COVID-19 Impacts in the New Technological Era: Cross-Border Privacy Issues With Emphasis on AI

Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou, and Konstantinos E. Psannis, *Member, IEEE*

***Abstract*—Apart from the impacts on the economy, health, and society, the systematic, essential, and massive processing of personal data during the management of the global pandemic of COVID-19, demands the analysis of specific legal issues regarding privacy. Many issues affecting data protection have been emerged as a result of this global crisis and are been analyzed in this research work, including the proper balance between public interest and data protection, the classification of privacy impacts and the analysis of cross-border data flows, considering current technology. In particular, this paper focuses on the privacy impacts of COVID-19 by examining the type and the context of these impacts, the cross-border data flows tools from a European law perspective, taking into consideration the contribution of artificial intelligence in scientific research during the global pandemic.**

***Index Terms*—IoT, big data analytics, cloud, algorithmic framework, AI, COVID-19, cross-border data, GDPR, personal data, privacy.**

I. Introduction

AS IT is well known, the recent technological initiatives affect privacy. Especially in the pandemic era, taking additional technological measures, which aim at limitation, have raised specific privacy impacts, taking into consideration cross-border data flows [1].

More specifically, this paper focuses on the privacy impacts of COVID-19 from a GDPR (General Data Protection Regulation) perspective, concerning also big data analytics services [2] and contact tracing applications [3]. The health sector and personal data concerning health demand big data processing with the increased use of information and communications technologies [4].

In the context of a pandemic, the processing[1] of big data with digital means is carried out during the operations of health systems and to the response to this global urgent situation as well. In addition, the worldwide spread of COVID-19, which requires international cooperation, shifts attention to the evolving framework of cross-border data flows. Meanwhile, as EU legislation has widened the EU[2] territorial privacy borders, it is obvious that not only companies and individuals [6] in the EU have to comply with GDPR but also non-EU-based entities and individuals. In particular, the focus has now shifted to where the data subject is located as well as to data processing of people living inside the EU [7], which could enable GDPR to become an international privacy tool [8]. Moreover, this research work combines the cross-border data flows tools with the essential intrusion of artificial intelligence. Consequently, through legal analysis, this study points out the main privacy issues of COVID-19 and specifies the privacy framework regarding artificial intelligence, by combining them with the specific field of cross-border data flows. This study's scope is to clarify the legal framework in areas of key importance, within the pandemic, considering the EU data protection legal context. The interference of technological aspects with the legal framework is considered essential to this analysis to present the possible solutions to the arising issues, with emphasis on the implementation.

In general, regarding data protection right, it is important to clarify that it is a qualified right [9], [10], which means that the restriction of this right could be permitted under specific circumstances (e.g., public interest, overridden interests, or fundamental rights).

II. Classification of Covid-19 Privacy Impacts

To present the data protection framework and the international data flows in regards to COVID-19, by examining also big data and artificial intelligence (AI) technologies, it is essential to illustrate the classification of the major privacy impacts. Figure 1 is a proposal about the main effects, based on the type of personal data within their context.

Initially, every personal data processing must be conducted legally under the conditions of Article 6 (1) GDPR (e.g., consent) and every sensitive[3] personal data processing must be conducted in addition to the conditions of Article 9 (2) GDPR (e.g., explicit consent).

Manuscript received 26 July 2021; revised 24 February 2022 and 2 August 2022; accepted 19 August 2022. Date of publication 9 September 2022; date of current version 15 December 2022. This work was supported by the Hellenic Foundation for Research and Innovation (HFRI) through the HFRI Ph.D. Fellowship Grant under Grant 290. *(Corresponding author: Konstantinos E. Psannis.)*

The authors are with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, 546 36 Thessaloniki, Greece (e-mail: rizstavroula@uom.edu.gr; ealex@uom.edu.gr; kpsannis@uom.edu.gr).

Digital Object Identifier 10.1109/TTS.2022.3203962

[1] 'processing' means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [Refer GDPR article 4(2)].

[2] GDPR applies to European Economic Area (EEA), which includes EU countries and Norway, Iceland and Liechtenstein [5].

[3] '... personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.' [Refer GDPR article 9(1)].

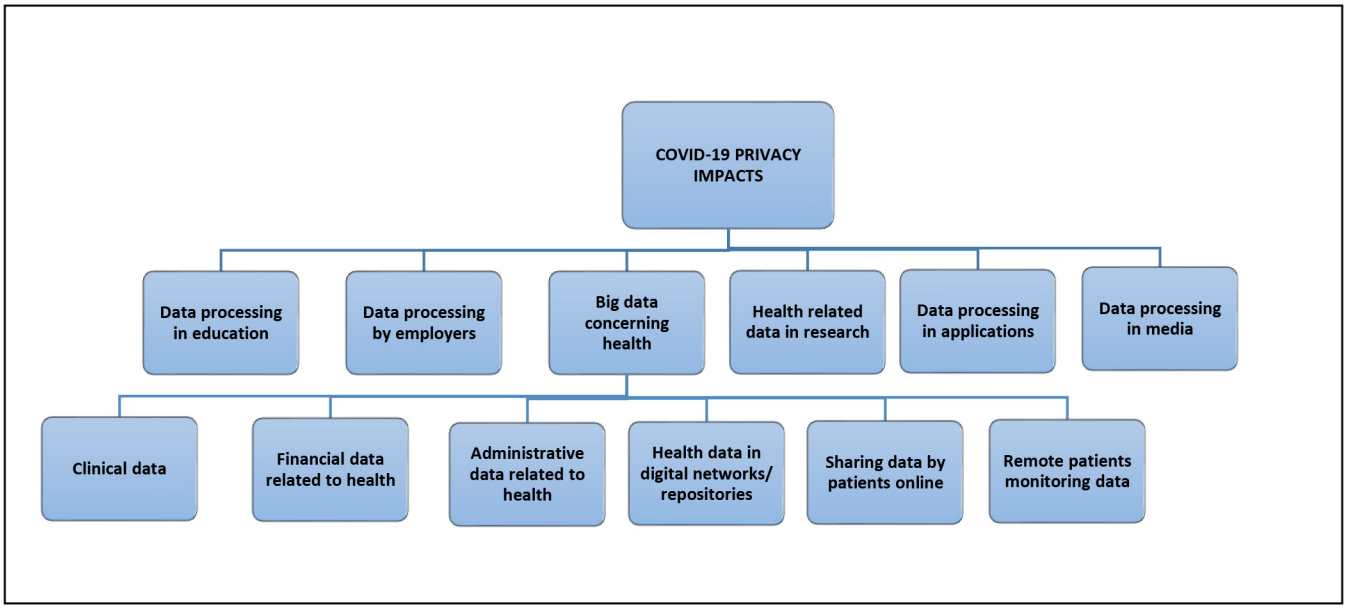

Fig. 1. COVID-19 privacy impacts.

