Preserving Minors' Data Protection in IoT-based Smart Homes According to GDPR Considering Cross-Border Issues

Stavroula Rizou [1], Eugenia Alexandropoulou-Egyptiadou[1], Yutaka Ishibashi[2], and Kostas E. Psannis[1]
[1] Dept. of Applied Informatics, University of Macedonia, Thessaloniki, 54636, Greece
[2] Graduate School of Engineering, Nagoya Institute of Technology, Nagoya, 466-8555, Japan
Email: rizstavroula@uom.edu.gr, ealex@uom.edu.gr, ishibasi@nitech.ac.jp, kpsannis@uom.edu.gr

Abstract —Apart from the positive effects of smart homes, such as economic, energy, and security enhancements, and the focus on their efficiency and reliability, it should also be paid attention to the legal, ethical and social impacts of these ICT systems. The field of children's data protection is challenging, as they are likely more vulnerable to online risks, and as a result, their protection requires a specialized privacy-preserving scheme. This research work addresses the crucial issues of minors' data protection, from a European law perspective, through IoT-based devices inside a smart home environment.

Index Terms—Children, cross-border data flows, data protection, GDPR, IoT, minors, smart homes

I. Introduction

In general, smart homes, which are in fact IoT applications [1], are considered to be "a dwelling incorporating a communication network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed" [2]. This actively demonstrates, for the components of smart homes (appliances and devices), that they can interfere with the members of the household smartly [1]. However, it should be mentioned that the definition may be subject to considerable variation due to the technologies which are included [3]. Considering the applications of smart homes concerning the field of the provided services, a basic classification includes home care services, comfort/entertainment sector, energy sector, and security applications [4]. Nevertheless, this classification cannot be considered as restrictive nor strict, as the potentials of smart homes are an evolving field. Smart home devices have been expanding rapidly in household members as consumers and thus data subjects [5]. The initiatives of smart homes, smart cities, and in general the innovations of the field of communications, have emerged alongside risks and restrictions as well [6], [7]. According to B. K. Sovacool and D. D. F. Del Rio [8], the highest number of risks, related to smart homes, is attributed to privacy and security risks under experts' opinions. Inside the smart home environment, the data subjects consist of adults and minors, and therefore of people with different levels of vulnerability concerning privacy risks. Smart home applications would contribute to the improvement of many aspects of minors' education, therapy [9], and entertainment. Children require specialized data protection according to GDPR [1], as they may not be aware of the privacy issues [10], [11] that come with the usage of a smart device. The EU level of data protection has an international reflection for entities, as it applies to data subjects located in the EU and data subjects located outside the EU, when the processing refers to the operations of a controller or a processor inside EU [10]. This suggests that entities located outside the EU (for example USA) as well should take into consideration the presented GDPR requirements, where it is required according to the Article 3 of GDPR. As a consequence, it is thus essential to present the cross-border data flows context. This paper presents a specialized framework for preserving minors' data protection in the environment of smart homes, with emphasis on privacy by design approach.

The rest of this paper is organized as follows. Section II explains the framework of minors' data protection in smart homes, and more specifically subsection A presents the anonymization technique, subsection B presents the privacy by design measures, subsection C analyzes the Data Protection Impact Assessment and subsection D examines the parental control issues, minority and parental consent. Section III focuses on the implications of minors' privacy for cross-border data flows. Section V concludes the paper.

II. The Framework of Minors' Data Protection in Smart Homes

Initially, in order to illustrate the context of minors' data protection inside the smart home environment, it is crucial to specify the obligations established by GDPR and the responsible parties as well. To begin with, the suggested data protection context is not only about the devices and services, which have been designed for

Manuscript received August 17, 2021; revised February 18, 2022.
This work was supported by the Hellenic Foundation for Research and Innovation (HFRI) under the HFRI Ph.D. Fellowship grant (Fellowship Number: 290).
Corresponding author email: kpsannis@uom.edu.gr
doi:10.12720/jcm.17.3.180-187

[1] General Data Protection Regulation [10].

children, but also all the smart home applications that can be offered to minors. As the data controller is the part that have to prove [2] the compliance with the processing principles of GDPR, the data controller is also responsible for implementing the appropriate measures in order to preserve data protection of the minors in the context of the smart home IoT devices.

