IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal
SPECIAL SECTION ON FUTURE GENERATION SMART CITIES RESEARCH: SERVICES, APPLICATIONS, CASE STUDIES AND POLICYMAKING CONSIDERATIONS FOR WELL-BEING [PART II]

Received April 25, 2020, accepted May 25, 2020, date of publication June 8, 2020, date of current version June 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3000662

GDPR Interference With Next Generation 5G and IoT Networks

STAVROULA RIZOU, EUGENIA ALEXANDROPOULOU-EGYPTIADOU, AND KONSTANTINOS E. PSANNIS, (Member, IEEE)
Department of Applied Informatics, School of Information Sciences, University of Macedonia, 54636 Thessaloniki, Greece

Corresponding author: Konstantinos E. Psannis (kpsannis@uom.edu.gr)

The research work was supported by the Hellenic Foundation for Research and Innovation (HFRI) under the HFRI PhD Fellowship grant (Fellowship Number: 290).

ABSTRACT This article examines the specific data protection framework with regards to 5G networks, which is the current high-end evolution of the previous four generations of cellular technology networks. Taking into consideration practical issues, that have emerged from 5G (Fifth Generation) technology, the scope is the presentation of legal solutions. As this digital mobile transformation will begin from 2020, affecting applications of a wide range of services in energy sector, transport services, banking sector, health field, as well as in industrial control systems, and progressively in everyday life through all smart devices. It is crucial to specialize and sum up the interference between European data protection legal framework and 5G networks, in order to provide a new path to the addressing issues.

INDEX TERMS Data privacy, 5G networks, GDPR, the IoT.

I. INTRODUCTION

The evolution of digital applications and hence the possibilities offered to both individuals and entities, aiming primarily at economic progress, has made integral the introduction of specialized legal protection and clarification of the existing privacy framework. The above-mentioned requirements are of key importance, so that 5G (Fifth Generation) is fully implemented to achieve its goals: monitoring communications and supporting applications. In many circumstances, 5G function could require the cooperation of numerous network providers, both at home and abroad, under different jurisdictions. Initially the cross-border dimension of 5G technology raises the issue of EU[1] and international law harmonization and cooperation [1]. Beyond this worldwide technical base of 5G, the EU legislation has widened the EU territorial privacy borders, as not only companies and individuals [2] in the EU have to comply with GDPR but also the non-EU based entities and individuals, as the focus has now shifted to where the data subject is located as well as to data processing of people living inside EU [3].

This paper presents the interaction of European data protection law on applications dealing with 5G, analyzing through top down approach the legal instruments based on Regulation (EU) 2016/679 (the 'GDPR'), which is one of the strictest and most accurate privacy laws worldwide.

Primarily, personal data consist in any information concerning an identified or identifiable natural person [GDPR article 4 PR 1], including IP address[2] and cookies.[3] The 5G, which will have been spread across the spectrum of IoT [5], is going to come with the access of mobile and fixed Internet at broadband speeds of the order of 10 Gbps, about a hundred times faster than theoretically possible with the current generation [6]. As a result, the transition of large data will rapidly increase now more than ever. It is worthwhile to make specific legal issues clearer for privacy, such as the main data processing principles, the data subject's rights, the controller's obligations, the international transfers of personal data and the preventive methods of security privacy matters through the design phase of a system or a method.

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel Jesus Torres Ruiz.

[1]More specifically, GDPR applies to European Economic Area (EEA) [4], which includes EU countries and Norway, Iceland and Liechtenstein.

[2]Internet protocol: the technical rules that control communication on the internet [https://dictionary.cambridge.org/dictionary/english/ip]

[3]A piece of information stored on a computer about viewed internet documents [https://dictionary.cambridge.org/dictionary/english/cookie?q=COOKIES]

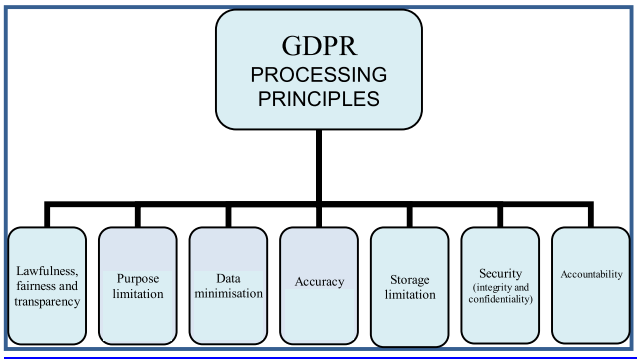

FIGURE 1. GDPR processing principles.

II. DATA PROTECTION PROCESSING PRINCIPLES[4] ACCORDING TO GDPR

In order to illustrate the data protection context regarding 5G networks, it is crucial to clarify the seven data processing principles as reported by GDPR. The seven basic principles, presented in article 5 of the GDPR, except from defining the data subject's[5] rights and data controller's[6] (e.g. a company) and data processor's[7] obligations, also apply to the specific type of data processing, that compose a separate chapter of GDPR, the cross-border[8] data transfers.

A. SEVEN PROCESSING PRINCIPLES

The below graphic demonstrates, the defined seven processing principles, according to GDPR, underpinning obligations and rights.

1) LAWFULNESS, FAIRNESS AND TRANSPARENCY

Lawfulness of the processing lies to the principle of legality of a very specific legal purpose of the processing [7], based on a specific legal basis that should have been defined. Lawful processing requires the consent[9] of the data subject or another legitimate way. Besides consent, article 6 (1) of the GDPR includes five additional lawful processing bases (for the performance of a contract, in the exercise of public authority, for compliance with a legal obligation, for the legitimate interests of the controller or third parties,[10] or if necessary to the vital interests of the data subject) [8]. As for fairness and the transparency of any procedure of processing, are about unhidden data processing and informed data subjects and public authorities in order to be able to exercise their rights and examine the GDPR compliance respectively.