A. Data Processing in Education

As a result of social distancing and the shutdown of educational units on a global scale, a main current educational method is e-learning, putting into practice software for video conferencing [11].

In this digital context, with the possible interaction of different devices (IoT), it is essential to ensure the authentication of the data subjects when entering an online e-learning platform. In general, the GDPR processing principles of data minimization and purpose limitation [12], should be implemented, taking into account the necessity and the specific purpose of every processing. Accordingly, big data analytics[4] is not considered as compatible processing with the initial purpose regarding educational-related matters [12].

In terms of the subject's consent, as a legal basis for lawful processing, in the case of e-learning may include both adults and minors. GDPR in Article 8 distinguishes the minors' consent in two categories based on their age: (a) 16 years and over; and (b) under 16 years of age. More specifically, the consent of a minor 16 and over is sufficient, while in the second case parental consent or parental approval of minors' consent is essential [13]. It should be mentioned though, that GDPR allows Member States jurisdictions, reminding a Directive, to decide the right age limit for mandatory parental consent or approval, setting as a general threshold the age of 13 [14].

Regarding the security of personal data, according to [15], the encryption method is a solution for processing minors' personal data in a digital environment. Moreover, it has been discussed that security and privacy approaches regarding e-learning, could be based on blockchain technology [16], in order to enable rapid disclosure of a data breach [17]. This idea is not new, as blockchain technology was proposed even in academic assessment by universities [18].

B. Data Processing by Employers

To begin with, the consent of employees, cannot be generally the legal basis for data processing, because of the relationship of dependency between employer/employee. As a result, the processing of personal data during employment should rely on another Article's 6 of GDPR or Article's 9 of GDPR condition. Employee's free consent could be given only in case of no effects based on this consent [19].

Regarding teleworking, the organizational and security measures concerning privacy are in a definitely different context [20]. In particular, controllers of the data processing should implement additional measures for remote working. For instance, supervision during remote working hours, by recording the employee's screen or the time spent in an application, etc, has risen privacy issues. These practices are not compatible with Article's 6 par. 1 (f) legitimate interests of the employers [19] and to the principle of proportionality, and as a result, this kind of processing does not have a legal basis.

As Cloud Computing has been implemented in many entities, the protection of the employees' personal data is a major issue, especially in the cross-border characteristics of Cloud Computing. In particular, personal data of employees, which are placed in the cloud, can be transferred to other parties, who are located in a country outside the EU [19], [21]. Inside the cloud, an entity needs to clarify the existence of a cross-border data transfer, in order to use one of Articles' 45-49 of GDPR mechanisms for this transfer outside the EU and the elements of every data processing.

As for security schemes for Cloud Computing, efforts have been made to address privacy and security issues by technological measures [22], by establishing, for example, according

[4]"data analytics" refers to personal data used in the computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations and refers to the whole data management lifecycle of collecting, organising and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours [12].

to [23], a security "wall" in the middle of the Cloud Server and the users of the Internet, taking into account big data.

Processing of health data in the environment of work is a crucial privacy issue during a pandemic. As personal data concerning health are considered as sensitive personal data, the legal basis should be relied mainly upon Article's 9 (2) provisions of GDPR. According to [24], lawful health monitoring in a place of work depends on the proportionality principle. This would mean that processing of, e.g., body temperature, should be a lawful measure of last resort for the data controller, after precluding the possibility of other measures, instead of systematic and massive monitoring of employees' overall health.

C. Big Data Concerning Health

In the context of a pandemic, to conduct a data protection analysis of health data, with the characteristics of big data (velocity, volume, variety) [25], it is essential a further categorization about these data.

Initially, the increase of big data due to the IoT (Internet of Things) and Cloud Computing [26], has brought the rapid growth of processed data. Personal data in the health sector is nowadays massively (big data) processed [25], with the advent of electronic health records (EHRs) [27], AI in healthcare and medical research, etc. In order to present the overall context of lawful data processing of health data, taking into account the COVID-19 pandemic, it is important to describe the subcategories of this kind of data. More specifically, according to their content, big data concerning health can be described as the below (1), (2), (3) and according to their context of processing to the below (4), (5), (6). Big data in the health sector [28], [29], can be considered as follows:

1) Clinical Data: Data, which are collected by hospitals, clinics, medical practices, and in general by all health care institutions, including digital health records [29], medical results etc. In fact, this category consists only of personal data closely associated with health.

2) Financial Data Related to Health: Personal data, such as costs and healthcare insurance claims [28], [29], are very important regarding privacy, as they can reveal clinical data, and other personal data as well, of a data subject [30]. In addition, it is important to mention that personal data of the below-mentioned (number 4) national or international networks and databases contain not only clinical data but financial and healthcare insurance data as well.

3) Administrative Data Related to Health: This category of health big data contains all the registrations of personal data inside a health care system, when these data cannot be considered as purely clinical data or financial data.

4) Health Data in Digital Networks/Repositories: In general, data, which are included in this category, could be medical data, data from health monitoring devices, EHRs, and many other health data. However, the importance of underling this category arises from the volume and the connectivity of personal data, the possible impacts in case of a data breach, and the need for international cooperation during a global pandemic.

In order to ensure the continuity of healthcare for EU citizens through the cross-border flows of personal data [31], the EU has created an *eHealth* network under the Directive 2011/24/EU. Health data are being shared through this network under *eHealth Digital Service Infrastructure* [32]. As a response to the pandemic, EU members of this network transfer anonymized personal data under the policy of contact tracing applications against the COVID-19 spread [33]. As for the USA, the database entitled "All of Us" by the National Institutes of Health (NIH) has been implemented. This database contains health data, which have been collected voluntarily, from data subjects [34].

5) Sharing Data by Patients Online: Big data concerning health, composing important datasets, can be found online, as data subjects reveal this information on a voluntary basis at forums, networks, etc [29].

6) Remote Patients Monitoring Data: Remote monitoring of patients has become the center of attention, with the advent of new medical technologies and the IoT over the past years. Furthermore, the pandemic has shifted the attention to social distancing through digital medical supervision and home monitoring initiatives [35], in order to decrease the pandemic spread.

Privacy framework of health data: To begin with, the privacy framework of health data during a pandemic under GDPR is reflected in Recital 46.[5]. The legal basis for processing health data, which are sensitive personal data, could be: (a) data subject's explicit consent [Article 9 par. 2 (a) GDPR], (b) preventive or occupational health care basis [Art. 9 par. 2 (h) GDPR] or (c) public interest in the context of protection of public health [Article 9 par. 2 (i) GDPR] [36].

