Ljubica Pendaroska*

INTERNATIONAL TRANSFER OF PERSONAL DATA BETWEEN THE EU AND COUNTRIES OUTSIDE THE EU

-Abstract-

Since May 2018, the global concept of personal data transfer has seen major changes, driven by the reforms of the EU's Data Protection Legislation, when the new regime of diversified mechanisms for transfer to third countries came into effect. The article aims to give an overview of the European Union's contemporary legal framework and the tools for international data transfer. In addition, the article will briefly present the legal provisions for personal data transfer of some other countries, constructed and further developed under the influence and inspiration of the "almost perfect" EU regulatory solution. The purpose and the main value of the paper is to demonstrate that internationally harmonized mechanisms for transfer of personal data will not hinder, but positively govern the global international exchange, development and cooperation. The value of the article is increased due to the fact that improved mechanisms for international data flow are a relative novelty, and in certain parts of the economically developed world, which will be briefly covered, are in their absolute infancy. The main hypotheses of the paper are based on the following premise: GDPR's data transfer tools are the best mechanisms so far, which tend, with certain improvements in practical implementation, to ensure the full realization of personal data protection right, in case of data flows outside the EU borders, and the legal provisions for personal data transfer of certain foreign countries (Middle East/Gulf Cooperation Council members) are a reflection of the GDPR, thus providing the same level of personal data protection during transfer to those countries. At the same time, the rules are not an obstacle for the smooth running of international business and other types of valuable transactions.

Keywords: Personal data, Transfer mechanisms, GDPR, Middle East

I. INTRODUCTION

"The goal is to turn data into information, and information into insight".[1] But nowadays "Data are becoming the new raw material of business"[2]!

* Ljubica Pendaroska, PhD Candidate, Ss. Cyril and Methodius University Skopje, Iustinianus Primus Faculty of Law Skopje, e-mail: ljubicapendaroska@gmail.com

[1] Carly Fiorina, the former CEO of Hewlett-Packard speech, "Information: the currency of the digital age", Oracle OpenWorld, San Francisco, December 6, 2004.

[2] Craig Mundie, a former Senior Advisor to the CEO at Microsoft.

At a time when accurate and complete information is a key operating factor, the transfer of personal data between institutions within a country, as well as between countries and various regulatory systems, is an indispensable ingredient, especially for the international trade, cooperation and research. With the growing digital economy, electronically stored and transferred data have become an extremely important resource for a large field of economic activity.[3]

The "personal data transfer" concept refers to the secure exchange of information and data files between systems or organizations that simultaneously ensure the data subject's rights are safeguarded when data are transferred outside the subject's country of origin.

Following the trends in data flows and recognizing the increased risks towards transferred personal data, a successful legal system must create a compounded apparatus to manage those risks and complexities involved in cross-border transfers. Although many countries have adopted data protection and privacy laws that regulate the cross-border transfer of personal data in detail,[4] it is evident that the regulations governing data transfers vary between jurisdictions, thus potentially add additional layers of risk to some extent.

The European Union's system for personal data protection is considered as the leader and the strongest pillar in the exercise of this human right in case when personal data are being transferred. Its ultimate value consists in the fact that the system starts from the need not to hinder the free flow of personal data, while, at the same time, special safeguards are foreseen to ensure that the protection travels along the data. In that spirit "Ensuring the data subject's rights are safeguarded when data are transferred outside the EU allows the protection afforded by EU law to follow the personal data originating in the EU".[5]

Two countries from the Middle East are taken into account within the scope of this paper, in line with the latest figures demonstrating that the Gulf Cooperation Council (GCC) countries is the EU's 6th largest export market and an important source and destination of investment for EU Member states. At the same time, the EU is the 2nd biggest trade partner of the GCC, representing 12.3% of the GCC's total trade in goods with the world in 2020. Two-way trade in services between the EU and the GCC in 2019 amounted to €51.7 billion, with EU's imports of services representing €18.0 billion and exports €33.7 billion.[6] Furthermore, the paper considers that international trade flows in services is more touched by the GDPRs transfer mechanisms compared to trade flows in goods, because services are more reliant on personal data.

