organizations to analyse the potential impacts of new technologies on society. In 2015, the European Data Protection Supervisor launched several initiatives to assess the impact of large data sets and the Internet on morality. In particular, it has set up an Ethics Advisory Group, which aims to promote "an open, informed discussion on the ethics of digital technologies, which will enable the EU to realize the benefits of technology for society and the economy, while strengthening human rights and freedoms, especially the right to privacy and data protection" (European Data Protection Supervisor, 2016). The processing of personal data is also a powerful tool in the hands of corporations. Today, it can disclose detailed information about a person's health or financial situation - information that

corporations use to make important decisions for individuals, such as the health insurance premiums that apply to them or their creditworthiness. Data processing techniques can also have an impact on democratic processes when used by politicians or corporations to influence elections, for example by "micro-targeting" of voters' communications. In other words, although privacy was initially perceived as the right to protection of individuals against unjustified interference by public authorities, in the modern age it may also be threatened by the powers of private entities. This raises questions about the use of technology and predictive analysis in decisions that affect people's daily lives and reinforces the need to ensure that fundamental rights requirements are met in all processing of personal data. Data protection is inextricably linked to technological, social, and political change. That is why the EU must meet modern challenges with adequate legislation so that European citizens' data can be protected and their privacy guaranteed.

2. Reform of the EU data protection legislation

Progress in the technological development of humanity and the processes of globalization have changed the notion of privacy by fundamentally changing the way we collect, make available and use our data. In this sense, 2016 was a key moment in the implementation of the reform of data protection legislation in the EU. Measures to protect against data transfer misuse have been enriched with diversified tools of various mechanisms that create opportunities for relatively secure data transfer to third parties: adequate solutions, common contractual clauses, derogations, mandatory company rules, certification mechanism, codes of conduct, etc. In this sense, it should be noted that, unlike the regime relating to international data transfers established by the provisions of the 1995 Data Protection Directive (European Parliament and The Council of European Union, 1995), the reform of the legislation provides for the creation of better conditions for the use of existing mechanisms, while introducing more convenient and easy to use tools for international transfers, adapted to the new realities of the modern world.

Data is a key element of digital transformation. This is one of the main motives for the EU to focus the key priorities of its legislative reform in relation to data protection in the implementation of international transfers with the adoption of the Strategy for International Data Flows (European Commission, 2017). This approach proposes specific provisions on cross-border data flows and respect for the right to privacy, which should be included as part of international trade negotiations and also in the conclusion of various international agreements (a good example of international

agreements involving the transfer of personal data are Passenger Name Records (PNR) and the Terrorist Finance Tracking Program (TFTP)).

The next step was taken in February 2020 with the formal presentation of the European Data Strategy (European Commission, 2020b), with the EU proposing concrete ideas and actions for digital transformation to make the Union more secure and competitive on a global technological scale. The aim of this strategy is to turn the EU into a role model and leader in a society that, thanks to data, has more room for action. In this sense, it provides for the creation of a single European data space, which could unleash the potential of unused data, thus allowing it to move freely within the European Union to benefit different industries of economics, science and social life.

Until the presentation of the strategy, the EU treats data sharing more as a threat, while the new approach focuses on greater data sharing between institutions and companies. In this sense, there is a stronger European and weaker national jurisdiction over the data, generated by the users of the member states. As a result of such measures, there is a growing consolidation of data across Europe, but as it will be shared on a voluntary basis, the world's largest players, the US and Chinese technology giants, will continue to dominate. The data is a major asset for companies such as Facebook, Google and Amazon, which in recent years have come under strict EU scrutiny over the rules for the protection and storage of European users' personal data. The proposed strategy can be seen as a step forward in Europe's attempts to create its own digital giant.

The development of the idea of clearer rules on the protection of personal data and their transfer outside the EU is becoming increasingly clear with the publication of the Strategy for Union institutions, offices, bodies, and agencies to comply with the “Schrems II” Ruling (European Data Protection Supervisor, 2020). The European Data Protection Supervisor presented it on October 29, 2020, and the reasons for its development include the dissemination of information that the European Parliament's website for the management of COVID-19 tests (European Parliament, n.a.) has been repeatedly attacked in order to track users of the site. Moreover, most of these “trackers” redirect data to various companies located in the United States.