D. Health-Related Data in Research

As a result of the pandemic, scientific medical research plays an important role, including various health data. Initially, data processing in the context of scientific research (Article 89 GDPR) should contain security measures of pseudonimization and anonymization, if scientific research can be achieved along with their implementation.

In particular, the legal basis for health-related data processing within scientific research, are considered: (a) explicit consent of [Article 9 par. 2 (a) GDPR], (b) public interest in the area of public health of [Article 9 par. 2 (i) GDPR], (c) scientific research of [Article 9 par. 2 (j) GDPR] [37]. However, the details that govern the processing based on (b) and (c) conditions, are regulated by EU or Member State law [38].

E. Data Processing in Applications

Contact tracing[6] apps worldwide could contain personal data, including location data, health data, name, phone number,

[5]'...Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.' [Refer Recital 46 GDPR].

[6]"Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission" [39].

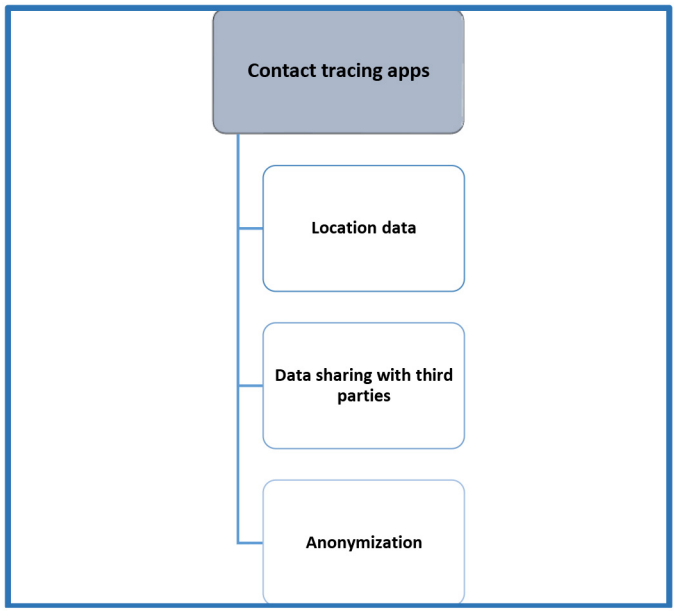

Fig. 2. Key challenges of COVID-19 contact tracing apps in 5G networks.

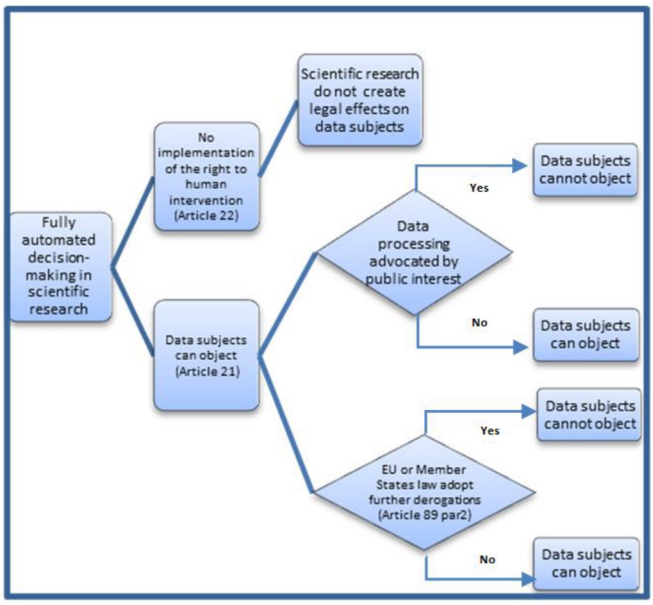

Fig. 3. Fully automated decision-making restrictions of GDPR in scientific research.

name, email address, etc [3]. Contact tracing procedure, in general, can track the cases and their possible contacts [40]. It is very important to mention the intrusion of 5G networks environment regarding these apps and clarify the major privacy challenges, as it is illustrated in figure 2. Depending on the kind of personal data, which is being processed by mobile contact tracing applications, the legal basis rests on either Article 6 or Article 9 of GDPR.

1) Location Data in 5G Networks: In fact, a big majority of the eligible personal data consists of location data. Location data, with the advent of 5G generation of cellular technology networks, is particularly important. More specifically, an initiative of 5G networks, governing mobile applications, is high-efficiency device positioning and localization, which means a larger amount of personal data about the subject's location and thus possible interference with further personal data [14].

2) Data Sharing With Third Parties: According to [3] study, some of these applications share personal data with third parties. The impact of this processing would be automated decision-making of personal data and profiling for advertising purposes, including big data analytics. As a result, the main goal is to respect the data subjects' rights according to GDPR [36] through the emergency circumstances of a pandemic (not to be subject to automated decision-making, right to be informed, and consequently consent of the data subject).

3) Anonymization: Anonymization could be a sufficient security measure for data protection of location data [41], which is required throughout the operation of contact tracing apps and after reaching their end as well. Anonymization is a security technique applied, according to the state of the art, to personal data, in order to convert them into non-personal data [42]. Anonymization, in general, could be an efficient privacy tool for 5G environments [14]. More specifically, the critical issues are: (a) attainment and continuation of anonymization technique, even in linked data, in order to process data out the scope of GDPR and (b) consideration should be given to the principle of storage limitation, prohibiting the conservation of personal data after the end of the pandemic, when data should be either deleted or anonymized [36].

F. Data Processing in Media

In general, according to Article 85 GDPR, the right to freedom of expression and information, which refers to journalism, should be balanced by national laws of Member States with the right to the protection of personal data [43]. In particular, this does not mean that the balancing between the rights should not be required in ad hoc implementation of national provisions as well. In addition, the disclosure of information about deceased people is a processing that is out of the scope of GDPR. However, national jurisdictions may have adopted safeguards regarding data protection of deceased people (Recital 27 GDPR). Nevertheless, the publication of deceased people may affect other people's personal data [24], thus a legal basis for this processing is required under Article 6 or Article 9, depending on the kind of personal data.

III. Considering AI Privacy Issues During the Fight Against Covid-19

Artificial Intelligence (AI) has a vital role in efforts to address COVID-19, including contact tracking, diagnosis, drug treatment and last but not least vaccines [44], [45]. Moreover, the applications of AI could contribute in the automation of health care institutions' operations [46]. Therefore, following the classification of the general privacy issues in the light of the pandemic, it is essential to present the specific interference of data protection with AI. The applications of AI, which emerge ethical issues as well [47], [48], demand specific data protection, as it presented in this Section, and more particularly in figure 3.