Globally, many countries, especially those that are considered "economic boomers" follow the example of the EU and its most powerful legal instrument – the General Data Protection Regulation, known as "GDPR", when designing the system and practical tools and mechanisms for international data transfer. Following that spirit, the GDPR will be taken as a central point for elaboration and further comparison.

---

[3] Wolf J. Schunemann, and M. Baumann, *Privacy, Data Protection and Cyber security in Europe, (*Springer, 2016), p. 5.

[4] See Kuner Christopher, *Trans border Data Flows and Data Privacy Law*, (OUP Oxford, 2013).

[5] European Union Agency for Fundamental Rights/Council of Europe*, Handbook on European Data Protection Law*, *2018 Edition,* (European Union Agency for Fundamental Rights/Council of Europe, 2018), p. 250.

[6] More information from the European Commission on: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/gulf-region_en

II. CONTEMPORARY LEGAL FRAMEWORK AND MECHANISMS FOR INTERNATIONAL TRANSFER OF PERSONAL DATA OF THE EUROPEAN UNION

According to the GDPR, when personal data are transferred from the Union to the controllers,[7] processors[8] or other recipients in third countries or to international organizations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organization to controllers, processors in the same or another third country or international organization.[9]

Under the EU law, transfers may take place if the third country ensures an adequate level of protection or if the data controller or processor provides appropriate safeguards, including enforceable data subject rights and legal remedies, through means such as standard data protection clauses or binding corporate rules.[10]

The alternative grounds and mechanisms when a transfer is considered as legal[11] are the: Transfers on the basis of an adequacy decision; Transfers subject to appropriate safeguards; Binding corporate rules; Transfers or disclosures not authorized by Union law.

1. Transfers on the basis of an adequacy decision

In case when a third country provides certain guarantees for personal data which are "essentially equivalent" to those in the European Union, then the European Commission may adopt so called Adequacy decision, and barriers for data transfer to that third country will no longer exist. Such a decision can be, also made for a certain territory of a country or for one or more specific sectors.

The concept "adequate level of protection" grounded with the Directive 95/46,[12] was further expanded with the Court of Justice of the EU Schrems case decision, naming that "while the "level of protection" in the third country must be "essentially equivalent" to that guaranteed in the EU, "the means" to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the [EU]".[13] Both the content of applicable rules to personal data transferred to a third country or an international organization and the system in place for ensuring effectiveness of those rules, are relevant and should be considered when assessing the equivalency of personal data protection.

---

[7] Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[8] Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[9] GDPR, Recital 101 to the Article 44.

[10] European Union Agency for Fundamental Rights/Council of Europe, *Handbook on European Data Protection Law, 2018 Edition*, (European Union Agency for Fundamental Rights/Council of Europe, 2018), p. 253.

[11] Chapter 5 of the Regulation.

[12] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995).

[13] Case C- 362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015 (§§ 73, 74)

The Adequacy decision has inherent value because it is not arbitrary nor politically motivated, but is based on an assessment of the adequacy taking into account the following precisely determined elements or criteria:[14]

- The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- The international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

The procedure for adoption of the Adequacy decision itself, further guarantees the level of data protection, through the following steps: A proposal from the European Commission; an Opinion of the European Data Protection Board, as an independent body; an approval from representatives of EU countries and the adoption of the decision by the European Commission. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay, as providing adequate protection.[15]
The particular mechanism puts emphasis on the specific states' legislation and its internal tools for ensuring the protection of personal data.
In the 2015 Schrems case,[16] the Court of Justice of the European Union declared the European Commission's 2000 decision on the 'adequacy' of the EU-US Safe Harbor[17] regime invalid. One of the main concepts on which the reasoning of the Court relies is the 'equivalence' between the levels of protection existing in a third country, and the European data protection system. The Court invalidated the Safe Harbor Adequacy decision as it did not contain any findings regarding