Regarding the household exception [3] of GDPR, the controllers of smart homes data process them at a professional level and not in private level, excluding this processing from falling into this exception [12]. In fact, it should be pointed out that Article's 2 paragraph 2 (c)[2] GDPR exception refers to the activity regarding the controller of the processing and thus does not concern the activity of the data subjects inside smart homes [13].

The following measures and obligations in subsections A, B, C, and D (established by GDPR) represent the compliance with GDPR when processing [4] concerns children in smart homes environment. These elements are illustrated in Fig. 1, demonstrating their significance and interference.

A. Anonymization

The full data protection, which the data controller should implement, is offered by the anonymization of personal data. GDPR obligations, rights and principles do not apply to anonymous data, which are in fact not related to an identified or identifiable natural person[5]. In this context, it is crucial to mention that smart home IoT devices face evolving technological initiatives, depending on key enabling technologies in the industry. As a result, anonymization is required to be examined regarding the new components of each processing inside smart home applications and thus regularly be reviewed in order to remain an efficient security tool [14]. If anonymization is not applied, all the following measures (subsections B, C, and D) should be implemented.

B. Privacy by Design Measures

The data protection of children should include enhanced privacy by design measures in order to protect their special situation and ensure the proper parental supervision and control, according to subsection D.

GDPR compliance demands the enforcement of technical and organizational measures regarding a specific data processing [6]. These proper measures complement the data processing principles, the obligations and rights of GDPR[7].

C. Data Protection Impact Assessment

At that point, we analyze the obligation of the data controller to conduct a Data Protection Impact Assessment (DPIA), before the processing of minors' personal data inside a smart home environment. DPIA is a risk-based management approach, which assesses the risk of every processing regarding to a specific context. DPIA is mandatory in case of:

(a) systematic and extensive evaluation of personal aspects,

(b) existence of big sensitive data (Article 9),

(c) data about criminal convictions and offences (Article 10), or

(d) systematic monitoring of a publicly accessible area on a large scale[8] [15].

In addition, nine criteria have been adopted, in order to determine the conduction of a DPIA and the establishment of specific lists by the member states at national level [16]. The existence of two or more criteria contributes to high risks and demands a DPIA conduction. In general, the criteria are: evaluation or scoring from personal data, automated decision-making, systematic monitoring, sensitive data or data of a highly personal nature, data processed on a large scale, matching or combining datasets, data concerning vulnerable data subjects, innovative use or applying new technological or organizational solutions, and finally the existence of a processing which prevent data subjects from exercising a right or using a service or a contract.

TABLE I: FACTORS OF THE DPIA CONDUCTION

Factors of IoT-based smart home aspects concerning minors which lead to the conduction of a DPIA
Vulnerability of the children
Systematic processing of big data
Automated decision-making processing
IoT is considered an innovative technology with potential privacy risks

In case of the processing of minors' personal data in the context of smart home applications, as it is presented in Table I, the first criterion which contributes to the conduction of a DPIA, is the vulnerability of the children as data subjects. The children are considered a sensitive category of data subjects for the possibility of higher risks [16], as they might not be able to understand and manage the decisions, which determine the protection of their personal data. Secondly, from the perspective of the kind of processing in relation to the specific technology, smart home IoT devices could include systematic processing of big data and automated decision-making.

[2] [Refer GDPR Article 5 para 2]

[3] '*This Regulation does not apply to the processing of personal data: …by a natural person in the course of a purely personal or household activity'* [Refer GDPR Article 2 para 2 (c)].