2) PURPOSE LIMITATION

The limitation principle underlining that personal data collected for a particular purpose can only be further processed for a purpose compatible with the primary collection purpose; in addition, it is noted that every next processing, beside being proven compatible, has to be based on another legal basis of the article 6 of the GDPR (i.e., a new valid consent) [9].

3) DATA MINIMIZATION

An utterance of proportionality principle is data minimization, with contributions to several directions. More specifically, it is about the kind and the mass of the personal data, referring directly to the necessity of any processing. In other words, this necessity requirement not only refers to the quantity, but also to the quality (i.e. data sensitivity or impact) [10].

4) ACCURACY

The condition and the quality of personal data protected by the accuracy principle, impose the controller to maintain and process only correct personal data, amending the incorrect parts or deleting the wrong or no longer applicable data without delay.

5) STORAGE LIMITATION

The storage limitation is the second principle, determined by proportionality (what is necessary) and refers to the limited duration of the conservation of personal data; [11] through the specific period of time, personal data may be retained and then be deleted after its intended use [12]. Moreover, GDPR encourages the establishment of time limits by the controller. (Recital 39)

6) SECURITY (INTEGRITY AND CONFIDENTIALITY)

Security is aimed at ensuring the 'integrity' and 'availability' of personal data. Data should be accessible to the responsible parties. They should not be changed or deleted by unauthorized persons. This triplet, 'confidentiality, integrity and

[4] '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)].

[5] Personal data means any information relating to an identified or identifiable natural person 'data subject' [Refer GDPR article 4(1)].

[6] 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data [Refer GDPR article 4(7)].

[7] 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [Refer GDPR article 4(8)].

[8] '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)].

[9] 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [Refer GDPR article 4(11)].

[10] 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data [Refer GDPR article 4(10)].

availability', has been presented as a duty to secure personal data [13]. Examples of harmonization measures with security requirements are: (a) pseudonymization (b) anonymization (c) the ability to restore data after an incident; and (d) the ability to redefine and constantly review all the security measures that have been taken into action [10].

7) ACCOUNTABILITY

The obligation for controllers to demonstrate that any processing is in compliance with the legal rules for data protection [14]. It is obvious that the accountability principle is one of the basic controller's responsibilities among with these described in Chapter IV (GDPR).

III. 5G AND GDPR

To this point, it is essential to represent the initiatives of the fifth-generation (5G) mobile communication technology, from the previous 4G and to try to examine the existence of the interrelation with GDPR obligations and rights.

A. 5G INITIATIVES RELATED TO PRIVACY ISSUES

The 5G innovations [15], forming the point of interest to privacy matters are the following:

- Higher data rates: 4G networks offer the maximum peak data rate (maximum achievable data rate for a user under ideal conditions) of 1Gbps and the maximum user experienced data rate (achievable data rate for a user in the real network environment) of around 10 Mbps. In 5G networks the peak data rate is expected to be enhanced by up to 20 Gbps and the user experienced data rate will be improved 100 times over 4G networks and reach up to 1 Gbps [16].
- Higher traffic density: as a result of massive MIMO[11] antennas and millimeter wave communication technologies [17]; although 5G ultra-dense cellular network is still a density-limited communication system [18].
- Higher reliability: the capability of guaranteeing the success rate of data transmission under stated conditions over a certain period of time (5G expected rate of up to 99.999%) [19].
- Lower latency; massive MIMO have decreased the latency. More specifically, the 5G system is expected to reduce the latency ten times in the user plane, down to 1 millisecond, and half in the control plane, down to 50 milliseconds, compared to the 4G system [20].
- Connectivity for many more devices: 5G would support a connection density of up to 1 billion connected devices per square kilometer, 100 times more devices compared to 4G networks [19].
- Lower power in support of the Internet-of-Things (IoT): 5G networks would be 100 times more energy efficient than 4G networks [19], resulting in Iot devices growth.

[11] Massive MIMO is a technology that uses arrays of antennas containing few hundred antennas which are at the same time in one time, frequency slot serving many tens of user terminals, extracting all the benefits of MIMO but on a larger scale [18].

Nevertheless, the fact that 5G mobile communication technology is still IP-based [21], could be an effective factor to privacy concerns, since the allocation of IP addresses could result in other personal data as well.

B. GDPR RIGHTS AND OBLIGATIONS

The liabilities that arise from GDPR data protection obligations separated by GDPR to data subject's rights and data controller's (e.g. a company) and data processor's obligations.

1) SUBJECT'S RIGHTS

RIGHT TO BE INFORMED (ARTICLE 13,14)

It is the pinnacle of data protection rights, as without proper information given to the data subjects it is not possible to exercise their other rights as well. The key is the transparent process of personal data [22].

2) RIGHT OF ACCESS (ARTICLE 15)

Data subjects have the right to access their personal data and certain information, given by the controller, concerning the processing. This right constitutes an integral part of the European data protection law [23].

3) RIGHT TO RECTIFICATION (ARTICLE 16)

The right to have their personal data in the correct form; pointing directly to the accuracy principle (Recital 65 GDPR).

4) RIGHT TO BE FORGOTTEN (ARTICLE 17)

The right to demand the erasure of data subject's personal data without undue delay. The right to be forgotten was established at first place before GDPR in the case "*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*" by the European Court of Justice [24].

5) RIGHT TO RESTRICTION OF PROCESSING (ARTICLE 18)

Another right in the context of data subject's fully supervision and control of personal data, is the right to restrict the processing of personal data for a specific period.