[14] GDPR, Article 45.
[15] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[16] Schrems v. Irish Data Protection Commissioner, (2015), case asking the Irish data protection authority to suspend data transfers from Facebook Ireland to Facebook Inc. due to his concern that his personal data could be accessed by US intelligence authorities and his data protection rights guaranteed by EU legislation would be violated that way.
[17] The EU-US Safe Harbor agreement between the European and United States, the parties agreed a mechanism which will allow US companies to meet the adequate level of protection required with the EU's data protection rules.

the existence in the USA of laws and practice limiting interference to the right to privacy and data protection (e.g. interference by public authorities for security purposes), nor of effective judicial remedies for individuals. Consequently, the European Commission and the USA negotiated in 2016 a new framework for transatlantic exchange of personal data, known as the Privacy Shield.[18]

But, at the time-period of writing this paper, the EU-US Privacy Shield is no longer in force and the President of US signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities which provides a new framework for legal data transfers between the EU and US. Is this the new era for data transfers "across the ocean"?

2. *Transfers subject to appropriate safeguards*

In case when a data transfer cannot be carried out on the basis of an Adequacy decision, and in order not to prevent the development of activities that depend on the transfer of personal data, the Regulation allows the movement of data if the controller or processor has provided adequate safeguards.

The absence of an Adequacy decision indicates a lack of sufficient data protection in the third country, so the appropriate safeguards are conceived as its suitable compensation.[19] Unlike transfers based on an Adequacy decision, where the states' legislation and practical guarantees are in stake, here the responsibility for obtaining and implementing adequate safeguards is located with the controllers and/or processors. The safeguards should set the seal on compliance with the Union's data protection standards and availability of enforceable data rights, as well as of effectual legal remedies.

The appropriate safeguards, without requiring any specific authorization from a supervisory authority, include:

- A legally binding and enforceable instrument between public authorities or bodies;[20]
- Binding corporate rules;[21]
- Standard data protection clauses adopted either by the European Commission or by a supervisory authority;
- An approved Code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
- An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In addition, the requirements foresee the possibility the transfer to happen when, subject to the authorization from the competent supervisory authority, some of the following safeguards are provided by:

- Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or

[18] See more in S. Monteleone, and L. Puccio, *From Safe Harbor to Privacy Shield, Advances and shortcomings of the new EU-US data transfer rules, (*European Parliamentary Research service, 2017).

[19] More about: IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*, (ITGP, 2020).

[20] For example, an international agreement to share data between an EU-based public authority and one in a third country. See more in Kuner, Bygrave, Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary, Article 46 GDPR*, (Oxford University Press 2020), p. 806.

[21] In accordance with the GDPR, Article 47.

- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

These mechanisms have prominent central role in international data arena, since the vast majority of countries outside EU or international organizations do not have their own Adequacy decision under the relevant GDPR requirement.

2.1. Binding corporate rules (BCRs)

The essence of Binding corporate rules comes down to providing internal legally binding rules and policies that enable the transfer of data within an international group of companies or group of undertakings engaged in a joint economic activity. These rules enable for transfer of data within the same corporate group to countries that don't provide an adequate level of protection for personal data as required under the GDPR.[22] Their main drive force is the fact they are drafted by the company, but reviewed by the supervisory authorities in the EU Member states and finally approved by the European Data Protection Board.[23] In that direction, the European Data Protection Board registers and constantly renews a list of approved BCRs.[24]

In addition to ensuring the smooth exercise of the right to personal data protection, they are a convenient solution for companies, as they can be tailored according to the needs of the business and once operational, are much easier to carry on with.[25]

The competent supervisory authority shall approve binding corporate rules in line with the consistency mechanism, provided they:

- are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
- fulfilling specific requirements.[26]

The BCRs must be binding within the group. This may seem fair enough but the applicant from the group must demonstrate in its application that the BCRs are binding on all members within the group: this requires the company to examine the structure of its group and the applicable law to each member of the group.[27]

Binding corporate rules ensure their validity through the obligatory incorporation of data, among others, those that refer to:

- categories of personal data - the subject of transfer;
- the group structure, reducing it to a list of entities bound by the rules and their contact details;

---

[22] Guido Reinke, *Blue Paper on Data Protection, Data Transfer between the European Union and third countries, (*GOLD RUSH Publishing, 2019), p. 53.