[4] *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, 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)].

[5] [Refer GDPR Recital 26]

[6] [Refer GDPR Recital 78]

[7] [Refer GDPR Article 25 para 1]

[8] [Refer GDPR Article 35 para 3]

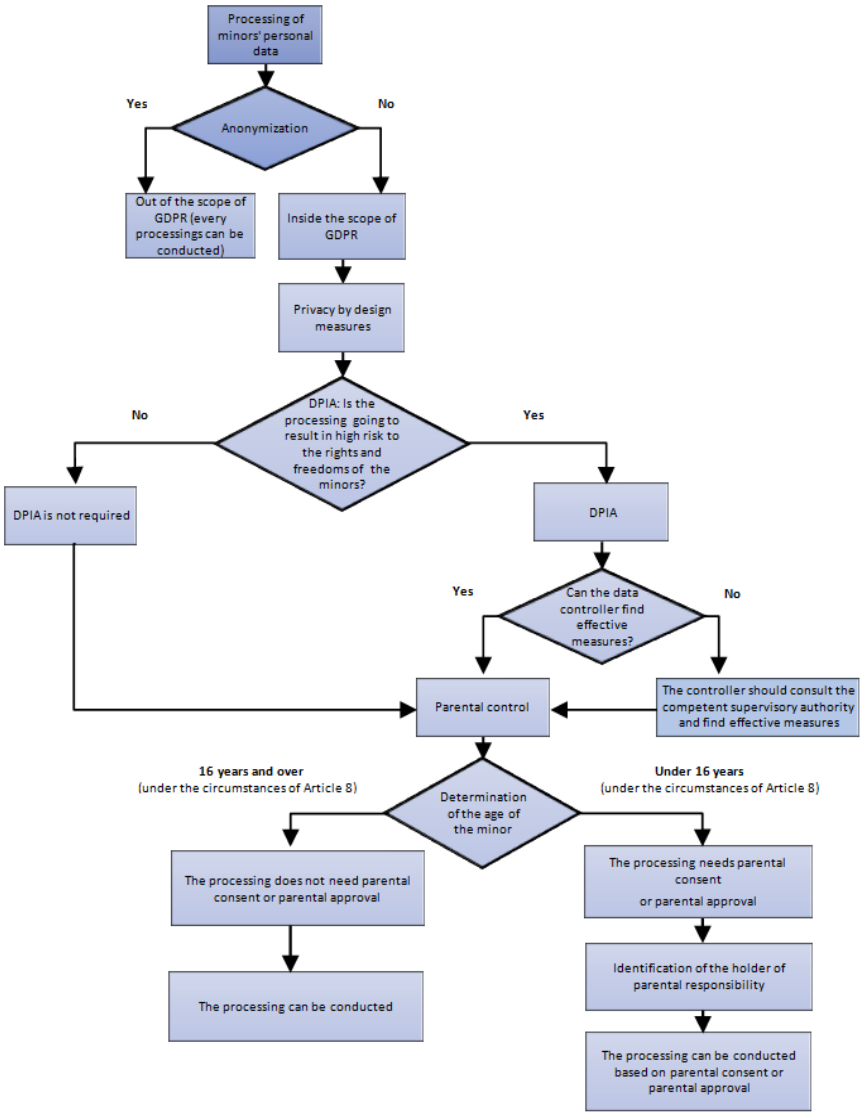

Fig. 1. Minors' data protection measures in IoT-based smart homes

More specifically, the devices of smart homes could continuously process big data due to the nature of their usage, concerning for instance, home security and energy consumption. Automated decision-making processing, including profiling, which has specific protection in Article 22 of GDPR [17] [18], is notably being associated with the data processing of home aspects.

