

Project Acronym and Title:

5GhOSTS - 5TH GENERATION SECURITY FOR TELECOM SERVICES

Deliverable:

D1.4: PRIVACY REQUIREMENTS FOR 5G TELECOM SYSTEMS RUNNING VIRTUALIZED MULTI-COMPONENT SERVICES

Lead Author and Affiliation:
Mykyta Petik (KU Leuven)

mykyta.petik@kuleuven.be

 Copyright © 5GhOSTS Consortium 2019-2023

D1.4

Project funded by the European Commission within the Horizon 2020 Programme Dissemination Level		
PU	Public	**X**
CO	Confidential, only for members of the consortium (incl. the Commission Services)	
CL	Classified, as referred to in Commission decision 2001/844/EC	

Deliverable number:	1.4
Deliverable name:	Privacy requirements for 5G Telecom Systems running virtualized multi-component services
Work package:	**1**
Lead WP / Deliverable beneficiary:	EAB / KU LEUVEN

	Status of deliverable **By**	**Date**
Submitted (Author(s))	Mykyta Petik (KU Leuven)	2021-05-01
Verified (WP leader)	Hans Eriksson (EAB)	2021-05-09
Approved (PMB member)	Christoph Baumann (EAB) Jan Tobias Muehlberg (KU Leuven)	2021-05-13
Approved (Coordinator)	Jan Tobias Muehlberg (KU Leuven)	2021-05-13

Author(s)		
Name	**Organisation**	**E-mail**
Mykyta Petik	KU LEUVEN	mykyta.petik@kuleuven.be
Olia Kanevskaia	KU LEUVEN	olia.kanevskaia@kuleuven.be
Peggy Valcke	KU LEUVEN	peggy.valcke@kuleuven.be
Christian Schaefer	EAB	christian.schaefer@ericsson.com
Christoph Baumann	EAB	christoph.baumann@ericsson.com
Eddy Truyen	KU LEUVEN	Eddy.Truyen@cs.kuleuven.be
Jan Tobias Muehlberg	KU LEUVEN	jantobias.muehlberg@cs.kuleuven.be

 Copyright © 5GhOSTS Consortium 2019-2023

Public introduction
A study of the privacy requirements for 5G Telecom Systems running virtualized multi-component services, including a state of the art overview of the relevant legal requirements under the sector-neutral GDPR (which entered into force on 25 May 2018) and the (upcoming) sector-specific e-Privacy Regulation (which is a "lex specialis", intended to particularise and complement the rules of the GDPR for the electronic communications sector), and offering a comprehensive analysis of the impact of implementing regulation-compliant privacy in an NVF execution environment.

Executive Report Summary
This deliverable provides an analysis of potential legal challenges to privacy, data protection, and security in the 5G value chain running virtualized multi-component services based on the use cases listed above and develops privacy requirements for such services. The deliverable describes and analyzes technological novelties relevant to the challenges to privacy, security, and data protection with a focus on 5G core network such as Software-defined networking (SDN), Network Function Virtualization (NFV), and Network Slicing (NS). Major disrupting technological novelties in 5G are assessed and linked to the applicable legal framework. This deliverable provides a legal qualification of roles and responsibilities of stakeholders in the 5G value chain and the influence of novel technologies on compliance with EU law. Also, it examines the scope of applicable laws at the EU level, namely that of the ePrivacy Directive, European Electronic Communications Code, and GDPR, as well as the potential impact of the draft ePrivacy Regulation (if adopted). The principles relating to processing personal data listed in GDPR are linked to specific challenges in 5G networks. The deliverable explains the main legal concepts stemming from the EU privacy and data protection framework. This includes the potential risks to user's rights to security, privacy, and data protection in 5G networks based on the use cases analyzed in deliverable D1.3 'The trust model for multi-tenant 5G telecom systems running virtualized multi-component services'. Further, this deliverable analyzes and suggests possible techniques, strategies, and best practices to mitigate the legal risks regarding privacy and data protection in 5G. Potential legal challenges arise from the implementation of SDN and network function virtualization (NFV), introducing new stakeholders in 5G networks, usage of cloud-based solutions, the status of electronic communication service providers, and the problem of identifying processors and controllers of personal data.

 Copyright © 5GhOSTS Consortium 2019-2023

Table of Contents

1. Introduction 6
2. 5G networks and virtualized multi-component services 8
2.1. Technological novelties in 5G networks 8
2.2. Main 5G disrupting innovations and their impact on privacy, data protection, and security 11
3. EU legal and policy framework applicable to 5G 14
3.1. Privacy as a human and fundamental right 15
3.2. Initial European efforts in harmonization of privacy legislation 17
3.3. GDPR 18
3.4. ePrivacy Directive 32
3.5. Open Internet Regulation 34
3.6. European Electronic Communications Code 35
4. Privacy, security, and data protection risks in virtualized 5G networks 37
5. Implementing privacy, security and data protection risk mitigating measures in 5G networks 44
6. Conclusion 50

 Copyright © 5GhOSTS Consortium 2019-2023

Glossary of abbreviations used

Abbreviation	Description
5G	The 5th generation of mobile network
29WP	Article 29 Working Party
AR	Augmented Reality
BEREC	Body of European Regulators for Electronic Communications
CJEU	Court of Justice of the European Union
CSP	Cloud Service Provider
DPA	Data protection authority
DPD	Data Protection Directive
DPIA	Data protection impact assessment
ECN	Electronic communication network
ECS	Electronic communications service
EDPB	European Data Protection Board
EECC	European Electronic Communications Code
GDPR	General Data Protection Regulation
ICS	Interpersonal communications service
IMSI	International Mobile Subscriber Identity
IoE	Internet of Everything
IoT	Internet of Things
M2M	Machine-to-Machine
MIMO	Massive-input-massive-output
NF	Network function
NFV	Network function virtualization
NRA	National regulatory authority
NS	Network Slicing
RAN	Radio access network
RS	Remote surgery
SDN	Software-defined networking
SO	Smart office
V2I	Vehicle-to-Infrastructure
VM	Virtual Machine
VNF	Virtualized network function
VR	Virtual Reality