In this sense, the analysis of the objectives of the Strategy shows that the main ambition in its development is to provide more control and guarantees in compliance with the “Schrems II” Ruling by the European institutions. In addition, it should be noted that this strategy is not relevant to corporate organizations or non-EU institutions, but provides valuable information that can be useful to all organizations regarding the views of the European Data Protection Supervisor on the transfer of personal data at the international level.

It is noteworthy that short- and medium-term compliance measures and actions are envisaged, such as the preparation of a Transfer Impact Assessment prepared for each new process of cross-border data transmission to the United States. As elements of the mentioned assessment are added: 1) information on a certain transfer of personal data; 2) information on whether the recipient country provides an equivalent level of protection that meets the conditions set by the EU.

The presentation of a document with such specific content should be seen as confirmation that constructive changes are taking place at the European level with regard to the matter in question. As a positive element, it should be noted the change that has already taken place in connection with the "Schrems II" Ruling regarding the transfer of data to third countries located outside the EU and in particular to the United States. The adequacy of the EU-US Privacy Shield, which currently regulates the cross-border transfer of personal data between the EU and the US, has been called into question (CJEU, 2020b). Moreover, the EUCourt of Justice has argued that: 1) the legislation applicable in the United States allows public institutions to collect and process personal data from the EU, without the existence of appropriate protection measures and guarantees of legality that comply with the data protection criteria set by European legislation; 2) there is no effective means of seeking compensation against the US government from EU data subjects.

In the context of the "Schrems II" Ruling, the European Data Protection Board adds that there is no provision for a "transitional period" in which EU data controllers can transfer data to the United States under the Privacy Shield. As a result, there is a need to seek another legal basis for the protected and controlled transfer of personal data from the EU to the US, which complies with the provisions of the GDPR.

Of course, there are still some possible alternatives for EU data controllers to transfer data to the US, such as standard contractual clauses and binding corporate rules within a common corporate group, approved by at least one European Data Protection Supervisor.

In the context of the reform of the EU data protection legislation analysed above, it should be summarized that the judgment of the Court of Justice in Case C-311/18, "Schrems II" will leave its lasting mark on international trade and relations. The Strategy prepared by the European Data Protection Supervisor clearly outlines the beginning of a new stage in the development of the matter, accompanied by new rules and restrictions. In addition, it is important to emphasize that both the European Data Protection Supervisor and the European Data Protection Board are focusing their efforts on the preparation of additional Guidelines on the lawful transfer of personal data to the United States. On the one hand, it is a process that requires extra attention and time. On the other hand, however, it is imperative to find an appropriate solution to bring current data transmission practices

in third countries into line with the new direction outlined by the Court of Justice and the EU institutions.

3. International data flows

The transfer of personal data outside the EU is part of the day-to-day work of the European institutions. The scope of these activities can be extremely wide and varied in the subject matter. Cloud technology, web-based services, and organized travel outside the Union are just a few examples of this. The international transfer of data from the EU to countries outside the European Economic Area is described in detail in Chapter V (Articles 44 - 50) of EU Regulation 2018/1725. The provisions of the latter determine the framework for transfers of personal data to third countries or international organizations through: 1) transfers based on a decision on adequacy (Article 45); 2) transfers subject to appropriate safeguards (Article 46); 3) binding corporate rules (Article 47); 4) transfers or disclosures not permitted by Union law (Article 48); 5) derogations for specific situations (Article 49) (European Parliament and the Council, 2016a).

Among the priority topics in relations between the EU and countries outside its borders, including international organizations, are those related to the protection of European citizens' personal data (Dimitrov, 2020). In this direction are the actions taken by the Union in connection with the improvement and strengthening of the existing procedures for international data transfer. A good example of this is the existing adequacy procedure, according to which the EU checks whether a particular third country provides an “adequate” level of personal data protection and to what extent it regulates their transfer from the EU to that third country. It is through such measures that a kind of security guarantee is been created that European citizens enjoy the same rights as third-country nationals in the EU when their data is been exported outside the Union. In this context, it is logical for the EU to strive for the same level of protection in its cooperation with third countries, as well as to promote high standards of data protection worldwide.