More specifically, home devices can reveal different aspects of the personality of the home members, increasing the potentiality of profiling and targeted advertisement [19]. The required specialized preservation of minors' personal data concerns especially "the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child"[9]. In order to process children's personal data, through automated decision-making, the processing is only allowed under the exceptions of Article 22 paragraph 2 (a), (b) or (c), aiming at protecting the rights, freedoms and legitimate interests of the children [20]. In addition, IoT is considered an innovative technology in the context of this privacy assessment [16].

All these aspects demonstrate the significance of the assessment of privacy risks. As for the DPIA result, it should be mentioned that if the risks maintain after the application of privacy and security measures, the controller should consult the competent supervisory authority [16].

D. Parental Control, Minority and Parental Consent

A very crucial aspect of smart home applications, in relation to children, is parental control issues. Parental controls are tools, which allow parents or guardians to intimate terms on minors' online activity [21]. Not only parental control could limit risks on cybersecurity, but should be placed to reduce privacy risks. The application of parental consent or parental approval of the minors' consent depends on the fact that a minor is the user of a specific application. The identification of the minority

[9] [Refer GDPR Recital 38]

condition therefore, is a prerequisite for all the next steps of lawful processing.

The next level includes the determination of the minors' age. The discovery of the age of a minor plays a vital role in the consent, which could be the legal basis of every processing. Furthermore, another aspect of minors' data protection in smart homes is the identification of the holder of parental responsibility[10]. The consent should be given, not from any adult of the household but from the person that has the custody of the minor. In terms of a child's consent, under the circumstances[11] of Article 8 (1) GDPR, there are two paths based on their age: a) 16 years and over and b) under 16 years of age.

In the first case, the consent of a minor 16 and over is sufficient, while in the second case parental consent or parental approval of minors consent is mandatory [22]. Nevertheless, member states are allowed to set, as in the case of a Directive, the right age limit for mandatory parental consent or approval, with a general threshold of the age of 13 [15]. Accordingly, the Children's Online Privacy Protection Rule (COPPA) of the USA sets the same age limit (13 years old) for the protection of the children. More specifically, the Children's Online Privacy Protection Rule generally demands parental consent with specific exceptions, before the online collection of personal data from minors under 13 [23]. This provision of GDPR, actively demonstrates that data controllers and particularly application developers should recognize and enforce the proper age limit, according to the particular country legislation, where the minor is located [24]. It should be mentioned that if the circumstances[8] of Article 8 (1) GDPR are not applicable, the parental consent should be given according to the national jurisdiction for the minority.

Concerning technical measures, it should be mentioned that the contribution of artificial intelligence has been proposed [21] to the discovery of minors' age. More specifically, in the context of smart homes, the behavior and the choices of a specific user, related to multiple and different types of applications, could be factors that indicate the age of an individual. Therefore, the data, which are processed via smart homes, could contribute to the data privacy of the children as a technical safeguard. However, as artificial intelligence could be included in smart homes privacy measures, consideration must be given to the avoidance of the cases, which are referred to in Recital 38 GDPR, and to the anonymization of these data.

[10] [Refer GDPR Article 8 para 2]

[11] '*…in relation to the offer of information society services directly to a child'* [Refer GDPR Article 8].

III. Practical Implementation and Cross-border Issues

Cross-border[12] data flows are described as "the transfer of personal data to recipients to the jurisdiction of another State or an international organization" [25]. Foreign jurisdictions, in the perspective of the EU, consist of every country outside EEA [13], which includes EU countries and Norway, Iceland, and Liechtenstein [26].

Regarding minors' activity via smart home devices, it is essential to analyze the cross-border ramifications. More precisely, the collection and in general the processing of minors' personal data, in the environment of an IoT-based smart home can contain cross-border data flows. Therefore, if a subsidiary company based in the EEA transfers the minors' data to its parent company outside EEA, then the transfer should be relied upon a GDPR mechanism for international transfers, in addition to the matter of minors' specialized protection, as it is presented in Fig. 2.