 Copyright © 5GhOSTS Consortium 2019-2023

1. Introduction

The telecommunications industry has gradually migrated from legacy telephony networks to telephony networks based on an Internet Protocol (IP) network to deliver communication services.[1] The 5th generation of mobile networks (5G) takes advantage of virtualized networks, software-defined networking (SDN), and cloud-based solutions to provide lower latency and faster processing of data to users. The use of the Internet Protocols (IP) as the primary means of transportation of all services was introduced already in the predecessors of 5G, namely the 3rd and 4th generation of cellular networks (3G and 4G, respectively). 5G uses IP on a larger scale than its predecessors. Virtualization, edge computing, SDN, and cloud-based solutions bring new actors into the EU mobile networks, change the way networks are secured, affect how privacy is protected and personal data is processed. Previous generations of mobile networks did not use cloud native solutions, such as micro service virtualization, SDN, and edge computing which is why technical and legal research is needed to study the implications of such technical novelties in 5G networks for users' security, privacy and data protection. It is forecasted that by 2025, 5G will occupy 20% of the market share of mobile telecommunication technologies worldwide.[2] The majority of Europeans use smartphones and share their sensitive personal data via mobile networks. The constant presence of smart devices in daily lives reinforces the notion of humans being 'always connected' due to the large-scale utilization of modern technologies and inherent challenges to privacy it entails.[3]

Currently, 5G is in the state of roll-out, and large-scale commercialization of this technology is expected in the 2020s.[4] Only a few companies in the world are considered to be technologically capable of delivering end-to-end solutions necessary to deploy 5G mobile networks and contribute to the relevant international technical standards. These companies are Ericsson (Sweden), Huawei, ZTE (both are from China), Nokia (Finland), and Samsung (South Korea).[5] Other companies have been mentioned as being essential suppliers of equipment and software for 5G mobile networks while not providing end-to-end solutions. These include large chipset manufacturers Qualcomm and Intel, manufacturer of network hardware Cisco Systems, computer data storage company Dell EMC, wireless networking company Aruba (all from the US), and computer equipment manufacturer Lenovo (China).[6] As we can see, since two of only five companies

[1] Zhang, Y. (2017). Network Function Virtualization: Concepts and Applicability in 5G Networks (Wiley - IEEE) (1st ed.). Wiley-IEEE Press, 1.

[2] O'Dea, S. (2020b). Mobile technology share by generation 2016-2025. Statista. https://www.statista.com/statistics/740442/worldwide-share-of-mobile-telecommunication-technology/

[3] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF), p. 1. https://doi.org/10.1109/5gwf.2018.8516981.

[4] Kania, E. (2019). (Rep.). Center for a New American Security. doi:10.2307/resrep20451 p. 6

[5] See also for instance in this regard, study on 5G patents: https://www.iplytics.com/report/5g-patent-study-2020/; https://www.iplytics.com/report/who-is-leading-the-5g-patent-race/ (if you are to use it explain in the text or footnotes that those are essential technology owners, so difference between companies having patents and making infrastructure); see also these guys: https://www.stiftung-nv.de/en/node/2717 https://www.stiftung-nv.de/en/node/2511 on 5G enablers and players.

[6] See for example: Kania, E. (2019). (Rep.). Center for a New American Security. doi:10.2307/resrep20451 p. 2; Moor Insights and Strategy. (2019, October 18). Who Is "Really" Leading in Mobile 5G, Part 4: Infrastructure Equipment Providers. Forbes. https://www.forbes.com/sites/moorinsights/2019/07/19/who-is-really-leading-in-mobile-5g-part-4-infrastructure-equipment-providers/#3843b3939130; Moorhead, P. (2020, March 3). Intel Aggressively Updates Xeon And Announces Key 5G Product Lines. Forbes.

 Copyright © 5GhOSTS Consortium 2019-2023

capable of deploying 5G networks are located in the EU Member States, the EU has a chance of becoming a world leader in the development of 5G technology.

Structure of the document

This deliverable will provide an analysis of potential legal challenges to privacy, data protection, and security in the 5G value chain running virtualized multi-component services based on the use cases listed the 'Methodology and use cases' section and develop privacy requirements for such services.

Section 2.1. of this deliverable describes and analyzes technological novelties relevant to the challenges to privacy, security, and data protection in the 5G core network. Major privacy-disrupting technological novelties in 5G are assessed in Section 2.2. Section 3 analyses and outlines the applicable legal framework, provides a legal qualification of roles and responsibilities of stakeholders, and the influence of novel technologies on compliance with EU law. Also, it examines the scope of applicable laws at the EU level, namely that of the ePrivacy Directive[7], European Electronic Communications Code, and GDPR, as well as the potential impact of the draft ePrivacy Regulation[8] (if adopted).[9]

Section 4 identifies and explains the potential risks to user's rights to security, privacy, and data protection in 5G networks based on the use cases.

Section 5 analyzes and suggests possible techniques, strategies, and best practices to mitigate the legal risks regarding privacy and data protection in 5G. Potential legal challenges arise from the implementation of SDN and network function virtualization (NFV), introducing new stakeholders in 5G networks, usage of cloud-based solutions, the status of electronic communication service providers, and the problem of identifying processors and controllers of personal data based on GDPR requirements.

Section 6 sums up the findings of the deliverable.

Purpose of the document

https://www.forbes.com/sites/moorinsights/2020/03/03/intel-aggressively-updates-xeon-and-announces-key-5g-product-lines/#63f737fc4062.

[7] Directive is a binding legislative act of the European Union (EU) which sets legal goals the EU Member States are obliged to comply with. Each Member State decides the way to transpose the EU Directive into the national legislation.

[8] Regulation is a binding legislative act of the EU with direct legal effect meaning that there is no need for Member States to adopt additional laws to transpose it.

[9] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance. OJ L 321, 17.12.2018, p. 36–214; 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, OJ L 119, 4.5.2016, p. 1–88 ('General Data Protection Regulation'); Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD)

 Copyright © 5GhOSTS Consortium 2019-2023

It comes as no surprise that the emergence of novel technologies and large-scale use of the Internet is associated with the challenges to the right to privacy and balance of interests: in fact, the right to privacy has occupied academics' minds for more than a century.[10] Given the recent changes in data protection regulation and the evolving case law of the Court of Justice of the European Union in this regard (Case C-131/12 ("Google Spain") and Case C-311/18 ("Schrems II")), the issues of privacy and data protection have become a prime factor in the modern digital economy. Recent technological advances such as the massive use of mobile and computer networks for the transfer of data, cloud services for storing and processing data, and social networks provided more grounds for large-scale invasion of privacy and the need to impose stricter rules on handling personal data. Implementation of 5G networks will have a dramatic impact on the economy and society and the legal safeguards and protection of privacy and personal data.