Undoubtedly, AI and thus automated decision-making demand the processing of big data, and more specifically the processing of a large amount of health data [49] and as a result sensitive personal big data. Generally, big data privacy risks are summarized in "three Vs": (a) volume related to the quantity of data, (b) velocity representing the speed of data processing, and (c) variety meaning different kinds of data included in a processing [25]. Automated decision-making, which is achieved through algorithms or AI systems [50], is divided into fully automated (without any human intervention) and partly automated decisions [51].

Three major pillars characterize fully automated decision-making in the context of scientific research under GDPR. The first issue refers to Article's 22 prohibition on fully automated processing (with its exceptions) [52], which is not though applied in the context of scientific research. In particular, the results of scientific research generally do not create legal effects of a personal nature [53], and as a result, automated processing can be conducted ab initio, without the need to turn to the exceptions of Article 22 par. 2. This avoiding of the general prohibition of fully automated decisions in terms of scientific research is based on the condition in Article 22, which applies as long as the processing creates "legal effects"[7] on natural persons.

Secondly, the right of data subject to object to automated decision-making has a restriction, which refers to scientific research under public-interest activities (Article 21 par. 6). Accordingly, the data subject has no right to object to scientific research, which is based on artificial intelligence, and is aimed at public interest. According to [38], the efforts that aim at addressing the pandemic of COVID-19, are covered by public interest.

In addition, EU or Member States law may adopt further derogations to data subject's right to object (Article 89 par.2), limiting, even more, the scope of Article 21, when it comes to scientific research.

Therefore, it is becoming clear that scientific research through a global pandemic, with the support of artificial intelligence, does not meet the privacy obstacles of fully automated processing, due to emergency circumstances.

IV. Cross-Border Data Flows

This Section analyzes the current legal framework of cross-border data flows, as it was established by the recent legal reforms.

International data flows contribute to the global economy, with this contribution to be expected to grow even more in the coming years [54]; cross-border data flows are going to be increased in subsequent years with the advent of artificial intelligence, IoT, next-generation mobile networks, Cloud Computing and other technological initiatives that support data digitalization and sharing. In a context of a global pandemic, especially in the field of research and COVID-19 monitoring, the transfer of personal data has become necessary [38]. As a result, it is of great importance to clarify and present, with a focus on practical implementation, the currently available paths of conducting international transfers of personal data.

Cross-border transfer mechanisms of GDPR are essential before every processing of personal data, which are exported from an EEA country to a non-EEA country. It should be mentioned that distant access (e.g., Cloud Computing) or any other processing of personal data, which are located in EEA from a third country is a cross-border data flow [55]. In particular, the lawful international transfer of personal data is the second hurdle we need to overcome in order to process any personal data, after relying on a legal basis of Article 6 or Article 9 and their relevant provisions, as well as enforcing the processing principles of Article 5 [56].

A. Available Mechanisms for Cross-Border Data Flows

After determining the legal basis for the processing and respecting the processing principles, the next step for the data exporter[8] is to base the cross-border data transfer on an available instrument of GDPR. It is important to mention that among EEA countries, the free movement of personal data is applicable [57]. The cross-border data flows from an EEA country to a third country can be conducted under the following mechanisms, which are presented in order of importance, in terms of the evaluation of the data protection level.

1) Adequacy Decisions (Article 45): The first-tier transfer tool, as it is the best possible recognition for a third country or an international organization, is a relevant adequacy decision of the European Commission. In particular, as long as the third country has received this decision, there is no need to turn to other tools, and thus cross-border data flows can be conducted fully or partly (may refer to a specific field) to the third country [7]. However, the catalog [58] of the countries,[9] for which adequacy decisions exist, may be reviewed by the European Commission or modified by the Court of Justice of the European Union (CJEU) [55].

2) Safeguards (Article 46): Entities can seek a mechanism described in Article 46 GDPR, regarding a transfer to a country that has not received an adequate decision. More particular these tools are: (a) standard data protection clauses (SCCs), (b) binding corporate rules (BCRs), (c) codes of conduct, (d) certification mechanisms, (e) ad hoc contractual clauses [55]. The SCCs and the BCRs should be further analyzed as they are considered the most common tools [59]. BCRs, which should be first approved by the supervisory authority,[10] apply in international transfers of multinational companies, in order to ensure that the processing complies with the data protection provisions of GDPR. The SCCs, which should be first approved by European Commission or

[7]'. . . legal effects concerning him or her or similarly significantly affects him or her'[Refer Article 22 par 1GDPR].

[8]"Data exporter" means the controller or processor within the EEA who transfers personal data to a controller or processor in a third country [56].

[9]Countries with adequacy decisions: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

[10]Article 46 par. 2 and Article 46 par. 3 (a) GDPR.

by a supervisory authority, refer to the data importer's compliance with the data protection level of the exporter [25]. However, a recent commitment has been introduced by the Court of Justice of the European Union (CJEU) demanding the establishment of supplementary measures to SCCs by the controller to ensure compliance (C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems) [60].

3) Derogations for Specific Situations (Article 49): In case of no adequacy decision of safeguards of Article 46 exist, the processing can be based on the exceptions of Article 49 as a last resort. The specific derogations are the following [7]:

1) Given explicit consent of data subjects.
2) Necessary transfer for the performance of a contract between the data subject and the data controller.
3) Necessary transfer for the performance of a contract, which contributes to data subject's interests.
4) Necessary transfer for important reasons of public interest.
5) Necessary transfer in terms of legal claims.
6) Necessary transfer for protecting data subject's vital interests.
7) Transfers of personal data from public registers.

In general, the derogations should be treated as exceptions from a regular situation, given the data subject explicit consent or the accomplishment of the conditions (b), (c), (d), (e), and (f) of Article 49 par. 1 [56].

When a transfer cannot be based on Article 45, Article 46, or Article 49 par. 1 (a-g), a cross-border transfer can be realized only under the conditions of Article 49 par. 1 subparagraph 2. In this case, the controller shall inform the supervisory authority of the transfer.[11]

B. The Framework of International Data Flows After Brexit

The free transfer of personal data from the EEA to the U.K. after Brexit was ensured under the EU-UK Trade and Cooperation Agreement [61], which is a transitional agreement. This scheme was provisional,[12] as it was going to be in force until an "adequacy decision" by the European Commission is given or up to 6 months deadline. It has become apparent from the provision[13] of the Agreement that the next model of international personal data transfers from the EEA to the U.K., would be the first-tier mechanism of "adequacy decision", to maintain the scheme of free transfer of personal data from the EU [62]. European Commission recognized on 28 June 2021 the adequate level for transfers of personal data to the U.K., under the GDPR [58].