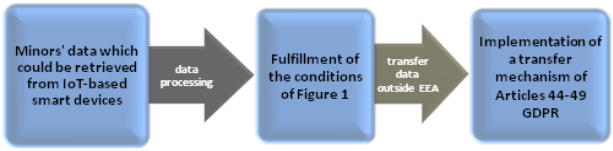

Fig. 2. The stages of minors' data protection

Initially, the cross-border data flows are set out in Articles 44-49 of GDPR. The cross-border data flows can be conducted in case of a European Commission's adequacy decision, regarding the data protection legislation in force in a particular third country (Article 45); appropriate safeguards, such as standard data protection clauses (SCCs) and binding corporate rules (BCRs) provided by the data controller (Article 46); derogations (Article 49), such as an explicit consent [27].

In order to examine the cross-border context of minors' data protection, it is crucial to present the EU approach through recent and selected decisions of different EU national data protection authorities.

A. Evidence from the EU Data Protection Authorities

Firstly, we would like to mention the decision of the Norwegian Data Protection Authority, which has determined an administrative fine of EUR (Euro) [28] 47,500 to a Municipality [29]. More specifically, in the context of a digital learning platform, children's health personal data were being processed. After the notification of a data breach from the controller and thus further investigation, it was found out that the level of security of

[12] *'cross-border processing' means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State* [Refer GDPR article 4(23)].

[13] European Economic Area [26].

the application was not proportionate with the risks. The key elements of the decision refer to the lack of integrated Data Protection Impact Assessment (DPIA) before conducting any processing via the specific application. The decision made it clear that security measures are essential and should be proportionate to the risks related to minors.

Secondly, the Swedish Data Protection Authority has determined an administrative fine of four million SEK (Swedish krona) [30] due to the findings of ineffectual data security measures in an information technology system regarding minors' personal data [31]. Regarding this decision, it was noted that the continuous evaluation of the level of protection is of key importance in the context of big data processing.

In addition, the Italian Data Protection Authority recently decided to limit the processing of an online application [32], concerning the data subjects whose age could not be ascertained. As a result, the examination of the age of a minor under EU legislation is a prerequisite for the lawful processing of minors' personal data. Apart from the main issue of the case, it should be mentioned that the decision noticed that the application has recently informed about its main establishment's registration in the EU. This establishment transfer may result in the GDPR implementation and thus the avoidance of cross-border limitations to third countries.

The identification of cross-border transfers and their mechanisms were also pointed out in the Proceedings of the Italian Data Protection Authority about a social network [33].

B. Cross-border Mechanisms and Minors' Data Protection

To begin with, the first mechanism of cross-border data flows is a European Commission's adequacy decision for the third country, which consists of the European Commission's assessment of the level of data protection in the third country [34]-[36]. This assessment is extensive and could contain several aspects of the obligations and rights of GDPR, including the provisions that protect minors. For example, in the European Commission's adequacy decision for the United Kingdom, is being inspected whether the age limit for minors' consent under Article 8 is compatible with GDPR [37]. This reference, which was confirmed to be within the limits of GDPR, demonstrates that the assessment in the context of the adoption of an adequacy decision takes into account the data protection legislation regarding minors.

If there is no adequacy decision about a country, which is going to import personal data, then the data controller should use the appropriate safeguards of Article 46. This transfer rule demands an assessment of the effectiveness of the selected tool, among those which are mentioned in this rule, regarding all the aspects of the particular transfer [27]. This safeguard rule, in the case of IoT-based smart home devices used by minors, should take into consideration the third country's general data protection about minors. If the minors' data protection is compatible with EU legislation, a transfer tool of Article 46 could be used for the transfer. In another case, the controller should enforce further measures, such as the adoption of security policies [27].

In parallel, and more specifically in the case of the transfer tool of binding corporate rules (BCRs) of Article 46, it should be approved by the competent supervisory authority. In this context, it should be mentioned that data protection of children is included in the list of the proposed form for BCRs of the Article 29 Data Protection Working Party [38]. Therefore, it is concluded that the treatment of minors' data protection via smart home applications, in the case of BCRs, should be reflected by the text of the BCRs.