The presence of various stakeholders in 5G requires legal analysis to determine their roles and responsibilities concerning privacy, data protection, and security. This deliverable will provide state of the art, explain the challenges posed by 5G and associated technologies to privacy, security, and data protection, and outline the applicable EU legal framework.

Methodology and use cases

This deliverable uses an interdisciplinary literature review of legal and technical publications and descriptive research to outline the relevant legal framework, clarify technical concepts such as SDN, NFV, network slicing, and their impact on the law.

This deliverable relies on the use cases described in deliverable D1.2, "Use cases and initial conceptualization of the 4 ESRs's research projects, inter-project relations, and interdisciplinary common approach". These use cases are:

- Vehicle to Infrastructure (V2I)
- Smart Office (SO), including augmented and virtual reality (AR/VR) applications
- Remote Surgery (RS)

2. 5G networks and virtualized multi-component services

2.1. Technological novelties in 5G networks

A higher reliance on Internet-based services and a drastic increase in cellular data volume growth causes network operators and service providers to change existing approaches to establishing and maintaining core networks by paying more attention to security and efficiency. Modern telecommunication service providers have to manage many challenges related to growth in mobile data exchange and in a number of devices such as increasing operational costs, the necessity to accommodate the coexistence of different

[10] One of the earliest definitions to the right to privacy was given in Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220. doi:10.2307/1321160.

 Copyright © 5GhOSTS Consortium 2019-2023

generations of cellular networks such as 3G, 4G, and 5G, the need to upgrade equipment and the need to expand network capacity to accommodate an unprecedented number of Internet-connected devices. The amount of data in existing mobile networks will grow because of rising numbers of personal smart mobile devices and industrial Internet of Things (IoT) devices, with research claiming that Machine-to-Machine (M2M) communications will generate more significant amounts of data than all data generated by humans combined.[11] The expansion of physical infrastructure alone is not enough to keep up with mobile technologies and their usage.[12]

To optimize the high capital expenditure and to operate expenditure when upgrading equipment and deploying 5G networks, telecommunication providers and other stakeholders have been implementing two relatively new and fundamental technologies: Network Function Virtualization (NFV) and Software-Defined Networking (SDN).[13] Virtualization itself is not a very new concept: Virtual Machines (VM) are used to manage large amounts of simultaneous operations and deal with security and privacy risks. A technology similar to VMs, called 'container,' has become extremely popular since 2013. Containers virtualize only the functions necessary to run a separate application rather than a whole computer.[14] This means that they are faster to start up and use less memory than VMs, and one physical machine can host a larger number of containers for different applications, which use the same operating system of the physical machine but are isolated from each other. The coordination and control of containers are performed by a high-level software called 'container orchestrator,' and the process is known as 'container orchestration.' Virtualization in 5G networks has been described as "*crucial and inevitable*" since the broad application of virtualization is the main requirement for ensuring the envisaged connectivity and adaptation to technological developments.[15]

5G networks rely partially on previous generations of mobile networks' technologies and infrastructure, namely 4G and 3G. To benefit from the potential of 5G technology, telecommunication providers and other actors such as SDN and cloud-service providers have to change the architecture, operations, and services. It is possible to say that considering all the technological novelties, 5G is not just succeeding 4G as the next generation of mobile networks but paves the way for an entirely new type of mobile network.[16]

Being an evolution of previous mobile network technology, 5G technology offers substantially higher data transfer rates, significantly shorter network latency, and greater bandwidth, allowing faster download and upload speeds and a broad spectrum of use cases. 5G will become a major enabler for the Internet of Things (IoT) and the Internet of Everything (IoE), which paves the way for remote surgery, telemedicine, autonomous cars, smart homes, and smart highways. 5G will impact privacy, security, and data protection

[11] Zhang, Y., 2018. Network Function Virtualization. Hoboken, NJ: Wileys, IEEE Press, pp.1-4.
[12] *Ibid*, pp.1-4.
[13] Condoluci, M., & Mahmoodi, T. (2018). Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges. Computer Networks, 146, 2–4. https://doi.org/10.1016/j.comnet.2018.09.005
[14] Buchanan, S., Rangama, J., & Bellavance, N. (2019). Introducing Azure Kubernetes Service: A Practical Guide to Container Orchestration (1st ed.). Apress, pp. 4-5.
[15] Ivezic, M. (2020, August 16). Unlocking the Future – Why Virtualization Is the Key to 5G. 5G Security - 5G, MIoT, CPSSEC, Security Blog by Marin Ivezic. https://5g.security/5g/virtualization-key-5g/;
[16] Quote: "*Because 5G is not the same as the Gs that came before. Implementing this technology does not simply require an upgrade of the current network, it demands a new type of network altogether*." per Ivezic, M. (2020, August 16). Unlocking the Future – Why Virtualization Is the Key to 5G. 5G Security - 5G, MIoT, CPSSEC, Security Blog by Marin Ivezic. https://5g.security/5g/virtualization-key-5g/;

 Copyright © 5GhOSTS Consortium 2019-2023

practices everywhere since this technology will allow us to connect everything to the Internet that can be connected. Users generate massive amounts of personal data through IoT sensors and devices such as smartphones, autonomous vehicles, and smart home appliances, among others. In terms of privacy and data protection, it means that this personal data will be uploaded to internet-based cloud storages for processing, where it is vulnerable to a wide range of possible attackers. While privacy concerns in traditional telephone networks were initially related primarily to eavesdropping, their scope changes with technological advancement. High speed of data processing in virtualized 5G networks may lead to practical problems in obtaining data subject's consent, providing information on processing, informing authorities, and affected data subjects on data breaches as well as concerns regarding interoperability and the execution of the right to erasure and rectification of personal data.[17] 5G will contribute to generating unprecedently huge amounts of personal data, which may require stricter standards of handling and processing, and will be transferred and processed continuously.