6) RIGHT TO BE NOTIFIED REGARDING THE RECTIFICATION OR ERASURE OF PERSONAL DATA OR PROCESSING RESTRICTION (ARTICLE 19)

Data subject must be noticed about any rectification or erasure of personal data or any restriction of processing regarding to any receiver, to that degree this notification is neither impossible nor disproportionate [25].

7) RIGHT TO DATA PORTABILITY (ARTICLE 20)

This right concerns the transmission, mobility and the flexibility of personal data, by providing data subjects the right to receive their personal data, in a structured, commonly used and machine-readable format [26], and forwarding those data to other controllers.

8) RIGHT TO OBJECT (ARTICLE 21)

Data subjects can invoke their right to object to personal data processing [9]. An important expression of this right, is the obligation for the controller to provide the means for submitting requests electronically and to respond to these requests promptly and till one month at the latest, in addition to providing explanations in case of non compliance with any such requests (Recital 59).The difference between the right to object and withdrawal of consent refers to the processing legal basis; especially the withdrawal of consent requires the consent as processing legal basis, while the right to object may refer to any processing legal basis.

9) RIGHT NOT TO BE SUBJECT TO AN AUTOMATED DECISION –MAKING PROCESSING (ARTICLE 22)

In general, processing that includes automated decision-making, including profiling, is prohibited by GDPR [27], and is allowed only in case of human intervention during the procedure, data's subject's consent or existence of a contract, or support from Member State law or EU law [10].

C. SUBJECT'S CONSENT

Subject's consent as a legal basis for lawful processing, is one of most common ways to perform in practice the processing of personal data and is one of the controller's obligations to prove this given consent.

Explicit consent is mandatory for processing special categories of data, the cross-border data transfers to third countries and on automated individual decision-making, including profiling [22].

Withdrawal of consent is as important as consent, making impossible the process of personal data for the future and demanding the erasure of these data, if the process is not based on another legal basis.

1) CHILD CONSENT

The provision of 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. 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 essential [28]. However GDPR leaves up to the national 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.

D. SECURITY OF PERSONAL DATA (ARTICLES 25, 32-35)

GDPR ensures security, urging on pseudonymisation and anonymization, both further expressions of privacy by design complementary principle to data minimization principle (Article 25), expression of internal control of the security level of privacy. There are four criteria for privacy by design: (a) data minimization, (b) minimum extent of the processing, (c) time storage minimization and (d) minimum accessibility) [29].

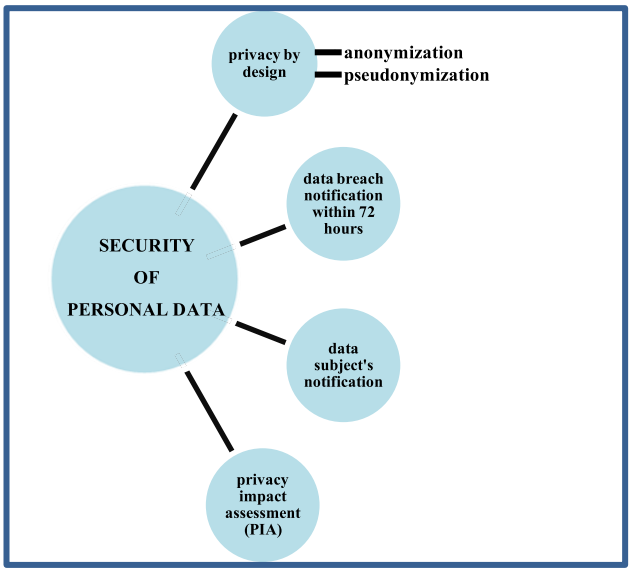

FIGURE 2. GDPR security measures.

Furthermore, GDPR states the very important obligation for the controller, to notify the supervisory authority of a personal data breach within 72 hours, or to justify the further delay above this time limit, while the data subject, often subjects, must be notified in case of high risk effect of a data breach on data subject rights (Recital 86) [30].

Privacy impact assessment (PIA) is a risk management approach which complement the privacy by design context [31], [32], evaluating the risk of every processing regarding to a specific initiative. PIA is necessarily carried out especially, in case of a (a) systematic and extensive evaluation of personal aspects (profiling), (b) existence of big data sensitive (Article 9) or (c) data about criminal convictions and offences (Article 10) and (d) a systematic monitoring of a publicly accessible area on a large scale. If PIA result indicates high risk, rises the controller's obligation to consult the competent supervisory authority before every processing.

E. CROSS BORDER DATA FLOWS (ARTICLES 45-49)

The transfer of personal data outside EU, is prohibited unless the country that receives the data has been considered to be ''adequate'' to European data protection law, or companies have a data transfer mechanism, such as Binding Corporate Rules [10], or controller provide appropriate safeguards or can rely on a statutory derogation. It is obvious that GDPR, has an international impact even being a European Regulation [33].

IV. CORRELATION BETWEEN 5G TECHNOLOGY AND GDPR OBLIGATIONS AND RIGHTS

5G new technology shifts and focuses interest on the above mentioned seven 5G initiatives related to privacy issues. Due to these technical characteristics, 5G networks are expected to serve a wide range of applications and sectors (such as

TABLE 1. Correlation between 5G technology and GDPR obligations and rights.

	High speed data rates	High traffic density	Massive number of connected devices (Iot)	IP-based
Right to be informed	X		X	
Right of access			X	
Right to rectification	X		X	
Right to be forgotten	X		X	
Right to restriction of processing	X		X	
Right to be notified about rectification or erasure	X		X	
Right to data portability			X	
Right to object			X	
Right to deter automated decision –making	X	X	X	X
Subject's consent and withdrawal of consent			X	
Child consent			X	
Privacy by design		X	X	X
Breach Notification within 72h	X		X	
Privacy impact assessment (PIA)	X	X	X	
Location privacy		X		X

energy, transport, banking, and health, industrial control systems, elections) [34], and result in a huge volume of data [35]. In consequence, the initiatives of 5G networks would contribute to the data subjects' capability of creating and spreading more personal data on the web [36]. It should be noted that, the important differences, compared with threats to existing networks, would be the nature and intensity of potential impacts of privacy threats, thanks to 5G wider intrusion into economic and societal functions via its performance initiatives [34].