Moreover, if there are neither adequacy decisions nor safeguards, the data transfer should be based on the derogations of Article 49 [39]-[41]. It is worth noting that especially the condition of Article 49 paragraph 1 (f), where the intended transfer is necessary to protect the vital interests of the data subject or other people (in case of data subjects who are physically or legally incapable of giving consent), may refer to the legal incapability of the minors, depending on the national jurisdiction [42].

IV. Conclusion

This research work intended to present the framework of minors' data protection, according to GDPR, by combining the technological and legal field through supporting ICT specialists in designing and applying the security and privacy walls on smart home applications, especially in terms of the specialized data protection, which is essential for minors. Moreover, the research presented the cross-border aspects of the framework.

More specifically, the aim of the study is the clarification of the data protection measures of practical implementation, which are the key challenges of minors' data protection via smart homes. In parallel, it should be mentioned that the presented framework has a privacy by design dimension, in order to provoke the establishment of an integrated treatment for minors' data protection rights.

In the next step of our research, we intend to examine the specific privacy by design measures that could ensure parental control over the IoT environment.

Acknowledgment

The research work was supported by the Hellenic Foundation for Research and Innovation (HFRI) under the HFRI PhD Fellowship grant (Fellowship Number: 290). All the websites in this paper were accessed on 7 November 2021.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

All the authors contributed for the paper and approved the final version of the paper.

References

[1] Q. F. Hassan ed., *Internet of things A to Z: Technologies and Applications*, John Wiley & Sons-IEEE Press, 2018.

[2] N. King, Smart Home – a Definition, *Intertek Research and Testing Center*, 2003, pp. 1–6.

[3] J. Bugeja, "On privacy and security in smart connected homes," Doctoral dissertation, Malmö University 2021.

[4] C. Badica, M. Brezovan, and A. Badica, "An overview of smart home environments: Architectures, technologies and applications," *BCI (Local)*, 2013.

[5] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," in *Proc. ACM on Human-Computer Interaction, (CSCW)*, 2018, pp. 1-20.

[6] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, pp. 174-184, 2018.

[7] V. A. Memos, K. E. Psannis, Y. Ishibashi, B. G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," *Future Generation Computer Systems*, pp. 619-628, 2018.

[8] B. K. Sovacool and D. D. F. D. Rio, "Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies," *Renewable and Sustainable Energy Reviews*, p. 109663, 2020.

[9] J. Berrezueta-Guzman, I. Pau, M. L. Martín-Ruiz, and N. Máximo-Bocanegra, "Smart-Home environment to support homework activities for children," *IEEE Access*, vol. 8, pp. 160251-160267, 2020.

[10] 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).

[11] E. Alexandropoulou-Egyptiadou, "The General Data Protection Regulation 2016/679/EU-Challenges of implementation," in *Proc. 1st Interdisciplinary Conference 'Law and Informatics: Addressing the digital era's challenges'*, Komotini, Greece, May 2018, pp. 17-30.

[12] J. Chen, L. Edwards, L. Urquhart, and D. McAuley, "Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption," *International Data Privacy Law*, 2020.

[13] CJEU, *Judgment of the Court (Fourth Chamber) of 11 December 2014, in Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů*.

[14] Council of Europe, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01, Strasbourg.

[15] 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.

[16] Article 29 Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk, for the purposes of Regulation 2016/679," WP 250.

[17] 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.

[18] F. J. Zuiderveen Borgesius, "Strengthening legal protection against discrimination by algorithms and artificial intelligence," *The International Journal of Human Rights*, pp. 1-22, 2020.

[19] J. Bugeja and A. Jacobsson, "On the design of a privacy-centered data lifecycle for smart living spaces," *IFIP International Summer School on Privacy and Identity Management*, Springer, Cham, August 2019, pp. 126-141.