SDN allows splitting (decoupling) the router control and forwarding (data) planes in networking. This means that SDN-based networks have physically separated control and data planes, allowing a control plane to control several different devices independently of data flowing through the network. SND-based networks are more centralized and directly programmable, which makes their maintenance and scalability easier. Network design employed by SDN offers possibilities in cost reduction, security improvement, and increased reliability. NFV is a closely related technology to SDN, which serves as a platform for virtualization. NFV allows us to fully virtualize entire network functions, allowing them to create virtual networks on top of standard hardware networks, bringing the whole network infrastructure closer to cloud infrastructure. NFV is a term for a concept of virtualizing network functions, while VNF (Virtualized network function) refers to an implemented virtualization of a network function. Cloud infrastructure and Cloud Service Providers (CSP) will become essential players in the mobile market since mobile data will be transferred into the cloud for analysis, computing, and storage purposes. Telecom operators will have to deploy numerous data centers or rely on existing CSPs and their capabilities to ensure continued increase in data consumption. NFV and SDN technologies are considered to be 'key enablers' for 5G networks.[18]

A study on the implications of the emerging technologies Software-Defined Networking and Network Functions Virtualisation on the future Telecommunications Landscape published by the European Commission stated that "*SDN and NFV will play an important role in the future telecommunications landscape*" and "SDN and NFV are likely to be instrumental in the development and roll-out of innovative services, applications, and products as well as in facilitating major trends with substantial economic and societal impact."[19] The same study states, that NFV and SDN technologies shall serve as an "*enabling toolkit*" for various products and services such as connected cars (V2I), AR and VR applications (SO), and universal communication, and exact implications are difficult to estimate or forecast for now.[20]

[17] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, 8, 108056. https://doi.org/10.1109/access.2020.3000662.

[18] Yousaf, F. Z., Bredel, M., Schaller, S., & Schneider, F. (2017). NFV and SDN—Key Technology Enablers for 5G Networks. IEEE Journal on Selected Areas in Communications, 35(11), 1. https://doi.org/10.1109/jsac.2017.2760418.

[19] European Commission. (2017). Implications of the emerging technologies Software-Defined Networking and Network Function Virtualisation on the future Telecommunications Landscape. https://ec.europa.eu/digital-single-market/en/news/implications-emerging-technologies-software-defined-networking-and-network-function, p. 4.

[20] Ibid, p. 55.

 Copyright © 5GhOSTS Consortium 2019-2023

2.2. Main 5G disrupting innovations and their impact on privacy, data protection, and security

The implementation of virtualization, SDN, NFV, and wider reliance on IP and cloud technologies as the primary means of data transportation creates a plethora of privacy challenges in 5G networks. 3GPP, an international standardization body, defines the 5G system architecture as the one consisting of a core network and a radio access network (RAN).[21] RAN enables radio communication between the network and user's devices, such as mobile phones.[22] The core network handles the transportation of the data and contains network functions (NF).[23] Important virtualization-related novelties lie in the core network, including the application of network slicing technology which contributes to network optimization.[24] This deliverable concentrates on the core network since the majority of disrupting technologies are contained there. 5G may become the encompassing channel of communication for nearly all data and create a situation where almost all individuals will be using 5G network through one of their devices.[25]

Researchers suggest the following classification of privacy categories in 5G networks (See Figure 1):[26]

- **Data privacy –** incorporates all data generated and transferred by the consumers through 5G mobile networks. Special attention is paid to the protection of sensitive personal data, such as health or biometric data;

- **Location privacy –** the above-mentioned omnipresence of 5G-enabled sensors and devices allows the precise geolocation and tracking of users. Such tracking can be performed by various actors in 5G networks, such as third-party application developers, cloud and edge computing service providers, and telecommunication providers themselves, among others;

- **Identity privacy –** since 5G networks involve an enormous number of interconnected devices and their users, it is essential to ensure the protection of subscribers' identities. Subscriber's identity includes the usage of International Mobile Subscriber Identity (IMSI – used for identification and location of subscribers) by user's device and the risk of exposing the IMSI to potential attackers.[27]

[21] 5G PPP. (2020). 5G PPP Architecture Working Group View on 5G Architecture, https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf
[22] Cox, C. (2020). An Introduction to 5G: The New Radio, 5G Network and Beyond (1st ed.). Wiley, 1.
[23] Ibid.
[24] Penttinen, J. T. J. (2019). 5G Explained. Wiley, xvii. https://doi.org/10.1002/9781119275695
[25] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 9. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[26] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF), 2. https://doi.org/10.1109/5gwf.2018.8516981.
[27] Specific threats are related to the exposure of a clear text IMSI during Paging (sending a probing message by the networks to the inactive device) and the usage of the same IMSI in incoming and outcoming messages during Paging.

 Copyright © 5GhOSTS Consortium 2019-2023

Identity also includes the profile data used in various third-party apps, most importantly healthcare, fitness, banking and shopping apps, which gather and store large amounts of sensitive data.[28]

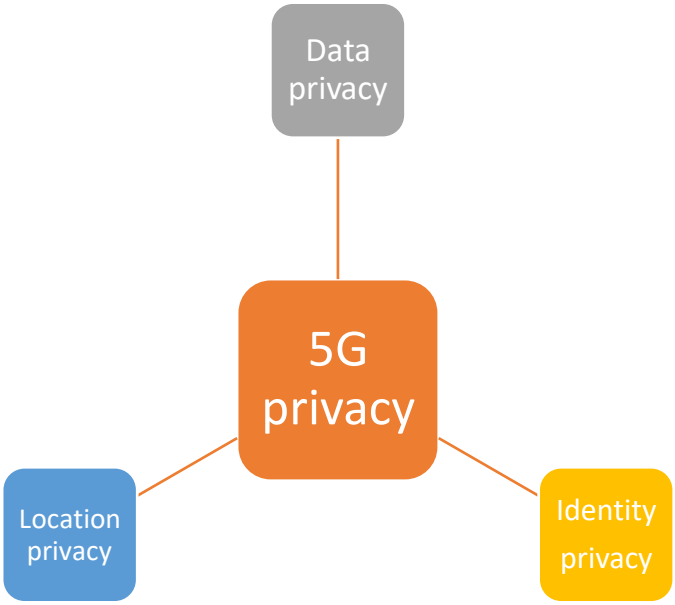

FIGURE 1. Visualization of different privacy categories in 5G networks

Virtualization, network slicing, edge computing, and geolocation were named as technologies potentially making the most substantial impact on privacy and security in 5G networks.[29] These technologies are analyzed below.

Attackers may use IMSI catchers – special devices used to steal subscribers' identifiers. See: Jimenez, E. C., Nakarmi, P. K., Naslund, M., & Norrman, K. (2017). Subscription identifier privacy in 5G systems. 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), 1–5. https://doi.org/10.1109/mownet.2017.8045947; Nakarmi, P. K., Ohlsson, O., & Hedman, P. (2019). Fighting IMSI catchers: A look at 5G cellular paging security. Ericsson. https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy;
Norrman, K., & Nakarmi, P. K. (2017). Protecting 5G against IMSI catchers. Ericsson. https://www.ericsson.com/en/blog/2017/6/protecting-5g-against-imsi-catchers.

[28] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF), p. 3. https://doi.org/10.1109/5gwf.2018.8516981.