[11]Recital 113 GDPR.

[12]The Trade and Cooperation Agreement is applicable from 1 January 2021 for up to 6 months [62].

[13]Article FINPROV.10A, par. 4 of 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.

C. The EU-USA Framework of International Data Flows After the Invalidation of Privacy Shield

Initially, the available personal data transfer mechanisms from the EU to the USA at the moment are all the above-mentioned tools except for 'adequacy decisions'. More specifically, the Court of Justice for the European Union (CJEU) invalidated the framework of transatlantic transfers from the EU to the USA "Privacy Shield" [63], which has been in force since 2016 and had enabled the first-tier tool of adequacy decision [59]. In addition, regarding SCCs, an obligation has been introduced by CJEU, requiring that data controllers should evaluate[14] the data protection level of the third country before the transfer [64] and even apply further ensuring safeguards (e.g., encryption). As a result, EU law demands an equivalent data protection framework for data, which are imported in the USA, and in general to every importer's country [55]. A new agreement between the EU and USA will be finalized in the near future.

V. The Framework of Cross-Border AI Data Processing in the Context of Covid-19 Research

The fully automated decision-making processing in medical research to address a global pandemic is essential at an international level, as mentioned in Section III. As a result, the presentation of the current and newly formed[15] framework of conducting cross-border data flows for automated decision-making purposes would be substantial for the field of research, based on AI, as well as for the cross-border framework in general.

The combination of the privacy impacts arising from AI (Section III) and the cross-border data flows framework (Section IV) is presented in this Section, which is reflected in figure 4.

Initially, the exporter of personal data from EEA to a third country should ensure persistent data protection even after the transfer, regarding the transfer mechanisms of Article 45, Article 46, and Article 49 [38].

As a result, the data transfer, which is intended for automated decision-making processing, can be conducted freely in a country that has received an adequacy decision with the reservation of the continuing protection of data subjects.

In the absence of an adequacy decision, the next issue we need to examine is whether the transfer for research purposes, including AI, is regulated by the mechanisms of safeguards of Article 46. Scientific research, which is carried out on a long-term basis, demands the usage of the safeguards of Article 46 GDPR [38].

More specifically, the transfer tool of safeguards of Article 46 GDPR includes: (a) the assessment of the level of data protection of the importer's country, regarding every intended

[14][. . . whether the law of the third country of destination ensures adequate protection, under EU law..] (par. 134, Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems).

[15]By the Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

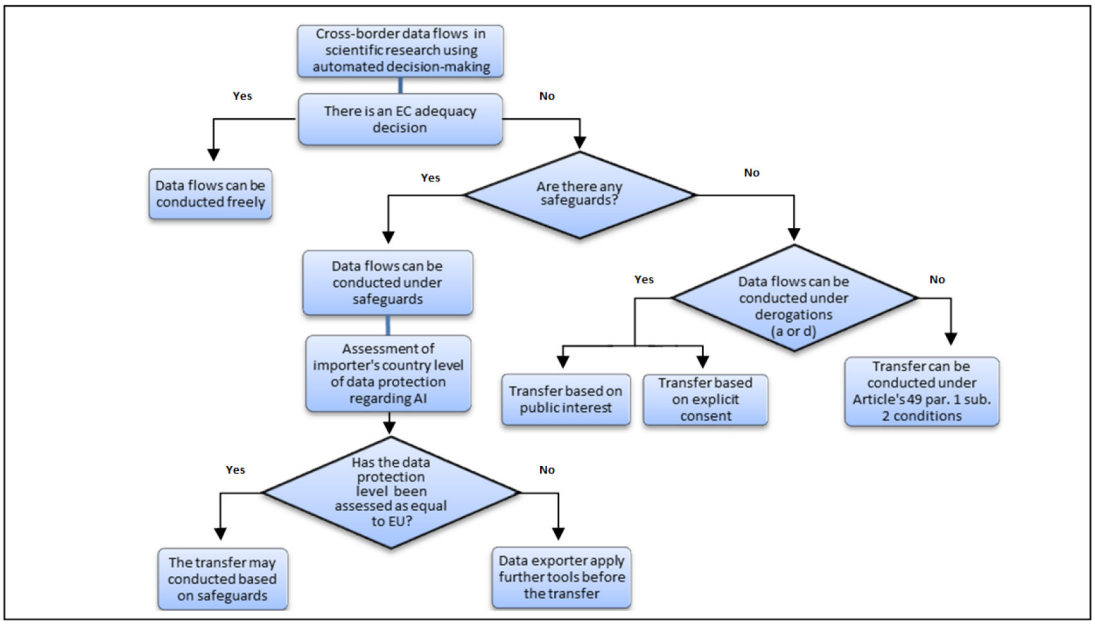

Fig. 4. Available mechanisms of cross-border transfers for data processing using AI in the context of scientific research of COVID-19.

processing, and (b) the implementation of further measures in case of a non-compliance determination, based on the assessment regarding the context of the transfer [55]. Regarding the context of a transfer for the purposes of automated decision-making processing, the assessment should be based on various factors that combine the processing (e.g., data subjects protection regarding AI in the third country, the existence of sensitive personal data).

In general, the examination of non-EEA countries' level of data protection regarding the context of the transfer is a complicated procedure, which is arising on both cross-border transfer tools (adequacy decision, safeguards) and demands access to third countries' legislation.

The essential assessment could be supported by the establishment of national repositories, providing the classification of privacy laws and legal provisions that could affect personal data (e.g., national security laws).

Based on the result of the assessment, the data exporter from EEA should apply further ad hoc measures (e.g., pseudonimization), depending on the context of every transfer [55]. However, it should be mentioned that the assessment of the third country's level of data protection, regarding every transfer, is a continuous and not stable procedure, which demands constant review and awareness about the data protection context of non-European countries.

If there are no safeguards, in the context of COVID-19 scientific research including AI, the derogations of the explicit consent and public interest are appropriate tools [38]. More particularly, in case of research proposes, being governed by public interest, the processing principles[16] (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, security, accountability) should be implemented, taking into consideration all the conditions of Article 49 par. 1 subparagraph 2.