Another important point is the practice of applying safeguards in connection with the transfer of personal data to the so-called inadequate countries. In this sense, in order for international data transfer to take place in the safest way, the safeguards envisaged should be outlined in the form of a legally binding instrument (e.g. an administrative arrangements or a memorandum of understanding between the transferring party and the recipient) (European Parliament and The Council of European Union, 2016a) as well as to meet certain criteria, such as being processed for a specific purpose and subsequently used only to the extent that this is not incompatible with the purpose of the transfer.

It is possible for personal data to be transferred between different countries in the context of international police and judicial cooperation in accordance with existing international agreements or treaties. In this way, transnational supervisors (e.g. Europol, Eurojust) directly apply data protection principles in the context of their activities.

Examples of agreements reached in connection with the provision of guarantees for the implementation of free and at the same time secure international data flows are: 1) Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (Official Journal, 2016); 2) Agreements between the EU and the US, the EU and Australia and the EU and Canada on Passenger Name Record (PNR); 3) Terrorist Finance Tracking Programme (TFTP) (European Commission, n.a.).

Providing protection for international data transfer outlines several more important challenges that the EU needs to address. The first of them is related to the legality of the collection, processing and storage of personal information. There is no obstacle to data sharing if this happens in accordance with the established rules for respecting the individual's free choice as to what and how much to share. Other challenges facing the EU include data quality, the right of individuals to information on the processing of data before and after the transfer, the rights of access and rectification by individuals, and the processing of special categories of personal data (health, ethnic origin, sexual orientation, etc.) only in specific circumstances. These categories have been formulated over the period of practical implementation of regulatory and safeguard mechanisms by the EU in data management.

Conclusions

Data is at the heart of the digital transformation. Access to ever-increasing arrays of information, as well as the ability to use them, is essential for technological development and innovation. The transfer of personal data to and from countries outside the Union and international organizations are necessary to stimulate international trade and deepen fruitful international cooperation. The increase in these flows triggers new challenges and concerns regarding the protection of personal data.

Uncertainty in data protection often refers to cross-border economic activities in the digital age. This could also be seen as one of the reasons for seeking and introducing regulatory mechanisms to ensure the protection of individuals and legal entities in the EU from malicious activity.

EU regulatory mechanisms do not prohibit data collection. The GDPR itself does not prohibit data processing activities, but instead allows them if certain principles are followed. It does so to ensure that the inviolability, dignity and fundamental rights of individuals, such as the right to privacy, are respected. In this sense, it is important to note that Europe is reaching a consensus and balance on the protection of European citizens' personal data and opportunities for technological development.

The dialogue on regulating and facilitating international data transfer in the context of the European legal framework is still evolving. Challenges related to the protection of individuals and legal entities from malicious actions will also appear in the context of the need to exchange information in the field of health services and research. This is particularly important for Internet services and complex automated data processing, such as the use of decision-making algorithms. In this sense, European legislation on the transfer of personal data should ensure their protection in a transparent, traceable and regulated manner. This creates the conditions for the transfer of personal data between different countries in the context of international police and judicial cooperation in accordance with existing international agreements or treaties. Within the EU, the free movement of data and harmonization of rules in each member state is guaranteed. Under these rules, there is at least one independent data protection authority in each Union country that oversees the lawful processing of personal data in relation to international data transfer.

In our increasingly digitalized world, every activity leaves a digital footprint that can be collected, processed and evaluated, or analysed. With the new information and communication technologies, more and more data are collected and recorded (European Commission, 2014). Until recently, no technology was able to analyse or evaluate data sets or draw useful conclusions. The data were simply too numerous to be evaluated, and too complex, poorly structured, and rapidly evolving to identify certain trends and habits. The international transfer of data took place without hindrance, as a result of which many people suffered precisely because of the violation of their right to privacy.

From the point of view of data protection, the main problems are related, on the one hand, to the volume and variety of personal data processed, and on the other hand, to the processing itself and its results. The introduction of complex algorithms and software to transform information arrays into a resource for decision-making purposes affects individuals and groups in particular, especially in cases of profiling or classification, and ultimately raises many issues related to the protection of the data.

Large data sets and artificial intelligence raise a number of questions about the identification of controllers and processors, as well as their responsibilities: Who owns the data when such a large amount of data is collected and processed? Who is the administrator when machines and software

process data? What are the specific responsibilities of each actor in the processing? In addition, for what purposes can large information arrays be used?