[29] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 5. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf; ENISA. (2020). 5G Supplement to the Guideline on Security Measures under the EECC, 13.

 Copyright © 5GhOSTS Consortium 2019-2023

Virtualization and network slicing

Virtualization and the related technologies such as SDN and NFV as described above, are the chief drivers of privacy disruption in 5G core network.[30] SDN allows a huge degree of flexibility in the network enabling the possibility of dynamic and automated adaptation to workload demands. Such dynamic and automatic changes essentially mean that the whole architecture including the security and privacy preserving components may be affected.

Network slicing is a technology which allows establishing a separate independent network within larger 5G network aimed at a specific use case.[31] Each network slice has its own network functions, which are programmable and serve as virtual equivalents to hardware. Network slice can be dynamically modified or even deleted through management functions. User's devices may interact with multiple network slices simultaneously, transferring data through each one. Network slices may be offered through Network slicing as a service (NSaaS) business model with third parties providing such services to telecommunication providers. Potential privacy problems related to network slicing technology include the vulnerability of the communication between inter-network slices, non-homogeneous privacy policies and protocols for various slices, potential affect of other slices because of resource exhaustion.[32] The legal assessment of such risks and the potential remedies are listed in sections 4 and 5 of this deliverable.

Edge computing

5G uses edge computing technology to provide ultra-low latency and cope with the need to compute enormous amounts of data. The key idea of edge computing is to process the data in close proximity to ('at the edge of') the network through edge computing facilities and data processing centers. Edge computing is especially crucial for the next use cases:

- Vehicle to infrastructure communication (autonomous self-driving vehicles);
- Industrial automatization (Smart plants and smart factories);
- Smart offices;
- Augmented reality and VR gaming;

https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/at_download/fullReport.

[30] According to AEPD (Agencia Española de Protección de Datos, the Data Protection Agency of Spain) virtualization in 5G networks "*is doubtlessly the greatest revolution of all, and what may have an important impact on privacy is the use of virtualization technologies*", see Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 4. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.

[31] Lei, W., Soong, A. C. K., Jianghua, L., Yong, W., Classon, B., Xiao, W., Mazzarese, D., Yang, Z., & Saboorian, T. (2019). 5G System Design: An End to End Perspective (1st ed. 2020 ed.), 278. Springer.

[32] Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Communications Surveys & Tutorials, 22(1), 13. https://doi.org/10.1109/comst.2019.2933899.

 Copyright © 5GhOSTS Consortium 2019-2023

- Remote surgery.

Distributed architecture of edge computing systems, presence of multiple trust domains, and massive amounts of processed data require new privacy-preserving techniques and mechanisms.[33] Data security and privacy challenges in edge computing include the following[34]:

- New requirements for data encryption methods and the challenge of multiple authorized parties;
- Distributed access control;
- Limited resources of edge devices;
- Efficiency.

Geolocation

Another disruptive technology used in 5G networks is geolocation. Although geolocation is not a new technology and is widely used in smartphones, 5G network architecture envisages larger number of connected devices and higher network density. These factors contribute to the localisation of the user with much higher precision than in previous generations of mobile networks. The introduction of massive multiple-input-multiple-output (MIMO) technology enables the precise 3D positioning of users' devices.[35]

Precise geolocation, especially the 3D positioning may potentially be incompatible with the principles of purpose limitation and data minimisation of the General Data Protection Regulation (GDPR). The EDPB maintains that data controllers must give preference to processing anonymized geolocation data rather than personal data.[36]

3. EU legal and policy framework applicable to 5G

This Section will focus on the overview of the most relevant EU laws relevant for the development of privacy requirements for 5G networks. Due to the General Data Protection Regulation, European Electronic Communications Code and ePrivacy Directive, the rules on data protection and electronic communications in Member States have been significantly harmonized. These laws serve as a lex specialis

[33] Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Access, 6, 1–2. https://doi.org/10.1109/access.2018.2820162.
[34] Ibid.
[35] 5G Italy. (2018). 5G Italy White Book: from Research to Market. https://www.5gitaly.eu/2018/wp-content/uploads/2019/04/5G-Italy-White-eBook.pdf.
[36] EDPB 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', 5. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

for the processing of personal data and regulation of electronic communications. The decisions of the Court of Justice of the European Union, opinions and guidelines of Article 29 Working Party (an advisory body made up of the representatives of European Data Protection Authorities (DPA), now replaced by European Data Protection Board - EDPB), European Data Protection Supervisor, and BEREC (Body of European Regulators for Electronic Communications) affect the implementation and application of privacy, security and data protection legislation and thus are crucial for developing privacy requirements for 5G networks.

When developing privacy requirements for 5G Telecom Systems running virtualized multi-component services the legal provisions related to protecting user's privacy and personal data protection must be certainly paid exceptional attention. Considering various types and categories of data to be transferred through 5G networks and the technical challenges to distinguish between the types and categories of data the privacy requirements must be developed with keeping in mind the possibility that any piece of data transferred via 5G networks may be considered personal data. The application of EU data protection and privacy rules in mobile communications is a broad topic. Data protection and privacy in the EU is regulated primarily by the GDPR as *lex generalis*. However, when it comes to 5G networks, there is a number of other relevant legal acts to be assessed, such as the European Electronic Communications Code.

In 5G networks various third parties will be involved in processing personal data such as CSPs and third-party application developers. How to coordinate between and balance the competing interests of these actors is one of the most important legal questions to be addressed in the context of data protection and privacy of individuals, especially in light of the data protection by design obligation in Article 25 GDPR. Different laws – both national and European – may apply depending on the exact legal qualification of stakeholders, thus there is a need for legal certainty, which includes stability, consistency, and clarity of the law. Insufficient legal safeguards to activities of new stakeholders in mobile networks also raise legal issues related to loss of control of data, loss of data ownership, and ambiguity of liability of processors and controllers of personal data. These challenges may greatly affect the protection of user's rights with regard to the privacy and personal data.

Transferring personal data via cloud-based means and virtualized networks results in a complicated technical environment with multiple stakeholders who pursue different interests and apply different security standards. SDN providers, together with Cloud Service Providers (CSPs) become important stakeholders on the 5G telecom market and will process personal data of end-users, as well as other data - such as machine-to-machine communications - which may contain personal data of other individuals.