In terms of practical implementation, the bellow Table 1 presents substantial new elements that 5G brings, in correlation with main and of practical significance GDPR rights and obligations, based on the specific nature and intensity of 5G characteristics impacts. It should be mentioned that next generation wireless technology would under circumstances, affect on every GDPR liability; the Table 1 presents the most affected GDPR obligations and rights under 5G.

A. HIGH SPEED DATA RATES

This upgrade of 5G, regarding to 4G, will serve users with data rates of several Gbps and will enhance new mobile applications [37]. In particular, new applications of 5G networks such as real-time multi-user gaming, virtual/augmented reality (VR/AR), 3D multi-site telepresence, ultra-high resolution video streaming and photo-video sharing, require an increase in existing networks data rates [38]. As a result, it is crucial to clarify how the performance of higher speeds, because of new applications and capabilities inside 5G environment, would affect every GDPR main requirement. Moreover, high data speed would lead to huge volume of data [35], and as a result to huge volume of data processing. Big data privacy risks are generally related to its "three Vs": (a) volume refers to the amount of data processed, (b) velocity refers to the speed of data and (c) variety to the number and diversity of types of data [8]. Although, the estimation of the extent to which personal data may be affected is not possible [8], in case of big data and extended data processing in 5G networks, it is possible to present an assessment of rights and obligations that demand attention in order to fulfill GDPR requirements.

Higher speeds would result in de facto failure to inform the data subject about the elements of their data processing, in response to unmanageable amount of data processing through 5G networks instead of 4G networks.

High data rates could also affect on rectification and erasure rights (right to rectification, right to be forgotten, right to restriction of processing, right to be notified about rectification or erasure), because of the fast transmission and sharing of data.

Furthermore, excessive amount of data processing, which occurred without human intervention, arises dramatic privacy concerns, through profiling of data subjects.

Meanwhile, faster transmission of personal data, could reduce the potential safeguard of mandatory notification of a data breach targeting on the restriction of damage. Precisely, the 72h time limit aims at data breach reduction; with new higher speeds, the mandatory report to the supervisory authority, even after this time limit, is going to affect the reported impact of a data breach. Additionally, when the data breach is considered to be notably severe for subjects' rights, it is mandatory to notify the subjects apart from the supervisory authority (Article 34). Taking into consideration the forthcoming faster data spreads and, as a result, qualitative important data as well, the requirement of subjects' notification would be a regular enforcing, in case of a data breach.

As for PIA conduction, conditionally under this new technology, PIA is mandatory as result of high privacy risks. Higher speeds would be considered as an affective factor of the context of these risks, as set out in Article 35 GDPR.

B. HIGH TRAFFIC DENSITY

5G networks will be denser and of higher capacity than current 4G technology, using Massive MIMO technology [39]. Due to the high density of small cells, the knowledge of the cell, which is associated with a data subject, can easily reveal the location information of that subject [40]. Densification would bring out location privacy issues, affecting therefore further GDPR obligations and rights. The below clarification shows the legal issues that arise and measures that have to be taken, in order to preserve data protection from location tracking inside dense 5G networks.

More specifically, a key point of 5G relating to density is high-efficiency device positioning and localization. Extracting and tracking the precise location of the device's user, except from providing more capabilities for location-based applications [41], could definitely bring out location privacy vulnerabilities as more personal data about subject's location transmitted, that would also can reveal or influence further personal data by cross-checking information about a location.

As a result, possible identification of personal data could be used for profiling and tracking.

As it is likely to face automated decision-making through profiling under denser networks, which could detect an exact location of data subjects, it is crucial to deter the existence of profiling in order to conduct a PIA before every processing [42].

Moreover, defaults aiming at data protection, during the designing or redesigning process of an IT system, should from the time that will face 5G networks, take into account during protection defaults making, the way an application or device processes the subject's personal data (e.g. location data, access to device files or applications, sensitive personal data). In other words, every new feasibility coming with 5G, should be analyzed via technical basis and take into consideration separately, especially for the above mentioned privacy by design criterion (d), defining the minimum accessibility the personal data [43], and also arising from the principle of data minimization.

C. MASSIVE NUMBER OF CONNECTED DEVICES (IoT)

5G networks are expected to support 100 times more devices compared to the 4G networks [19]. 5G will definitely interfere with both accomplished and forthcoming massive IoT, in which exists apart from user to device, more efficient device to device communication without any human involvement [44]. 5G new characteristics, mentioned above, such as lower latency, lower power, high reliability and high user speeds will develop, ameliorate and affect IoT [45]. Furthermore, 5G new antennas technology in NB-IoT[12] wireless access emerging technology will decrease the power requirements by about 10% in average [39].

[12]Narrowband Internet of Things (NB-IoT) is a technology based on cellular IoT, which supports massive device connections, wide area coverage, ultra-low power consumption, and ultra-lowcost [46].

The access in one device connected to another can put the personal data shared by this device are at risk [35]. The volume of data and the processing way would change with 5G due to the new characteristics of bigger amount of new devices, higher connectivity between devices, and as result big data.

In this context, the exercise of subjects' rights seems notably complicated to even unreachable. More specifically, inside the IoT environment, it is in most of the times unclear, who has the right of accessing and collecting data from different devices [9], and in general conducting any form of processing. In addition, it is respectively inconclusive for data subjects to exercise their rights [47] (the right to be informed, the right to access, the right to rectification, the right to be forgotten, the right to restriction, the right to be notified about erasure, the right to data portability, the right to object), due to the fact of not knowing data's content, the kind of processing, and the responsible data controller and data processor. It is important to mention the significance, in such a complex framework, of the obligation for the data controller to inform the data subjects about the exact way their data are being used.