[20] Article 29 Working Party. Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679. WP 251.

[21] Information Commissioner's Office. Age Appropriate Design: A Code of Practice for Online Services.

[22] E. Alexandropoulou-Egyptiadou, "Minors' data protection according to GDPR," *DiMEE*, vol. 1, pp. 5-19, 2018.

[23] Federal Trade Commission. Complying with COPPA: frequently asked questions.

[24] Article 29 Working Party. Opinion 02/2013 on Apps on Smart Devices, WP202.

[25] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (223/2018), Article 102.

[26] European Economic Area (EEA). Relations with the EU.

[27] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Brussels.

[28] Eurostat. Tutorial: Symbols and abbreviations.

[29] Norwegian Data Protection Authority. Final decision, administrative fine for Rælingen municipality.

[30] European Central Bank. Euro Foreign Exchange Reference Rates.

[31] Swedish Authority for Privacy Protection. Serious Deficiencies in the Stockholm online School Platform.

[32] Italian Data Protection Authority (Garante per la protezione dei dati personali). Tik Tok: Italian SA imposes Limitation on Processing After the Death of the Girl from Palermo.

[33] Italian Data Protection Authority (Garante per la protezione dei dati personali), Tik Tok Endangers Children's Privacy: Italian Dpa Initiates Proceedings Against the Social Network.

[34] *Handbook on European Data Protection Law*, 2018 edition, Publications Office of the European Union, Luxembourg, 2018.

[35] 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.
[36] J. Wagner, "The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?" *International Data Privacy Law*, vol. *8*, pp. 318–337, 2018.
[37] European Commission. Decision on the Adequate Protection of Personal Data by the United Kingdom - General Data Protection Regulation.
[38] Article 29 Data Protection Working Party. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data. WP264.
[39] I. Ntouvas, "Exporting Personal Data to EU-based International Organizations under the GDPR," *International Data Privacy Law*, vol. 9, pp. 272-284, 2019.
[40] W. G. Voss, "Cross-border data flows, the GDPR, and data governance," *Washington International Law Journal*, vol. 29, pp. 485-532, 2019.
[41] C. Sullivan, "EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era," *Computer Law & Security Review, vol. 35*, pp. 380-397, 2019.
[42] European Data Protection Board. Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679.

Stavroula Rizou was born in Thessaloniki, Greece. She graduated from Law School of Aristotle University of Thessaloniki in 2015 and she completed her Master's degree in Accounting and Finance in 2016, with a major in Finance, at the University of Macedonia, Department of Business Administration. Currently, she conducts PhD research on the legal framework of cross-border transfer of personal financial data, as a PhD Candidate at University of Macedonia, Department of Applied Informatics. She has received a PhD Fellowship grant (Fellowship Number: 290) from Hellenic Foundation for Research and Innovation (HFRI) in 2019.

Eugenia Alexandropoulou-Egyptiadou, currently Vice Rector and former Deputy Rector of the University of Macedonia (Thessaloniki, Greece), is Professor in I.T. Law at the Department of Applied Informatics, founder of the I.T. Law Scientific Group, www.itlaw.uom.gr and Director of the postgraduate Program (Master) in "Law and Informatics", www.mli.uom.gr. A former attorney at law at 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, Labour, 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 organizer, chair person and 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.