3.1. Privacy as a human and fundamental right

There is a need to explain the notion of privacy and its relation to data protection first. Privacy is not a new legal concept and is closely related to concepts of private life and personal interests.[37] US lawyers Samuel

[37] The protection of private life under Article 8 ECHR incorporates the notions of personal autonomy, autonomy, private social life (including communications), physical and moral integrity. See European Court of Human Rights. (2020). Guide on Article 8 of the European Convention on Human Rights. Council of Europe, pp. 21-23; and Schabas,

 Copyright © 5GhOSTS Consortium 2019-2023

Warren and Louis Brandeis argued for the recognition of the right to privacy in their article of the same name back in 1890 stating that "*Political, social, and economic changes entail the recognition of new rights*".[38] Through the developments in the 20th century, the right to privacy has become an accepted concept in Europe as well. The European Court of Human Rights (ECtHR) has adopted a dynamic and evolutive interpretation of the concepts of 'private life', which was stated to have a broad character "incapable of exhaustive definition", and 'personal interests', in order to produce decisions in line with technological advances.[39] The right to privacy is also mentioned and interpreted in recent cases of the Court of Justice of the European Union along with the right to data protection.[40]

The European Court of Human Rights (ECtHR) has adopted a dynamic and evolutive interpretation of the concepts of 'private life', which was stated to have a broad character "*incapable of exhaustive definition*", and 'personal interests', in order to produce decisions in line with technological advances.[41] Moreover, in a number of cases the ECtHR asserted that technologies such as electronic messages (Copland v. the United Kingdom[42]; Bărbulescu v. Romania[43]), Internet (Copland v. the United Kingdom), data stored on electronic storage devices (Wieser and Bicos Beteiligungen GmbH v. Austria[44]; Petri Sallinen and Others v. Finland[45]; Iliya Stefanov v. Bulgaria[46]) come within the scope of Article 8 of the European Convention on Human Rights (ECHR).[47] According to the Charter of Fundamental Rights of the European Union the right to privacy guarantees protection of private and family life, home and communications, with last point being especially relevant for this research. In the context of EU law, data protection and privacy are treated as separate concepts, with discussion ongoing on their precise legal nature.[48] Data protection in the EU

W. A. (2015). The European Convention on Human Rights: A Commentary (Oxford Commentaries on International Law) (1st ed.). Oxford University Press, pp. 369-370.

[38] Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220. doi:10.2307/1321160.

[39] European Court of Human Rights. (2020). Guide on Article 8 of the European Convention on Human Rights. Council of Europe, p. 21.

[40] Leenes, R., Brakel, V. R., Gutwirth, S., & Hert, D. P. (2017). Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, pp. 5-6. https://doi.org/10.1007/978-3-319-50796-5; see also Judgement of the CJEU in Case C-311/18.

[41] European Court of Human Rights. (2020). Guide on Article 8 of the European Convention on Human Rights. Council of Europe, p. 21.

[42] Copland v. the United Kingdom, 2007, ECHR 62617/00.

[43] Bărbulescu v. Romania, 2017, ECHR 61496/08.

[44] Wieser and Bicos Beteiligungen GmbH v. Austria, 2008, ECHR 74336/01.

[45] Petri Sallinen and Others v. Finland, 2005, ECHR 50882/99.

[46] Iliya Stefanov v. Bulgaria, 2008, ECHR 65755/01.

[47] European Court of Human Rights. (2020). Guide on Article 8 of the European Convention on Human Rights. Council of Europe, p. 105.

[48] See, for instance, Serge Gutwirth and Paul De Hert, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E Claes, A Duff and S Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006); Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' (2012) 26 International Review of Law, Computers & Technology 73; Gloria González Fuster and Serge Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 Computer Law & Security Review 531; Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 International and Comparative Law Quarterly 569; Damian Clifford, 'The legal limits to the monetisation of online emotions' (PhD thesis, KU Leuven 2019); Lorenzo Dalla Corte, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' in Dara Hallinan and others (eds), *Data Protection and Privacy: Data Protection and Democracy* (Hart Publishing 2020).

 Copyright © 5GhOSTS Consortium 2019-2023

legislation was interpreted in the context of economy, internal market and free movement of personal data.[49] Despite considerable overlapping, the legal nature of data protection and privacy differs in their scope. Privacy, being a fundamental right according to both the ECHR and the Charter of Fundamental Rights of the European Union is aimed to protect body, family, home and communications of the individual.[50]

Privacy, being a fundamental right according to both the ECHR and the Charter of Fundamental Rights of the European Union is aimed to protect body, family, home and communication of the individual.[51] The abovementioned article by Samuel Warren and Louis Brandeis raised the issue of privacy in context of newspaper publications and gossip, which may harm the reputation and psychological wellbeing of the individuals. Recent technological advances such as massive use of mobile and computer networks for storage of data, social networking and surveillance provided grounds for large scale invasion of privacy and the need to impose stricter rules on handling personal data. Implementation of 5G networks will have a dramatic impact not only on the economy and society, but also on the legal safeguards and protection of privacy and personal data.

3.2. Initial European efforts in harmonization of privacy legislation

The first European efforts to address the growing issue of data protection in computer era date back to 1970s. The Council of Europe adopted its Resolution 'On the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector' in 1973.[52] This short document defined the general principles of handling data by the members of the Council of Europe, but it was too early to speak about some European-wide approach to the protection of data and privacy. The legally binding Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108) was adopted in 1981 was the first major step in harmonization of privacy legislation in Europe, but considerable disparities in domestic privacy and data protection laws remained.[53]

The European Union undertook substantial efforts to develop and harmonize legislation pertaining to protection of personal data and privacy. The Data Protection Directive (DPD) adopted in 1995 was an important union-wide instrument for legislative harmonization in the field of data protection and privacy

[49] Leenes, R., Brakel, V. R., Gutwirth, S., & Hert, D. P. (2017). Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, pp. 5-6. https://doi.org/10.1007/978-3-319-50796-5.

[50] Gutwirth, S., Leenes, R., & Hert, D. P. (2016). Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection (Law, Governance and Technology Series Book 24) (1st ed. 2016 ed.). Springer, 198. https://doi.org/10.1007/978-94-017-7376-8.

[51] Ibid.

[52] Committee of Ministers of Council of Europe, Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, adopted on 26 September 1973 during 224th meeting of the Ministers' Deputies.

[53] Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37; Alsenoy, V. B. (2019). Data Protection Law in the EU: Roles, Responsibilities and Liability (6) (KU Leuven Centre for IT & IP Law Series) (First ed.). Intersentia, 3.