VI. Conclusion

This article examines the COVID-19 privacy effects, based on the EU legal system of data protection, by pointing out the crucial issue of cross-border data flows, especially during a global pandemic.z

Firstly, in regards to privacy issues of COVID-19, we intend to provoke and clarify them, by the processing manner and the kind of personal data, which can be affected, as a result of this crisis. The proposed classification presents the various aspects and recommendations about their legal treatment from a GDPR scope. Furthermore, it is of great importance to emphasize the legal approach of the contribution of artificial intelligence in the fight against COVID-19, in addition to an international approach to EU data transfers as well. Considering the recent requirements in cross-border data flows from the EU to third countries and taking into account the pandemic, the main scope is to ensure continuous data protection regarding a data transfer, which could contribute to precarious conditions. Consequently, it should be mentioned that this study highlights specific legal paths, regarding data protection, considering the arising issues in addition to exceptional conditions.

In conclusion, this research work points out the available mechanisms and their proper use to combine the technological and legal fields, pursuing fair and integrated treatment. In the next step of our research, we intend to examine the future and accomplished privacy impacts of the post-pandemic era, their correlation with emerging technologies, as well as the possible legal responses.

Acknowledgment

All the websites were accessed on 20 July 2021.

[16] Article 5 GDPR.

REFERENCES

[1] "Ensuring data privacy as we battle COVID-19." OECD. Apr. 2020. [Online]. Available: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/

[2] G. R. Shinde, A. B. Kalamkar, P. N. Mahalle, and N. Dey, *Data Analytics for Pandemics: A COVID-19 Case Study*. Boca Raton, FL, USA: CRC Press, 2020.

[3] M. A. Azad *et al.*, "A first look at privacy analysis of COVID-19 contact-tracing mobile applications," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15796–15806, Nov. 2021.

[4] P. Kitsos, M. Milossi, M. Nikita, and A. Yannoukakou, "Big and open data privacy risks in health sector: Developing a trend or establishing the future?" in *Proc. 5th Conf. E-Democracy Security Privacy Trust Digit. World*, Athens, Greece, Dec. 2013, pp. 1–11.

[5] "Relations with the EU." European Economic Area (EEA). [Online]. Available: https://www.efta.int/eea

[6] O. Karaduman, "The general data protection regulation: Achieving compliance for EU and non-EU companies," *Bus. Law Int.*, vol. 18, no. 3, pp. 225–232, Sep. 2017.

[7] "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)." Apr. 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[8] M. L. Rustad and T. H. Koenig, "Towards a global data privacy standard," *Florida Law Rev.*, vol. 71, no. 2, pp. 365–453, 2019.

[9] E. Ventrella, "Privacy in emergency circumstances: Data protection and the COVID-19 pandemic," *ERA Forum*, vol. 21, no. 3, pp. 379–393, Dec. 2020.

[10] M. Bottis, F. Panagopoulou-Koutnatzi, A. Michailaki, and M. Nikita, "The right to access information under the GDPR," *Int. J. Technol. Policy Law*, vol. 3, no. 2, pp. 131–142, 2019.

[11] S. Hakak, W. Z. Khan, M. Imran, K.-K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? survey, taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134–124144, 2020.

[12] "Guidelines on children's data protection in an education setting." Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Nov. 2020. [Online]. Available: https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting-

[13] E. Alexandropoulou-Egyptiadou, "Minor's data protection according to GDPR," *DiMEE*, vol. 1, pp. 5–19, 2018.

[14] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," *IEEE Access*, vol. 8, pp. 108052–108061, 2020.

[15] "Recommendation CM/Rec (2018) 7 of the committee of ministers of member states on guidelines to respect protect and fulfill the rights of the child in the digital environment (adopted by the committee of ministers on July 4 2018 at the 1321st meeting of the Ministers Deputies." Sep. 2018. [Online]. Available: https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html#

[16] A. Shukla, N. Patel, S. Tanwar, B. Sadoun, and M. S. Obaidat, "BDoTs: Blockchain-based evaluation scheme for online teaching under COVID-19 environment," in *Proc. Int. Conf. Comput. Inf. Telecommun. Syst. (CITS)*, Hangzhou, China, 2020, pp. 1–5.

[17] M. Humayun, "Blockchain-based secure framework for e-learning during COVID-19," *Indian J. Sci. Technol.*, vol. 13, no. 12, pp. 1328–1341, Aug. 2020.

[18] B. Duan, Y. Zhong, and D. Liu, "Education application of blockchain technology: Learning outcome and meta-diploma," in *Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Shenzhen, China, 2017, pp. 814–817.

[19] Article 29 Working Party (Eur. Commission, Brussels, Belgium). *Opinion 2/2017 on Data Processing at Work*. (Jun. 2017). [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

[20] I. Deguara. "Data protection and working remotely." Information and Data Protection Commissioner. Jun. 2020. [Online]. Available: https://idpc.org.mt/idpc-publications/data-protection-working-remotely/

[21] T. Mulder and M. Tudorica, "Privacy policies, cross-border health data and the GDPR," *Inf. Commun. Technol. Law*, vol. 28, no. 3, pp. 261–274, Jul. 2019.

[22] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020.

[23] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustain. Comput. Inform. Syst.*, vol. 19, pp. 174–184, Sep. 2018.

[24] (Hellenic Data Prot. Authority, Athens, Greece). *Guidelines 1/2020 on the Processing of Personal Data in the Context of the Management of COVID-19*. (Mar. 2020). [Online]. Available: https://www.dpa.gr/en/enimerwtiko/themes/data_Protection_COVID_19

[25] *Handbook on European Data Protection Law*, 2018 ed. Luxembourg City, Luxembourg: Publ. Office Eur. Union, 2018.

[26] A. P. Plageras *et al.*, "Efficient large-scale medical data (eHealth big data) analytics in Internet of Things," in *Proc. IEEE 19th Conf. Bus. Inform. (CBI)*, Thessaloniki, Greece, 2017, pp. 21–27.

[27] T. B. Murdoch and A. S. Detsky, "The inevitable application of big data to health care," *J. Amer. Med. Assoc.*, vol. 309, no. 13, pp. 1351–1352, Apr. 2013.

[28] P. Kitsos and A. Yannoukakou, "E-health in the age of big data: The EU proposed regulation on health data protection," in *Big Data: Challenges and Opportunities*, Huygens Editorial, Jan. 2013.

[29] S. Zillner and S. Neururer, "Big data in the health sector," in *New Horizons for a Data-Driven Economy*. Cham, Switzerland: Springer, 2016, pp. 179–194.

[30] W. N. Price, II and I. G. Cohen, "Privacy in the age of medical big data," *Nat. Med.*, vol. 25, pp. 37–43, Jan. 2019.

[31] E. Alexandropoulou-Egyptiadou, "Cross-border flows of health data," in *Proc. 5th Conf. Med. Responsibility Bioethics Health Genet. Data*, Athens, Greece, Jan. 2018.