[23] EDPB is an independent European body, composed of representatives of the EU national data protection authorities and the European Data Protection Supervisor, which contributes to the consistent application of data protection rules throughout the EU.

[24] The list, with filters as a useful tool for easy navigation and use, could be found on the following website: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

[25] That is why Binding corporate rules are seen as "the gold standard" for GDPR compliance in business world.

[26] Article 47 of the GDPR.

[27] D. Hodkinson, and P. Rees, *Binding Corporate Rules: A simpler clearer view?, (*Computer Law and Security Review, 23 (4), 2007), 352-356.

- a duty for each BCR member as well as for its employees to respect the rules;
- established complaint handling system and its procedure;
- information to be provided to the data subjects how their data is going to be processed and how they can exercise their guaranteed rights.

Furthermore, each Binding corporate rules must enable and demonstrate transparent and easy access to the rules by each interested relevant party.[28]

2.2. Standard Contractual Clauses (SCCs)

SCCs are a streamlined way of assuring a GDPR-conform data transfer to third countries with a non-adequate data protection level (e.g. the USA) through model contract clauses that have been "pre-approved" by the European Commission. As laid out in art. 46 GDPR, SCCs are – in absence of an Adequacy decision by the EU Commission – one possible way for data exporters to reach compliance with GDPR.[29] Modular in their approach, "ready-made", customized, easy-to-implement tool and issued by a public authority, as their core characteristics, sets them apart from other transfer mechanisms.[30]

After the Schrems II CJEU decision, which invalidated completely the Privacy Shield, the SCCs remain valid, but:

- parties to the SCCs must verify on a "case-by-case basis" whether the law of the data importer ensures adequate protection for personal data, as required by EU law; and
- upon receiving a complaint from a data subject, data protection authorities (DPAs) are required to suspend or prohibit a transfer of personal data to a third country where they take the view that, in light of all of the circumstances, the SCCs are not or cannot be complied with.[31]

The Commission Implementing Decision[32] establishes 18 concise clauses, which are separated in four modules, in order to depict various possible constellations between the contracting parties: 1. Controller to Controller (C2C); 2. Controller to Processor (C2P); 3. Processor to (sub)-processor (P2P); and 4. Processor to Controller (P2C).

The SCCs' content and meaning, due to their need to guarantee personal data protection, may not be changed, and need to be implemented in a legally binding manner. The text of the SCCs may not be altered, except:

- to select modules and/or specific options offered in the text;

---

[28] More about Evaluation of the BCR from different dimensions in Moerel Lokke, *Binding Corporate Rules: Corporate Self-Regulation of Global data transfers, (*Oxford University Press, 2012).

[29] See Nicole Beranek, *SCCs and CoCs and BCR – Untangling the web and spotting the difference*, (International Network of Privacy Law Professionals, 26.11.2021).

[30] As it is noted in the EC document "The new standard contractual clauses – questions and answers", feedback from stakeholders shows that they are by far the most used data transfer instrument for European companies. For example, according to the IAPP-EY Annual Privacy Governance Report 2019, "the most popular of these [transfer] tools – year over year – are overwhelmingly standard contractual contracts: 88% of respondents in this year's survey reported SCCs as their top method for extraterritorial data transfers […]".

[31] M. Evans, C. Ritzer, and J. Regan, *Schrems II landmark* ruling: Privacy Shield is invalid, Standard Contractual Clauses are valid but court puts obligations on parties and authorities, Data Protection Report, https://www.dataprotectionreport.com/2020/07/schrems-ii-landmark-ruling-privacy-shield-is-invalid-standard-contractual-clauses-are-valid-but-court-puts-obligations-on-parties-and-authorities/

[32] Commission implementing decision (EU) 2021/914 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.

- to complete the text were necessary (indicated by square brackets), e.g. to indicate the competent courts and supervisory authority, and to specify time periods;
- to fill in the Annexes or to add additional safeguards that increase the level of protection for the data.