Moreover, the withdrawal of consent should be equally easy for the data subject. However, this is difficult and essential to a sharing platform.

Minors' consent, in IoT is extremely important both for privacy and for the cyber protection of the children. It is an issue, how to ensure in practice the parental consent (for minors under 16 or less, up to 13), when different family members own and manage, through different accounts (even confirmed to be used by adults) many smart devices. Above valid consent, it is questioned the extent and the scope of the given consent, as IoT-enabled toys or generally devices designed for the purpose of recording and storing records of young children's conversations could process unlimited personal data [48]. Parental control issues, which have been addressed already in 4G networks [49], must precede parental consent. Parental consent must be given after providing the necessary information about every data processing and verifying of minors' age and custody, under the responsibility of data controller.

On the basis of given content for a lawful processing, the multiple data and processing operated via IoT could challenge the GDPR requirement for clear and informed consent [9], related to a specific data processing.

As for automated decision-making processing, it is of key importance to ensure the appropriate information to IoT users in order to understand the consequences of such processing for them [47], as among the mass number of devices it is easier, from a larger number of information sources, to cross-referencing different aspects of an individual's personality, behavior, interests and habits, that can be analyzed and valued [27].

As for the data breach notification and especially to data breach report, it is noticeable to focus on the process of the record of each data breach. Particularly within IoT context, it is possible to face multiple data breaches from as single

cause, via different devices and with different content. This situation complicates and delays the record of the incidents, because every data breach is recordable, as different types of personal data, breached in different ways should be recorded separately [50].

Regarding to big data, potentially sensitive, and within the IoT context, the practical example of demonstrating compliance with these GDPR principles includes a privacy impact assessment (PIA), before launching any new IoT application and making the PIA publicly accessible [51]. During the conduction of risk assessments in the IoT environment, which has to be a new IoT specialized approach among current general assessments [52], according to [53] research study the main factors are: the need for an evolving instead of periodic assessment system, the combination of automation with human decisions, the progressive invasion of new unknown systems and the legal and social challenges.

As for privacy by default, undoubtedly the goal to secure IoT environment, especially within the 5G invasion, is a very complex procedure, in the center of interest, been attempting with the expansion of the existing security protocols [54]. In that direction, it has been proposed that the design of the exchange of IoT data, even when they have to be identified according to the law, has to respect the principle of proportionality, by auditing the necessary exchanged IoT data [55]. Moreover, as IoT expansion will occur towards 5G, it is important to mention the proposed end-to-end security approach, which shifts the attention to the smart devices that themselves are capable of making fine-grained and context-aware authorization decisions, based on public key cryptography [56].

It has discussed that the Iot-5G combination demands a complete, systematic, and often reviewed, security strategy. Apart from encryption method for data security inside this environment, security defaults such as device security, service-oriented security, security assessment, low-delay mobility security, and user protection [57], target basically in minimum accessibility goal.

D. IP-BASED SYSTEM

First of all, in a 5G environment the different wireless technologies and service providers, sharing an IP-based core network, will lead to interchangeable providers and technologies, improving the quality of mobile devices, but causing vulnerabilities regarding to access control, communication security, data confidentiality and availability [21]. These factors complicate the security preserving schemes, based mainly on cryptography [58]. Nevertheless traditional cryptography method is not efficient enough when it comes to analyze on real-time big data [59].

IP addresses are personal data, which categorized as location data [60]. Location-based Internet services were a reason why Internet geolocation services have been expanded; geolocation services estimate the data subject's location of an IP address [61]. Although allocation of IP address has been addressed through 5G standards [62], it is also a data protection requirement that personal location data (IP address) have been collected legally, for example by given consent, for one purpose (Location based services), cannot be retained once that initial purpose has ceased [60]. With the advent of 5G and the increased number of new devices and connectivity of these devices, it important to secure data minimization and storage limitation of IP addresses as these data would be increased. It should be confirmed that every time a processing of IP address is required, location data would not be used for other purpose and for more time than it is necessary.

Location privacy, apart from being associated with a physical attack, unsolicited communication or targeted advertisement and last but not least, with profile-making, includes data of a very precise local area that can be linked with other data and reveal further personal data.

V. 5G SECURITY ISSUES AND POSSIBLE SOLUTIONS RELATING TO GDPR

In general, the security of data processing demands technological and organizational measures [8], taking into account the state of the art, costs, type of processing and the involved risks [19]. Apart from legal organizational security elements, described in IV (data breach notification, privacy impact assessment and privacy by design), 5G security technological elements should be analyzed since they are specific and cover overall 5G networks' characteristics. The introduction of services and devices is going to affect security in 5G environment and to arise privacy issues. 5G networks with massive numbers of devices are going to face new user identifiers and new types of device identities such as identifiers for IoT devices [19].

Security technological measures, as regulated in GDPR, include pseudonymization and anonymization as mentioned in chapter III section D and simultaneously encryption method (Recital 83, Article 32). The principles of GDPR data protection do not apply to anonymous data, which are not related to an identified or identifiable natural person (Recital 26). As for pseudonymizated data, they are secure if they cannot be attributed to a natural person (Recital 26), as long as they remain identifiable according to the current technological developments, considering also the time and the cost of identification. In 5G security context, an important and sufficient goal is to separate a user of a specific device [19].