In conclusion, it should be noted that EU regulatory mechanisms mark a new stage in the collection, processing, and free dissemination of data generated by users of Member States to ensure respect for the privacy, dignity, and fundamental rights of individuals, such as the right to of personal life. The case law applied because of the rulings of the Court of Justice in ensuring the lasting protection of personal data is evidence of the growing commitment of Member States in introducing uniform criteria for national application and regulation at the EU level in this sphere. Although EU rules on international data transfer seem complex and difficult to implement, the positives of the GDPR on the rights of European citizens and their protection are yet to be seen.

References

Angwin, J., Steel, E., (2011), Web's Hot New Commodity: Privacy, *The Wall Street Journal*, 28 February (retrieved from https://www.wsj.com/articles/SB100014240527487 03529004576 160764037920274)

Belova, G., Georgieva, G. (2017), A new data protection development in the EU judical and criminal area, *International conference Knowledge-Based Organization*, 23(2), pp. 144 – 149 DOI: https://doi.org/10.1515/kbo-2017-0103.

Belova, G., Marin, N., Georgieva, G, Kochev, Y. (2017), *Novi momenti v zashtitata na lichnite danni v Evropeyskia sayuz. // Nauchni trudove na Instituta za darzhavata i pravoto*, t. XVI, s.56-58.

Christakis, T. (2020), After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe (retrieved from https://europeanlawblog.eu/2020/07/21/ after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/).

CJEU (2010), Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert / Land Hessen [Grand Chamber], 9 November 2010, paragraph 48 (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092).

CJEU (2020a), Judgment of the Court of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18, “Schrems II”) ECLI:EU:C:2020:559.

CJEU (2020b), Court of Justice of the European Union, Press Release No 91/20, Luxembourg, 16 July 2020, Judgment in Case C-311/18, Data Protection Commissioner v Facebook Ireland and

Maximillian Schrems (retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf).

Dimitrov, D. (2021), EU Citizenship Law: Integration of Immigrants, *EURINT Proceedings*, volume 7, pp. 50 - 62.

ECHR (2020), European Court of Human Right's Press Unit, Factsheet – Mass surveillance, October 2020 (retrieved from https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf).

European Commission (2012), Press release: Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25.01.2012 (retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46)

European Commission (2014), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions Towards a thriving data-driven economy, COM/2014/0442 final, 2 July 2014 (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442# document1).

European Commission (2017), Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN).

European Commission (2020a), *White Paper on Artificial Intelligence - A European approach to excellence and trust* COM/2020/65 final (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065).

European Commission (2020b), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data, COM/2020/66 final (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1582551099377&uri=CELEX%3A52020D C0066).

European Commission (n.a.), *Transfer of air passenger name record data and terrorist finance tracking programme* (retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en).

European Council, Council of the European Union (2020), *Data protection in the EU* (retrieved from https://www.consilium.europa.eu/en/policies/data-protection-reform/).

European Data Protection Supervisor (2015), *Opinion 7/2015 Meeting the challenges of big data,* 19 November 2015 (retrieved from https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf).

European Data Protection Supervisor (2016), Decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection ('the Ethics Advisory Group'), *Official Journal*, C 33, 28.1.2016, p. 1–4.

European Data Protection Supervisor (2020), Strategy for Union institutions, offices, bodies and agenciesto comply with the 'Schrems II' Ruling, 29 October 2020 (retrieved from https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_ 0.pdf).

European Parliament (2020), *Fact Sheets on the European Union. Personal data protection* (retrieved from https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection).

European Parliament (n.a.), *European Parliament COVID-19 Test Centre Safety for Everyone: Fast & Reliable* (retrieved from https://europarl.ecocare.center/).

European Parliament and The Council of European Union (1995), 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, *Official Journal*, L 281, 23/11/1995 P. 0031 – 0050 (retrieved from https://eur-lex.europa.eu /LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML).

European Parliament and The Council of European Union (2016a), 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) (Text with EEA relevance), *Official Journal*, L 119, 4.5.2016, p. 1–88.

European Parliament and The Council of European Union (2016b), Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *Official Journal* 119, 4.5.2016, p. 89–131.

European Parliament and The Council of European Union (2018), Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) (retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725).

Official Journal (2012), Charter of Fundamental Rights of the European Union, *Official Journal*, C 326, 26.10.2012, p. 391–407.

Official Journal (2016), Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *Official Journal*, L 336, 10.12.2016, p. 3–13.