 Copyright © 5GhOSTS Consortium 2019-2023

in the EU.[54] The DPD defined the terms 'personal data' as "*any information relating to an identified or identifiable natural person ('data subject')*", and 'identifiable person' as "*one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".[55] The term 'privacy' was not defined separately and the text of the Directive refers to Article 8 of European Convention for the Protection of Human Rights and Fundamental Freedoms and 'the general principles of Community law'.[56] The DPD introduced important concepts of data processors and data controllers, with controller being a natural or legal person or public authority or agency which determines the purposes and means of the processing of personal data, and processor being any entity which processes this personal data on behalf of the controller.[57] Data processors and data controllers have distinct legal responsibilities with regard to the processing of personal data. The Directorate General of the European Commission for the Internal Market analyzed the application of the DPD and noted certain shortcoming of the Directive, but the adoption of the new text was considered untimely.[58]

3.3. GDPR

The reform of the EU legal and regulatory framework on data protection and privacy began in 2009 with the entry into force of the Treaty of Lisbon and creating major changes to the structure and competences of the EU.

GDPR serves as the general act on the protection of natural persons with regard to the processing of their personal data and applies inter alia to mobile networks. GDPR entered into force on 25 May 2018. Recital 2 explains the aim of GDPR and states that "*[t]his Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.*"

Recital 4 puts limits on the exercising the right to the protection of personal data, namely "*The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*."[59]

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31–50.
[55] Article 2(a) of the Directive 95/46/EC.
[56] Recital 10 of the Directive 95/46/EC.
[57] Article 2(d) and 2(e) of the Directive 95/46/EC.
[58] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 3.
[59] Recital 4 of 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, OJ L 119, 4.5.2016, p. 1–88 ('General Data Protection Regulation').

 Copyright © 5GhOSTS Consortium 2019-2023

5G technology is not directly referenced in GDPR, but its provisions are applicable to 5G technology and hence must be taken into account during the development of privacy requirements for virtualized components in the core network. In terms of 5GhOSTS project and considering the role 5G networks play in increasing the scale of collecting personal data the content of Recital 6 of GDPR is particularly relevant. It states that "*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."*[60]

Another important explanation is provided by Recital 26 which introduces the concepts of 'identified' and 'identifiable' persons as well as pseudonymization and anonymization in connection with personal data. Recital 26 reads: "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes*".[61]

Pseudonymization and anonymization techniques are extensively used in technology sector to preserve the integrity of data. A potential leak of two different pseudonymized sets of data containing entries on the same data subjects may result in identification of these persons. Considering the large number of various sets of data flowing through 5G networks the impact may prove to be substantial.

Territorial scope

Article 3 of GDPR contains provisions on the territorial scope of application of the regulation. This is particularly important for the development of privacy requirements for the purposes of 5GhOSTS research since many of service providers in 5G value chain are not located in the EU. Article 3(1) of GDPR sets that the regulation "*applies to the processing of personal data in the context of the activities of an*

[60] Recital 6 GDPR.
[61] Recital 26 GDPR.

 Copyright © 5GhOSTS Consortium 2019-2023

establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[62]

Article 3(2) further states, that GDPR also applies to the processing of personal data of EU data subjects even by controllers and processors not established in the EU territorially. Such cases include:

"*(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."[63]

This means that even if some service providers in 5G networks are not established in the EU they still have to comply with the provisions of GDPR.

Personal data

The concept of personal data is particularly important since it essentially defines the scope and aim of the whole regulation. According to Article 4(1) of GDPR personal data is "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

Since 5G networks enable the precise geolocation of users much easier compared to previous generations of mobile networks, the provision on location data of Article 4(1) of GDPR is of particular relevance. Another mobile network-specific piece of personal data is IMSI, as described in Par. 2.2.3. of this deliverable. The concept of personal data under GDPR is quite broad and the list provided in Article 4(1) is not exhaustive.

Controllers and processors

The concepts of 'controller' and 'processor' may prove to be the most confusing and problematic while developing privacy requirements for virtualized components of 5G networks. GDPR defines the controller as "*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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*".[64] Basically, any entity can become a controller, with organizations and companies of various legal forms constituting the majority of data controllers. This is confirmed by recent case law of the Court of Justice of the European Union (CJEU) in

[62] Article 3(1) GDPR.
[63] Article 3(2) GDPR.
[64] Article 4(7) GDPR

 Copyright © 5GhOSTS Consortium 2019-2023

Case C-272/19, V.Q. v Land Hessen. The CJEU stated that "*… the definition of the concept of 'controller' in Regulation 2016/679 is not confined to public authorities, but … is sufficiently wide to include any body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".[65] The broad interpretation of the concept of the controller is aimed at ensuring the protection of the rights of data subjects, as was stated by CJEU in Case C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV.[66] In practice a certain individual is usually appointed by this company or an organization to handle the responsibilities of the controller. In this case however the company or organization still bears the status of the controller and not the appointed individual.

A processor is "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".[67] A processor must constitute a separate entity from the controller. The processor processes data according to the instructions provided by the controller. The relationship between the controller and the processor is governed by a binding contract or other similar legal act.[68] A certain discretion remains with regard to the choice of technical and organizational means of processing but they still have to comply with the provisions of GDPR.

Joint controllership is a more complicated concept and involves two or more controllers jointly exercising their responsibilities and functions regarding the processing of personal data. It is important that while determining their respective responsibilities they must consider the rights of data subjects.[69] One corporate structure – involving a parent company and a subsidiary, for example – may have multiple controllers, especially in the case of distributed databases.[70]

According to the EDPB Guidelines on the concepts of controller and processor in the GDPR, the controller exercises influence through decision-making power over the processing of personal data.[71] In order to distinguish between a controller and a processor the factual but not formal analysis is needed.[72] This approach was confirmed by the CJEU in Case C-25/17, Jehovan todistajat.[73]

---

[65] CJEU 9 July 2020, C-272/19, ECLI:EU:C:2020:535 ('V.Q. v Land Hessen').

[66] "*As the Court has held previously, the objective of that provision is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects*", CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('Fashion ID case').

[67] Article 4(8) GDPR

[68] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. Adopted on 02 September 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[69] Ibid.

[70] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 149.