[32] (Eur. Data Prot. Board Eur. Data Prot. Supervisor, Brussels, Belgium). *EDPB-EDPS Joint Opinion 1/2019 on the Processing of Patients' Data and the Role of the European Commission Within the eHealth Digital Service Infrastructure (eHDSI)*, (2019). [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing_en

[33] (Eur. Data Prot. Board, Brussels, Belgium). *Comments on the Commission Draft Implementing Decision Amending Implementing Decision 2019/1765 as Regards the Cross-Border Exchange of Data Between National Contact Tracing and Warning Mobile Applications With Regard to Combatting the COVID-19 Pandemic*. (Jul. 2020). [Online]. Available: https://edps.europa.eu/data-protection/our-work/publications/comments/edps-comments-cross-border-exchange-data-between_en

[34] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, "Big data in healthcare: Management, analysis and future prospects," *J. Big Data*, vol. 6, no. 1, pp. 1–25, Dec. 2019.

[35] S. Gerke, C. Shachar, P. R. Chai, and I. G. Cohen, "Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19," *Nat. Med.*, vol. 26, pp. 1176–1182, Aug. 2020.

[36] "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak." European Data Protection Board. Apr. 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en

[37] "Opinion 3/2019 concerning the questions and answers on the interplay between the clinical trials regulation (CTR) and the general data protection regulation (GDPR)." European Data Protection Board. Jan. 2019. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/dictamen-art-70/opinion-32019-concerning-questions-and-answers_en

[38] "Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak." European Data Protection Board. Apr. 2020. [Online]. Available: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

[39] "Contact tracing in the context of COVID-19: Interim guidance." World Health Organization. May 2020. [Online]. Available: https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19

[40] K. Michael, R. Abbas, R. A. Calvo, G. Roussos, E. Scornavacca, and S. F. Wamba, "Manufacturing consent: The modern pandemic of technosolutionism," *IEEE Trans. Technol. Soc.*, vol. 1, no. 2, pp. 68–72, Jun. 2020.

[41] C. T. Nguyen *et al.*, "A comprehensive survey of enabling and emerging technologies for social distancing—Part II: Emerging technologies and open issues," *IEEE Access*, vol. 8, pp. 154209–154236, 2020.

[42] Article 29 Data Protection Working Party, "Opinion 05/2014 on anonymisation techniques," Eur. Commission, Brussels, Belgium, document WP216, Apr. 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[43] M. Bottis, F. Panagopoulou-Koutnatzi, A. Michailaki, and M. Nikita, "General data protection regulation: New ethical and constitutional aspects, along with new challenges to information law," *Int. J. Technol. Policy Law*, vol. 3, no. 2, pp. 172–187, 2019.

[44] Q. Pham, D. C. Nguyen, T. Huynh-The, W. Hwang, and P. N. Pathirana, "Artificial intelligence (AI) and big data for coronavirus (COVID-19) pandemic: A survey on the state-of-the-arts," *IEEE Access*, vol. 8, pp. 130820–130839, 2020.

[45] R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, "Artificial intelligence (AI) applications for COVID-19 pandemic," *Diabetes Metab. Syndrome Clin. Res. Rev.*, vol. 14, no. 4, pp. 337–339, 2020.

[46] K. A. Wittbold, C. Carroll, M. Iansiti, H. M. Zhang, and A. B. Landman. "How hospitals are using AI to battle Covid-19." Harvard Business Review. Apr. 2020. [Online]. Available: https://hbr.org/2020/04/how-hospitals-are-using-ai-to-battle-covid-19

[47] D. Peters, K. Vold, D. Robinson, and R. A. Calvo, "Responsible AI—Two frameworks for ethical design practice," *IEEE Trans. Technol. Soc.*, vol. 1, no. 1, pp. 34–47, Mar. 2020.

[48] D. Schiff, J. Borenstein, J. Biddle, and K. Laas, "AI ethics in the public, private, and NGO sectors: A review of a global document collection," *IEEE Trans. Technol. Soc.*, vol. 2, no. 1, pp. 31–42, Mar. 2021.

[49] M. B. Forcier, H. Gallois, S. Mullan, and Y. Joly, "Integrating artificial intelligence into health care through data access: Can the GDPR act as a beacon for policymakers?" *J. Law Biosci.*, vol. 6, no. 1, pp. 317–335, Sep. 2019.

[50] T. Araujo, N. Helberger, S. Kruikemeier, and C. H. De Vreese, "In AI we trust? perceptions about automated decision-making by artificial intelligence," *AI Soc.*, vol. 35, no. 3, pp. 611–623, 2020.

[51] F. J. Z. Borgesius, "Strengthening legal protection against discrimination by algorithms and artificial intelligence," *Int. J. Human Rights*, vol. 24, no. 10, pp. 1572–1593, 2020.

[52] M. Milossi, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "AI ethics: Algorithmic determinism or self-determination? the GPDR approach," *IEEE Access*, vol. 9, pp. 58455–58466, 2021.

[53] R. Ducato, "Data protection, scientific research, and the role of information," *Comput. Law Security Rev.*, vol. 37, Jul. 2020, Art. no. 105412.

[54] D. Nguyen and M. Paczos, "Measuring the economic value of data and cross-border data flows: A business perspective," in *OECD Digital Economy Papers No. 297*, Paris, France: OECD Publ., 2020.

[55] (European Data Protection Board, Brussels, Belgium). *Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance With the EU Level of Protection of Personal Data*. (Nov. 2020). [Online]. Available: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

[56] "Guidelines 2/2018 on derogations of article 49 under regulation 2016/679." European Data Protection Board. May 2018. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en

[57] E. Alexandropoulou-Egyptiadou, "Cross-border data flows from EU to USA: The recent CJEU decision in the light of the related activity of Facebook (C-362/2014, M. Schrems v data protection commissioner)," *DiMEE*, vol. 1, pp. 12–24, 2016.

[58] "Adequacy decisions." European Commission. 2016. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[59] L. Bradford, M. Aboy, and K. Liddell, "International transfers of health data between the EU and USA: A sector-specific approach for the USA to ensure an 'adequate' level of protection," *J. Law Biosci.*, vol. 7, no. 1, p. lsaa055, 2020.