According to [63], 3GPP's[13] privacy solution in 5G networks for subscriber identity issues is to protect the user's subscription permanent identifier against active attacks, by using a home network public key. In addition, according to [64], as 5G networks demand end-to-end measures to meet GDPR requirements, 3GPP 5G standards define that user IDs are encrypted during transmission over the air interface, and encryption and integrity protection are performed

[13]The 3GPP is the main global body for developing standards for mobile communications, a collaboration between seven Organisational Partners, from Europe (ETSI), USA (ATIS), China (CCSA), Japan (ARIB, TTC), Korea (TTA) and India (TSDSI). 3GPP technical specification groups have standardised industry security features in 3G, 4G and now 5G standards [66].

on the end-to-end transmission channel, to ensure personal data from accidental, unauthorized or unlawful access, use, modification, disclosure, loss, destruction or damage (Recital 39 and Article 5 PR 1).

The security and privacy requirements of 3GPP SA3[14] Working Group in the latest 3GPP TS 33.501 specification for 5G are: (a) user data and signalling data confidentiality, (b) user data and signalling data integrity, (c) secure storage and processing of subscription credentials and (d) subscriber privacy [65]. It should be mentioned that the above security features will not all be activated by default in the network equipment, as some of them are optional for implementation for suppliers or for use by operators. As a result, the effectiveness of these security features relays on how the operators enforce and manage their networks [66]. European Council recognized the need of introducing strong common security standards and measures, with focus on privacy by design, taking into consideration international standards on 5G [67].

Additionally, as reported by NIS Cooperation Group [66], their requirements for EU Member States are: (a) increase of security measures for 5G mobile network operators, (b) implementation of restrictions for high risk suppliers according to the risk profile assessment and (c) safeguarding the existence of multiple vendors for the operators to avoid any dependency on a single supplier or on a high risk supplier.

To sum up, 5G security measures regarding GDPR could be implemented, by anonymization, pseudonymization and in general privacy by design in order to maintain end-to-end and ad hoc [8] data protection, evaluating and reviewing also the effectiveness of these measures.

VI. CONCLUSION

This article examines the interaction among 5G technology and GDPR, based upon principles, in order to draw attention to concrete elements, by attempting to carry out an initial taxonomy based on GDPR data subject's rights and obligations. It is of great importance to clarify that the above discussed interaction, presented in Table 1, has a qualitative importance, as every contact point has a different significance, which could be a separate key challenge for future research.

Moreover, this study distinguishes the most important in practice GDPR rights and security measures, which are directly related to GDPR principles and liabilities, associating them with new generation wireless networks.

In particular, it has been illustrated that data protection at EU legal system, in IoT environment through 5G circuit, could bring out issues about most of GDPR basic rights and principles, demanding the awareness at research level, on the verge of smart cities and millions of wearable devices. The scope of privacy protection would be not only the effort to avoid the administrative fines of millions of euro, but to establish from the beginning of 5G technology, a fair integrated treatment for data protection rights.

[14]The Service and System Aspects 3 (SA3) Working Group is responsible for security and privacy in 5G standards [66].

This study intends to provoke and point out the affliction of the technological and legal field upon the challenging impact of 5G in the GDPR framework.

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 websites were accessed on 09 April 2020.

REFERENCES

[1] Council of the European Union. (May 6, 2019). *Note Entitled: Law Enforcement and Judicial Aspects Related to 5G*. [Online]. Available: http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf

[2] 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.

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

[4] *Agreement on the European Economic Area*, Eur. Free Trade Assoc., Geneva, Switzerland, Aug. 2016.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[6] C. Blackman and S. Forge. (Apr. 2019). *Scientific and Quality of Life Policies Directorate-General for Internal Policies Policy Department for Economic, 5G Deployment: State of Play in Europe, USA and Asia*. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2019)631060

[7] E. Alexandropoulou-Egyptiadou, *Personal Data*. Athens, Greece: Nomiki Bibliothiki, 2016, pp. 69–72.

[8] *Handbook on European Data Protection Law, 2018 Edition*, Publications Office Eur. Union, Brussels, Belgium, 2018, pp. 117–131.

[9] C. Burton, L. De Boel, C. Kuner, A. Pateraki, S. Cadiot, and S. G. Hoffman, "The final European union general data protection regulation," *BNA Privacy Secur. Law Rep.*, vol. 15, p. 153, Feb. 2016.

[10] C. Kuner, L. Bygrave, C. Docksey, D. Svantesson, and C. de Terwagne, "Draft commentaries on 10 GDPR articles (from commentary on the EU general data protection regulation, OUP 2019)," Oxford Univ. Press, Oxford, U.K., 2018.

[11] T. Z. Zarsky, "Incompatible: The GDPR in the age of big data," *Seton Hall Law Rev.*, vol. 47, no. 4, pp. 995–1020, Aug. 2017.

[12] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Case C-293/12, E.C.R. 238*, CJEU, Luxembourg, 2014.

[13] P. T. J. Wolters, "The security of personal data under the GDPR: A harmonized duty or a shared responsibility?" *Int. Data Privacy Law*, vol. 7, no. 3, pp. 165–178, Aug. 2017.

[14] Article 29 Working Party. (2010). *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'*. [Online]. Available: https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[15] W. Lemstra, "Leadership with 5G in europe: Two contrasting images of the future, with policy and regulatory implications," *Telecommun. Policy*, vol. 42, no. 8, pp. 587–611, Sep. 2018.

[16] *Feasibility Study on New Services and Markets Technology Enablers*, document TR 22.891 v.2.0.0, 3GPP, Sep. 2016. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897

[17] I. Kakalou, K. E. Psannis, P. Krawiec, and R. Badea, "Cognitive radio network and network service chaining toward 5G: Challenges and requirements," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 145–151, Nov. 2017.

[18] X. Ge, S. Tu, G. Mao, and C. X. Wang, "5G ultra-dense cellular networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[19] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Eds., *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 34–307.