These adaptations are not considered as altering the core text.[33]

2.3. Code of conduct (CoCs)

One of the novelties of the Regulation in the area of international data transfers is the express addition of Codes of conduct as adequacy mechanism.

Code of conduct needs to mandatory address specifically:

- essential principles, rights, and obligations arising under the GDPR for controllers or processors; and
- guarantees that are specific to the context of transfers, such as with respect to the issue of onward transfers and conflict of laws in the third country.

The drafted CoC must be submitted and approved by the competent national data protection authority, which is additional guarantee for respect of data protection right.

3. Transfers or disclosures not authorized by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.[34]

4. Derogations for specific situations

Struggling not to hinder the flow of data as a source of development, and taking into account real situations where there is no adequate level of protection or adequate safeguards, the transfer of personal data is still possible, if it coincides with one of the specific derogations provided by the Regulation:

- Data exports can lawfully be made with explicit and informed consent by the individual;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- Where necessary for reasons of substantial public interest;
- Where necessary for establishing, exercising or defending legal claims;
- Where necessary to protect the vital interests of the data subject or other persons;
- From information available on a public register provided that the person to whom the information is transferred complies with any restrictions on access to or use of the information in the register;
- If the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on

[33] European Commission, *The new standard contractual clauses – questions and answers, (*European Commission, 25.02.2022), p.6

[34] GDPR, Article 48.

the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

III. BRIEF OVERVIEW OF NON-EU COUNTRIES' EXAMPLES (MIDDLE EAST COUNTRIES)

Data protection is one of the fields in which the EU could be said to exercise global regulatory supremacy. Namely, the EU rules have now been used as a blueprint for regulatory regimes across the Western world.[35]

Until recently, most of the countries of the Middle East, had no legislation regulating the protection of personal data, and thus the international transfer. In a large portion of these countries, the specific laws are still not operational.

Saudi Arabia and the United Arab Emirates are taken into account, as an example of countries that are in the early phase of legal solutions' implementation.

Saudi Arabia[36] law sets only the legal possibility, in exceptional circumstances and upon cumulative fulfillment of several requirements, for the transfer of data outside the Kingdom.[37] These represent the vary opposite approach of the Law which imposes a general prohibition of international data transfer allowed in very restricted situations, while the GDPR does not prohibit transfers but insists on few conditions to be fulfilled in case when the data is being transferred to countries with a non-adequate protection.

The Executive Regulations elaborate in detail additional purposes for which data can be transferred,[38] and in particular the appropriate mechanisms and safeguards. In each single situation, except in extreme cases, before transferring the data, controller shall apply to the Competent Authority for obtaining written approval, which must be based on valid prescribed conditions.

Similar to the EU framework, Saudi's Executive Regulations provide an Adequacy list representing the countries that come up with an adequate level of protection for personal data and the rights of data subjects, based on fulfillment of the criteria:

- Existence of appropriate regulations and legislation related to protection of personal data and the rights of data subjects;
- The country is a party to appropriate international agreements and obligations, and

[35] For instance, Greenleaf conducted an analysis of the laws in place in 33 of the then 39 non-European countries with data protection laws which highlights that "European standards have had a far greater influence outside Europe than previously realized and that this influence is increasing. See more about Orla Lynskey, *The Foundations of the EU Data Protection Law, (*Oxford University Press, 2015).

[36] The first Personal Data Protection Law was published on 24 September 2021, and will take effect on 17 March 2023. It was further supplemented with a draft version of the Executive Regulations in March 2022, adding significant details to the law.

[37] It is important to point out that there is considerable ambiguity in the legal provisions concerning data transfers. The situation is aggravated by the availability of the law only in Arabic, and the free interpretative translation into English.

[38] Article 28 paragraph 2: a) Providing services directly to individuals if providing such services requires the transfer of Personal Data to outside the Kingdom, in a manner that is not contrary to the expectations of the individuals, and provided such individuals have given their consent in accordance with the consent procedures stated in this Regulation; b) Purposes relating to the public interest.