[60] "Strategy for EU institutions to comply with 'Schrems II' ruling." European Data Protection Supervisor. Oct. 2020. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf

[61] "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." Dec. 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01.0014.01.ENG

[62] "Guide to the general data protection regulation (GDPR)." Information Commissioners Office. Jan. 2021. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

[63] "Judgement of the court (grand chamber) of 16 July 2020 in case C-311/18 data protection commissioner V Facebook Ireland Limited and Maximillian Schrems," EUR-Lex, Luxembourg City, Luxembourg, document 62018CJ0311, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

[64] C. Kuner. "The Schrems II judgment of the court of justice and the future of data transfer regulation." Jul. 2020. [Online]. Available: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

Stavroula Rizou was born in Thessaloniki, Greece. She graduated from the Law School of Aristotle University of Thessaloniki in 2015. She received the master's degree in accounting and finance (with a major in finance) from the Department of Business Administration, University of Macedonia in 2016. Her Ph.D. research focuses on the legal framework of cross-border transfer of personal financial data, conducted with the Department of Applied Informatics, University of Macedonia. She received a Ph.D. Fellowship Grant (Fellowship Number: 290) from the Hellenic Foundation for Research and Innovation in 2019.

Eugenia Alexandropoulou-Egyptiadou is currently the Vice Rector and the Former Deputy Rector of the University of Macedonia, Thessaloniki, Greece, is a Professor of I. T. Law with the Department of Applied Informatics, the Founder of the I.T. Law Scientific Group (www.itlaw.uom.gr), and the Director of the Postgraduate Program (Master) in Law and Informatics (www.mli.uom.gr). A former Attorney at Law with the Greek Supreme Court, she headed the Legal Department of Egnatia Bank in Northern Greece. She was also a member of the editorial board of the Law Review "Harmenopoulos," edited by the Bar of Thessaloniki. She has written and/or edited numerous scientific articles and books in the area of civil, European, banking, labor, international, and IT law. Since 2001, her interests have focused mainly on personal data protection and on the legal environment of the Information Society. She has acted as the organizer, the chair person, and a speaker in several International and Pan-Hellenic Conferences on I.T. Law and Ethics, reviewed numerous papers and dissertations, and participates in many scientific associations and projects.

Konstantinos E. Psannis (Member, IEEE) was born and raised in Thessaloniki, Greece. He received the degree in physics from the Faculty of Sciences, Aristotle University of Thessaloniki, Greece, and the Ph.D. degree from the School of Engineering and Design, Department of Electronic and Computer Engineering, Brunel University, London, U.K.

He is currently an Associate Professor of Communications Systems and Networking with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, the Director of Mobility2net Research & Development & Consulting JP-EU Lab, a member of the EU-JAPAN Centre for Industrial Cooperation, and a Visiting Consultant Professor with the Graduate School of Engineering, Nagoya Institute of Technology, Nagoya, Japan. From 2001 to 2002, he was awarded the British Chevening Scholarship. The Chevening Scholarships are the U.K. Government's Global Scholarship Programme, funded by the Foreign and Commonwealth Office and partner organizations. The programme makes awards to outstanding scholars with leadership potential from around the world to study at universities in the U.K. His research spans a wide range of digital media communications, media coding/synchronization, and transport over a variety of networks, both from the theoretical as well as the practical points of view. His recent work has been directed toward the demanding digital signals and systems problems arising from the various areas of ubiquitous big data/AI-IoT/clouds and communications. This work is supported by research grants and contracts from various government organizations. He has participated in joint research works funded by the Grant-in-Aid for Scientific Research, Japan Society for the Promotion of Science, KAKENHI Grant, the Telecommunications Advancement Foundation, and the International Information Science Foundation, as a Principal Investigator and a Visiting Consultant Professor with the Nagoya Institute of Technology. He was invited to speak on the EU-Japan Co-Ordinated Call Preparatory Meeting, Green and Content Centric Networking (CCN), organized by the European Commission and the National Institute of Information and Communications Technology/Ministry of Internal Affairs and Communications, Japan (in the context of the upcoming ICT Work Programme 2013) and International Telecommunication Union (ITU-founded in 1865), SG13 meeting on DAN/CCN, Berlin, July 2012, amongst other invited speakers. He received a Joint-Research Award from the Institute of Electronics, Information and Communication Engineers, Japan, Technical Committee on Communication Quality, July 2009 and Joint-Research Encouraging Prize from the IEICE Technical Committee on Communication Systems, July 2011. He has more than 75 publications in international scientific journals and more than 107 publications in international conferences, 22 book chapters, and 11 technical reports and received more than 4750 citations (H-index 30, i10-index 66). He has several highly cited papers powered by Web of Science—Clarivate. He supervises three postdoctoral students and eight Ph.D. students and more than 150 M.Sc. thesis.

Prof. Psannis is serving as an Associate Editor for IEEE ACCESS and IEEE COMMUNICATIONS LETTERS. He is a Lead Associate Editor for the Special Issue on Roadmap to 5G: Rising to the Challenge, IEEE ACCESS, 2019. He is a Guest Editor for the Special Issue on Compressive Sensing-Based IoT Applications, *Sensors*, 2020. He is a Guest Editor for the Special Issue on Advances in Baseband Signal Processing, Circuit Designs, and Communications, *Information*, 2020. He is a Lead Guest Editor for the Special Issue on Artificial Intelligence for Cloud Based Big Data Analytics, *Big Data Research*, 2020. He is the TPC Co-Chair at the International Conference on Computer Communications and the Internet (ICCCI 2020), Nagoya Institute of Technology, ICCCI 2020, June 26–29 at Nagoya, and will be held in 2021 June 25–27 at Nagoya (http://iccci.org/) and the Conference Chair at the World Symposium on Communications Engineering held at the University of Macedonia, Thessaloniki, October 9–11, 2020 and to be held at the University of Macedonia, Thessaloniki, November 25–28, 2021 (WSCE 2021—http://wsce.org/). He is the TPC Co-Chair and the Session Chair, titled, Next Generation 6G-Enabled Artificial Intelligence of Things—Digital Twins—and Cobot Intelligence, in 5th World Symposium on Communication Engineering (WSCE 2022) to be held in Nagoya University in September 16–18, 2022. He is an Invited Speaker, titled, Next G-IoT, in the 10th International Conference on Computer and Communications Management, July 29–31, 2022, Okayama University, Japan, an Invited Speaker, titled, 6G-Enabled Massive Internet of Things, and the TPC Co-Chair in the IEEE International Conference on Computer Communication and the Internet (ICCCI 2022), Nagoya Institute of Technology, will be held in June 24–226, 2022, at Nagoya, and an Invited Speaker, titled, Massive Internet of Things, Information Technology and Applications Symposium (ITAS), to be held in Chiba, Japan, in July 1–3, 2022. He has been included in the list of Top 2% influential researchers globally (prepared by Scientists from Stanford University, USA), October 2020 (https://lnkd.in/dhSwdgB) and October 2021 (https://lnkd.in/gCk8FAxu).