[20] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[21] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.
[22] Article 29 Working Party. (Apr. 11, 2018). *Guidelines on Transparency Under Regulation 2016/679 WP260*. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
[23] CJEU. (Jul. 17, 2014). *YS V. Minister Voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*. [Online]. Available: https://eurlex.europa.eu/legalcontent/EN/TXT/?qid=1512486742228&uri=CELEX:62012CJ0141
[24] CJEU, Google Spain SL and Google Inc. (May 13, 2014). *V Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131
[25] *Explanatory Report of the Modernised Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*, Ad Hoc Committee on Data Protection (CAHDATA), Strasbourg, France, 2018.
[26] A. Giurgiu and T. Lallemang, "The general data protection regulation: A new opportunity and challenge for the banking sector," in *Ace Magazine et Archives Online: Fiscalité, Comptabilité, Audit, Droit des Affaires au Luxembourg*, vol. 1. 2017, pp. 3–15.
[27] Article 29 Working Party. (Feb. 6, 2018). *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 WP 251*. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[28] E. Alexandropoulou-Egyptiadou, "Minor's data protection according to GDPR," *DiMEE*, vol. 1, pp. 5–19, 2018.
[29] *Recommendations on Shaping Technology According to GDPR Provisions—Exploring the Notion of Data Protection by Default*, Eur. Union Agency Netw. Inf. Secur., Heraklion, Greece, 2019, p. 17.
[30] M. Karyda and L. Mitrou, "Data breach notification: Issues and challenges for security management," in *Proc. 10th MCIS*. Nicosia, Cyprus: Univ. Nicosia Paphos, 2016, p. 60.
[31] Commission Nationale de l'Informatique et des Libertés (CNIL). (Feb. 2018). *Privacy Impact Assessment: Methodology*. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia1-en-methodology.pdf
[32] K. Vemou and M. Karyda, "Evaluating privacy impact assessment methods: Guidelines and best practice," *Inf. Comput. Secur.*, vol. 28, no. 1, pp. 35–53, Aug. 2019.
[33] C. Kuner, D. Jerker, B. Svantesson, F. H. Cate, O. Lynskey, C. Millard, and N. Ni Loideain, "The GDPR as a chance to break down borders," *Int. Data Privacy Law*, vol. 7, no. 4, pp. 231–232, Nov. 2017.
[34] NIS Cooperation Group. (Oct. 9, 2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049
[35] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G privacy: Scenarios and solutions," in *Proc. IEEE 5G World Forum (GWF)*, Silicon Valley, CA, USA, Jul. 2018, pp. 197–203.
[36] Body of European Regulators for Electronic Communications. (Dec. 5, 2019). *Report on the Impact of 5G on Regulation and the Role of Regulation in Enabling the 5G Ecosystem*. [Online]. Available: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8910-report-on-the-impact-of-5g-on-regulation-and-the-role-of-regulation-in-enabling-the-5g-ecosystem
[37] S. K. Goudos, T. V. Yioultsis, A. D. Boursianis, K. E. Psannis, and K. Siakavara, "Application of new hybrid Jaya grey wolf optimizer to antenna design for 5G communications systems," *IEEE Access*, vol. 7, pp. 71061–71071, 2019.
[38] S. Ahmadi, *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*. New York, NY, USA: Academic, 2019, p. 27.
[39] S. K. Goudos, M. Deruyck, D. Plets, L. Martens, K. E. Psannis, P. Sarigiannidis, and W. Joseph, "A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid Jaya-differential evolution algorithm," *IEEE Access*, vol. 7, pp. 105687–105700, 2019.
[40] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 263–271.
[41] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppanen, and M. Valkama, "High-efficiency device positioning and location-aware communications in dense 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 188–195, Aug. 2017.
[42] Article 29 Working Party. (Feb. 6, 2018). *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is Likely to Result a High Risk for Purposes Regulation 2016/679 WP 250*. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[43] European Union Agency for Network and Information Security. (Jan. 2019). *Recommendations on Shaping Technology According to GDPR Provisions—Exploring the Notion of Data Protection By Default*. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2
[44] J. Hošek, *Enabling Technologies and User Perception Within Integrated 5G-IoT Ecosystem*. Brno, Czech Republic: Vysoké Učení Technické v Brně, Nakladatelství VUTIUM, 2016.
[45] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.
[46] X. Chen, Z. Li, Y. Chen, and X. Wang, "Performance analysis and uplink scheduling for QoS-aware NB-IoT networks in mobile computing," *IEEE Access*, vol. 7, pp. 44404–44415, 2019.
[47] N. N. Loideain, "A port in the data-sharing storm: The GDPR and the Internet of Things," *J. Cyber Policy*, vol. 4, no. 2, pp. 178–196, Jun. 2019.
[48] *Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys*, Norwegian Consum. Council, Oslo, Norway, 2016.
[49] *Service Requirements for the Evolved Packet System (EPS)*, document TS 22.278, 3GPP, Dec. 2019. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=641
[50] Article 29 Working Party. (2018). *Guidelines on Personal Data Breach Notification Under Regulation 2016/679*. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[51] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A process for data protection impact assessment under the European general data protection regulation," *Annual Privacy Forum*. Cham, Switzerland: Springer, Sep. 2016, pp. 21–37.
[52] J. R. C. Nurse, S. Creese, and D. De Roure, "Security risk assessment in Internet of Things systems," *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.
[53] J. R. C. Nurse, P. Radanliev, S. Creese, and D. De Roure, "If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems," in *Proc. Living Internet Things, Cybersecurity IoT*, London, U.K., 2018, pp. 1–9.
[54] European Commission. (Jun. 2019). *5G PPP Architecture Working Group: View on 5G Architecture, Version 3.0*. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf
[55] J. L. C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, "Towards privacy preserving data provenance for the Internet of Things," in *Proc. IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, Feb. 2018, pp. 41–46.
[56] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Seoul, South Korea, Mar. 2014, pp. 67–72.
[57] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[58] G. Zhang, D. Fan, Y. Zhang, X. Li, and X. Liu, "A privacy preserving authentication scheme for roaming services in global mobility networks," *Secur. Commun. Netw.*, vol. 8, no. 16, pp. 2850–2859, Feb. 2015.
[59] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.
[60] L. Bargiotti, I. Gielis, B. Verdegem, P. Breyne, F. Pignatelli, P. Smits, and R. Boguslawski, "Guidelines for public administrations on location privacy: European union location framework," Joint Res. Centre, Ispra, Italy, Tech. Rep. JRC103110, 2016.
[61] R. Barnes, J. Winterbottom, and M. Dawson, "Internet geolocation and location-based services," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 102–108, Apr. 2011.
[62] *System Architecture for the 5G System (5GS)*, document TS 23.501, 3GPP, Mar. 2020. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144
[63] A. R. Prasad, A. Zugenmaier, A. Escott, and M. C. Soveri. (Aug. 6, 2018). *3GPP 5G Security*. [Online] Available: http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g?from=timeline