- The country has a supervisory authority to ensure compliance with laws and legislation previously mentioned.[39]

For those controllers or processor of personal data from the countries that are not part of the Adequacy list, the transfer must be constructed on previously conducted potential risk and impact assessment for each case individually, applying both prescribed general and special criteria.[40]

Aside from the risk and impact assessment, the controller is obliged to provide relevant data transfer safeguards, equivalent to those provided by the GDPR, in particular:

- State in contracts and agreements standard clauses, approved by the Competent Authority, to restrict the transfer of personal data outside the Kingdom;
- Binding internal common rules (for companies operating as part of multinational group), approved by the Competent authority, incorporated as an appendix to the contract or agreement;
- Codes of conduct, previously approved by the Regulatory authorities or the competent authority ;
- Accreditation certificates, confirming appropriate safeguards, issued by an independent party;
- In case of public entities, being controllers or processors, shall sign a binding agreement for transfer of personal data, which shall include binding contractual provisions that ensure privacy of data subjects and protect their rights.

United Arab Emirates[41] law regarding the personal data protection sets out the requirements for the cross-border transfer and sharing of personal data for processing purposes.

Content-wise, the law uses a positivist consultative approach, and reflects the idea of data flow as a means of well-being. The law is considered a "golden standard", and reflects its breadth, which resulted from drafting the law in partnership with more than 30 of the largest technology private companies.[42]

"Similar data protection legislation" is the starting premise on which the international flow of data is permitted. Namely, the country-recipient of the data must have its own data protection legislation that does not contravene the UAE personal data provisions,[43] or it is a signatory of

[39] Executive Regulation, Article 30.

[40] While "general criteria" refers to what the controller shall take into account when assessing the level of protection of personal data for the particular case, the "special criteria" refers to assessing the country to which the data is sought to be transferred, in terms of applicable legislation, adopted international principles and standards for personal data protection, existing codes of conduct and whether the country is party to international agreements or obligations. Executive Regulation, Article 29 paragraph 1 point 1 sub points a and b.

[41] The Federal Decree Law No. 45 of 2021 regarding the Protection of Personal data, issued on 20 September 2021, entered into force on 2 January 2022. The law was part of the biggest legal reform framework in the country, with a goal to improve commercial, economic and investment climate, in addition to maximizing security, social stability and prescribed right both for individuals and institutions.

[42] Abu Dhabi Global Market data protection laws were updated in 2021, adding elements that mirror the EU's GDPR. More about other legal acts that reflect the EU's data protection rules: https://www.privacysolved.com/data-protection-is-trending-in-the-middle-east/

[43] The country to which the data is being transferred has local legislation that includes the main provisions, measures, controls, conditions and rules for protecting the confidentiality and privacy of the personal data, including the data subject's individual rights. PWC, *Data privacy handbook for the United Arab Emirates: A guide to compliance with the UAE's Data Protection Law, (*PWC, 2021), p. 28.

international agreements on data protection.[44] This mechanism may be treated as transfer based on "Adequacy decision", similar to the one of EU's tools.
The second line for international data transfers refers to the flow in countries with different data legislation or which do not legally regulate the protection of personal data at all, permitted through signing agreements with foreign institutions and companies to comply with the UAE personal data protection law,[45] and where either data subject consent is provided or the transfer is contractually necessary.[46]
It is rightly expected that Executive Regulations will shed light on the practical mechanisms for data transfer.
Personal data protection law of **Bahrain** came into force in August 2019, while **Qatar's** law was enacted in 2016. **Israel** has introduced its first Law on personal data protection in 1981, followed later by the Data Security Regulations in 2017. **Jordan** has published the draft of Data Protection Law in 2021.