Yutaka Ishibashi received the B.E., M.E., and Ph.D. degrees from Nagoya Institute of Technology, Nagoya, Japan, in 1981, 1983, and 1990, respectively. In 1983, he joined the Nippon Telegraph and Telephone Public Corporation (currently, NTT) Laboratories. From 1993 to 2001, he served as an Associate Professor of Faculty of Engineering, Nagoya Institute of Technology. Currently, he is a Professor of Graduate School of Engineering, Nagoya Institute of Technology. From June 2000 to March 2001, he was a visiting researcher, Department of Computer Science and Engineering, University of South Florida (USF), USA. He was the Head of Department of Computer Science, Nagoya Institute of Technology from 2005 to 2006 and from 2007 to 2009. He was a College Director at Nagoya Institute of Technology from 2016 to 2020. His research interests include networked multimedia, QoS (Quality of Service) control, and remote robot control with force feedback. He was the Chair of the IEICE Communication Quality (CQ) Technical Committee from 2007 to 2009. He served as TPC Chair of IEEE CQR (Communications Quality and Reliability) Workshop in 2011 and 2012. He also served as ACM NetGames (Network and Systems Support for Games) Workshop Co-Chair in 2006, 2010, 2014, and 2017, Executive Committee Chair of Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering in Japan, Chair of IEEE MAW 2017 (Metro Area Workshop in Nagoya, 2017), and so on. He was further IEEE Nagoya Section Chair in 2017 and 2018 and the Chair of ITE (The Institute of Image Information and Television Engineers) Tokai Section in 2020 and 2021. He is currently a Vice President of ITE. He is a Senior Member of IEEE, a Fellow of IEICE, and a Member of ACM, ITE, IPSJ, VRSJ, and IEEJ.

Konstantinos E. Psannis was born and raised in Thessaloniki, Greece. He is currently Associate Professor in Communications Systems and Networking at the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, Director of Mobility2net Research & Development & Consulting JP-EU

Lab, member of the EU-JAPAN Centre for Industrial Cooperation and Visiting Consultant Professor, Graduate School of Engineering, Nagoya Institute of Technology, Nagoya 466-8555, Japan.

Konstantinos received a degree in Physics, Faculty of Sciences, from Aristotle University of Thessaloniki, Greece, and the Ph.D. degree from the School of Engineering and Design, Department of Electronic and Computer Engineering of Brunel University, London, UK. From 2001 to 2002 he was awarded the British Chevening scholarship. The Chevening Scholarships are the UK government's global scholarship programme, funded by the Foreign and Commonwealth Office (FCO) and partner organisations. The programme makes awards to outstanding scholars with leadership potential from around the world to study at universities in the UK.

Dr. Psannis' 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 organisations.

Dr. Psannis has participated in joint research works funded by Grant-in-Aid for Scientific Research, Japan Society for the Promotion of Science (JSPS), KAKENHI Grant, The Telecommunications Advancement Foundation, International Information Science Foundation, as a Principal Investigator and Visiting Consultant Professor in Nagoya Institute of Technology, Japan. Konstantinos E. Psannis was invited to speak on the EU-Japan Co-ordinated Call Preparatory meeting, Green & Content Centric Networking (CCN), organized by European Commission (EC) and National Institute of Information and Communications Technology (NICT)/Ministry of Internal Affairs and Communications (MIC), 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. Konstantinos 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 (CS), July 2011. Dr. Psannis has more than 70 publications in international scientific journals and more than 100 publications in international conferences, 20 Book Chapters and 11 Technical Reports and received more than 3800 citations (h-index 27, i10-index 56). Professor Konstantinos has several highly cited papers powered by Web of Science - Clarivate.

Dr. Psannis supervises three post-doc students and eight PhD students. Prof. Konstantinos E. Psannis is serving as an Associate Editor for IEEE Access and IEEE Communications Letters. He is 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 TPC Co-Chair at the International Conference on Computer Communications and the Internet (ICCCI 2020), Nagoya Institute of Technology Japan, ICCCI 2020, June 26-29 at Nagoya, Japan, and will be held in 2021 June 25-27, at Nagoya, [http://iccci.org/] and Conference Chair at the World Symposium on Communications Engineering held at University of Macedonia, Thessaloniki, Greece, October 9-11, 2020 and to be held at University of Macedonia, November 25-28, 2021, Thessaloniki, Greece (WSCE 2021 - http://wsce.org/). Professor Konstantinos E. Psannis 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).