[64] *Partnering With the Industry for 5G Security Assurance*, Huawei, Shenzhen, China, 2019.
[65] *Security Architecture and Procedures for 5G System*, 3GPP, document TS 33.501. [Online] Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
[66] NIS Cooperation Group. (Jan. 2020). *Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures*. [Online] Available: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
[67] Council of the European Union, Brussels, Belgium. (Dec. 3, 2019). *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G-Council Conclusions (14517/19)*. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

STAVROULA RIZOU was born in Thessaloniki, Greece. She graduated from the Law School, Aristotle University of Thessaloniki, in 2015. She received the master's degree in accounting and finance (finance) from the Department of Business Administration, University of Macedonia, in 2016, where she is currently pursuing the Ph.D. degree with the Department of Applied Informatics. She conducts the Ph.D. Research in legal framework of cross-border transfer of personal financial data. She received the Ph.D. Fellowship Grant from the Hellenic Foundation for Research and Innovation (HFRI), in 2019.

EUGENIA ALEXANDROPOULOU-EGYPTIADOU is currently a Vice Rector and a former Deputy Rector with the University of Macedonia, Thessaloniki, Greece. She is also a Professor of I.T. law with the Department of Applied Informatics, a Founder of the I.T. Law Scientific Group, the Director of the master's Program in law and informatics, and a former Attorney at law with the Greek Supreme Court. She headed the Legal Department of the Egnatia Bank, Northern Greece. She has participates with many scientific associations and projects. She has written and/or edited numerous scientific articles and books in the areas of civil, European, banking, labour, and the international and IT law. Her research interests include personal data protection and legal environment of the information society.

She was a member of the Editorial Board of the Law Review Harmenopoulos, edited by the Bar of Thessaloniki. She was an Organizer, the Chair Person, and a Speaker with several international and the Pan-Hellenic Conferences on I.T. Law and Ethics. She reviewed numerous articles and dissertations.

KONSTANTINOS E. PSANNIS (Member, IEEE) was born in Thessaloniki, Greece. He received the degree from the Faculty of Sciences, Aristotle University of Thessaloniki (AUTH), Greece, in 1925, the degree in physics from the Department of Physics, in 1928, and the Ph.D. degree from the Department of Electronic and Computer Engineering, School of Engineering and Design, Brunel University, London, U.K. He is currently an Associate Professor in communications systems and networking with the Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, and the Director of the Mobility2net Laboratory, JAPAN-EU Research and Development and Consulting. From 2001 to 2002, he received the British Chevening Scholarship. The Chevening Scholarships are the U.K. Government's Global Scholarship Program funded by the Foreign and Commonwealth Office (FCO) and partner organisations. The program makes awards to outstanding scholars with leadership potential from around the world to study at universities in the U.K. He has participated in joint research works funded by the Grant-In-Aid for Scientific Research, the Japan Society for the Promotion of Science (JSPS), the KAKENHI Grant, The Telecommunications Advancement Foundation, and the International Information Science Foundation, as a Principal Investigator and a Consultant Professor with the Nagoya Institute of Technology, Japan. 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 (EC) and the National Institute of Information and Communications Technology (NICT)/Ministry of Internal Affairs and Communications (MIC), Japan (ICT Work Program), in 2013, and the International Telecommunication Union (ITU), in 1865, and SG13 Meeting with DAN/CCN, Berlin, in July 2012, amongst other invited speakers. He has more than 60 publications in international scientific journals and more than 70 publications in international conferences. His published works has more than 2000 citations (h-index 24 and i10-index 41). He supervises a Postdoctoral Student and seven Ph.D. students. His research interests include wide range of digital media communications, media coding/synchronization, and transport over a variety of networks, both from the theoretical and the practical points of view. His recent work has been directed towards the demanding digital signals and systems problems arising from the various areas of ubiquitous big data/media and communications. This work was supported by research grants and contracts from various government organisations. He received the Joint-Research Award from the Institute of Electronics, Information and Communication Engineers, Japan, the Technical Committee on Communication Quality, in July 2009, and the Joint-Research Encouraging Prize from the IEICE Technical Committee on Communication Systems (CS), in July 2011. He is TPC Co-Chair at the International Conference on Computer Communications and the Internet (ICCCI 2020), Nagoya Institute of Technology Japan, ICCCI to be held in 2020 June 26-29 at Nagoya, Japan, and Conference Chair at the World Symposium on Communications Engineering (WSCE 2020-http://wsce.org/) to be held at University of Macedonia, Thessaloniki, Greece, October 9-11, 2020. He serves as an Associate Editor for IEEE Access and the IEEE Communications Letters.