IV. CONCLUSION

The EU General Data Protection Regulation undoubtedly represents a multiple leap forward in the protection and security guaranties' related to the transfer of personal data, both between entities within the state and beyond its borders. It is achieving the goal by determining additional mechanisms for data transfer, previously unknown, but also by strengthening data protection tools within the framework of existing mechanisms. Compared to other legal systems around the globe, the EU's GDPR can rightly be considered a cornerstone and a leading example to be strictly followed.
However, the short time of implementation in practice so far, and the several court decisions that address precisely the shortcomings of the mentioned personal data transfer mechanisms, strongly indicate that additional reviews and adjustments of the mechanisms are more than needed. They should enable the achievement of the double desired goal: the highest possible degree of protection and guarantee of personal data transfers' and enabling the transfer of data as "fuel" for economic prosperity and development.
The ultimate level of protection during the transfer of data to other countries outside the EU, including those from the Middle East, imposed by the GDPR, as well as the high fines associated with non-compliance with these provisions, are certainly among the positive challenges for adopting appropriate legal solutions in these countries. Considering the very short period of application of these laws, there are no available data and figures that will demonstrate the exact benefits of applying the transfer mechanisms in practice. But the very fact that these legislations follow the example of the EU and incorporate similar or the same mechanisms for the transfer of personal data, gives hope they will provide an adequate level of personal data protection for their citizens, and for all others whose data is being processed under the application of their legislation.

[44] The Executive Regulations, which are still not drafted and enacted in the time when the paper is written, is expected to detailed more about the approved countries.
[45] Similar to the GDPR's standard contractual clauses.
[46] More about at: https://ai.gov.ae/personal-data-protection-law/

Bibliography:

1. Beranek Nicole, *SCCs and CoCs and BCR – Untangling the web and spotting the difference*, International Network of Privacy Law Professionals, 26.11.2021
2. Christopher Kuner, Transborder Data Flows and Data Privacy Law, OUP Oxford, 2013
3. C. Kuner, L. Bygrave, and C. Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary, Article 46 GDPR*, Oxford University Press, 2020
4. European Union Agency for Fundamental Rights/Council of Europe*, Handbook on European Data Protection Law*, 2018 Edition, 2018
5. Guido Reinke, *Blue Paper on Data Protection, Data Transfer between the European Union and third countries,* GOLD RUSH Publishing, 2019
6. IT Governance Privacy Team, ITGP*, EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*, 2020
7. Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global data transfers,* Oxford University Press, 2012
8. Orla Lynskey, *The Foundations of EU Data Protection Law,* Oxford University Press, 2015
9. P. Rees and D. Hodkinson, *Binding Corporate Rules: A simpler clearer view?,* Computer Law and Security Review, 23 (4), 2007
10. PWC*, Data privacy handbook for the United Arab Emirates: A guide to compliance with the UAE's Data Protection Law,* 2021
11. S. Monteleone, and L. Puccio, *From Safe Harbour to Privacy Shield, Advances and shortcomings of the new EU-US data transfer rules,* European Parliamentary Research service, 2017
12. Wolf J. Schunemann, Max-Otto Baumann, *Privacy, Data Protection and Cybersecurity in Europe,* Springer, 2016

Documents:

1. Commission implementing decision (EU) 2021/914 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, 2021
2. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995
3. Draft of the Executive Regulation of Personal Data Protection, Saudi Arabia, https://istitlaa.ncc.gov.sa/en/transportation/ndmo/pdpl/Documents/Draft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%209.pdf
4. Federal Decree Law No. 45 of 2021 regarding the Protection of Personal data, United Arab Emirates, 2021
5. Personal Data Protection Law Royal Decree M/19 of 9/2/1443H, 2021, Saudi Arabia, 2021
6. Regulation (EU) 2016/679 of the European Parliament and of the Council 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), 2016
7. The new standard contractual clauses – questions and answers, European Commission, 2021

Internet sources links:

1. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/gulf-region_en
2. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
3. https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en
4. https://www.dataprotectionreport.com/2020/07/schrems-ii-landmark-ruling-privacy-shield-is-invalid-standard-contractual-clauses-are-valid-but-court-puts-obligations-on-parties-and-authorities/
5. https://ai.gov.ae/personal-data-protection-law/
6. https://www.privacysolved.com/data-protection-is-trending-in-the-middle-east/