[71] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. Adopted on 02 September 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[72] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0. Adopted on 02 September 2020. Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[73] "*The case-law of the Court deriving from the judgment of 13 May 2014, Google Spain and Google (C-131/12, EU:C:2014:317), broadly defines the concept of 'controller' within the meaning of those provisions. Furthermore, it is clear from Opinion 1/2010 of 16 February 2010 on the concepts of 'controller' and 'processor' produced by the*

 Copyright © 5GhOSTS Consortium 2019-2023

Considering the complex software and hardware architecture of 5G networks in selected use cases (V2I, SO, RS) the identification of controllers and processors may prove challenging. The factual control, functions and data flows in these use cases must be established through an in-depth analysis, which requires a substantial amount of resources and expertise in both law and technology. 5G use cases may involve hundreds of different vendors with varying legal structures, responsibilities, and functions. The location of such vendors may include states from both EU and non-EU jurisdictions. Next to the principle of data protection by design established by the GDPR requiring companies to implement data protection measures at the earliest stages of designing processing procedures, there is a necessity to clarify the status of (joint) controllers and processors in virtualized 5G networks with a high degree of certainty. Such clarification is important for the purposes of liability, protection of user's rights, and transparency of personal data processing.

Recital 58 of GDPR states that "*the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected*". The Article 29 WP explicitly mentions that "*Complexity is no excuse for failing to provide information to the data subject*", which is extremely relevant to the case of 5G networks.[74]

Principles relating to processing of personal data and their application in virtualized 5G networks

Article 5 GDPR lists the principles relating to processing of personal data which serve as cornerstone rules of the whole Regulation.

According to Paragraph 1 of Article 5 GDPR personal data shall be (emphasis added):
"

*a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');*

*b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');*

Working Group set up pursuant to Article 29 of Directive 95/46, that, in particular, the 'effective control' and the conception that the data subject has of the controller must be taken into account.", CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('Jehovan todistajat case').

[74] The Article 29 Working Party 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP251rev.01, 25. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

*c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');*

*d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**');*

*e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);*

*f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**)."*[75]

Compliance with these principles is the foundation of privacy requirements for virtualized components of 5G networks.

Lawfulness, fairness, and transparency

Lawfulness, fairness and transparency incorporates three requirements and is aimed at protection of personal data from fraudulent gathering and processing. Recital 40 of GDPR articulates that "*In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*".[76]

Lawfulness is the first requirements of the principle and means that actors and vendors in 5G networks must respect all applicable laws and regulations regarding processing personal data. The DPD contained three 'cumulative conditions' necessary for compliance with the requirement of lawfulness, formulated by the CJEU as "*first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*".[77] Legitimate interest in a key component with regard to the compliance with the principle of lawfulness. As stated above, the legitimate interest must be pursued

[75] Article 5(1) GDPR.
[76] Recital (40) GDPR.
[77] CJEU 4 May 2017, Case C-13/16, ECLI:EU:C:2017:336 ('Rīgas satiksme case') and CJEU 11 December 2019, Case Case C-708/18, ECLI:EU:C:2019:1064 ('Asociaţia de Proprietari bloc M5A-ScaraA case').

 Copyright © 5GhOSTS Consortium 2019-2023

by (joint) controllers, third parties and parties to which the data are disclosed, which means that compliance with this requirement must be maintained by all actors in vendors processing personal data in 5G networks.

Transparency is defined in the relevant Recital 39 of GDPR as following (emphasis added):

"*Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data* ***be easily accessible and easy to understand****, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the* ***identity of the controller and the purposes of the processing*** *and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made* ***aware of risks, rules, safeguards and rights*** *in relation to the processing of personal data and how to exercise their rights in relation to such processing [...]*"[78]

The Recital provides us with the specific elements of transparency of data processing. They include (a) easy access to information regarding processing; (b) clear identity of the controller and the purposes of the processing; (c) provision of information regarding risks, rules, safeguards and rights. The vendors in 5G use cases must ensure compliance with these elements, namely give the information regarding processing personal data, identify the structure of (joint) data controllers and exhaustive explanations regarding purposes of processing and provide the information on possible risks, rules, safeguards and data subject's rights. As we mentioned before, the complex and dynamic software-defined architecture of 5G value chains may prove to be an obstacle to compliance with this principle.

Fairness requires that personal data must be obtained through valid and fair means and not through fraud, deception or without awareness of the data subject.[79] The fairness requirement is closely related to the transparency requirement, but is stated separately and explicitly in the GDPR. Fairness also implies that controllers and processors should process data only in ways that data subjects would reasonably expect.[80] In order to comply with the fairness requirement it is possible that a certain 'fairness assessment' or analysis of how processing personal data may affect the data subjects is needed.

The Article 5(1)(a) principle of lawfulness, fairness, and transparency of data processing affects the implementation of SDN and NFV in 5G due to the dynamic nature of these technologies as well as the presence of multiple new stakeholders in 5G networks and associated transparency risks.

[78] Recital 39 GDPR.

[79] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 314.

[80] Information Commissioner's Office. (2020). Guide to the General Data Protection Regulation (GDPR). ICO, 22. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

 Copyright © 5GhOSTS Consortium 2019-2023

Purpose limitation

Purpose limitation is the second processing principle defined by Article 5(1)(b) GDPR and requires that personal data is gathered for specified, explicit and legitimate purpose. This principle is linked to the principle of lawfulness, fairness and transparency. Recital 39 states: "*In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data*".[81] Processing of personal data without clear information regarding the limited and defined purposes is unlawful.[82] The controller must define the purposes of processing data and inform the data subject about them before such processing actually takes place. Since 5G value chain involves a large number of actors and vendors processing data it is important to ensure that all actors and vendors comply with the original purposes of data processing and do not use the personal data for any other purpose. According to Article 29 Working Party Opinion 03/2013 on purpose limitation "*[t]he development of new technologies results in increasingly more data being available, for a great diversity of purposes*".[83] According to the same Opinion, *"[t]he legitimacy of a given purpose can also change over time, depending on scientific and technological developments, and changes in society and cultural attitudes"*.[84] Data controllers operating in 5G market will need to ensure the provision of free, accessible, specific and unambiguous information on the purposes of personal data processing. Such purposes may vary depending on the specific vendor or party processing personal data. Purposes themselves must be clear, precise, explicit and legitimate. Legitimate purposes should not lead to a disproportionate interference with the rights, freedoms and interests of the data subject favoring the interests of the data controller.[85]

Data minimization

Data minimization principle is listed in Article 5(1)(c) GDPR and requires limiting the processing of personal data to 'what is necessary in relation to the purposes for which they are processed' providing a clear link with the principle of Purpose limitation. Recital 39 contains provisions explaining the principle of data minimization, namely "*The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access*

[81] Recital (39) GDPR.
[82] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 315.
[83] Article 29 Working Party 'Opinion 03/2013 on purpose limitation', 00569/13/EN WP 203', 14. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[84] Ibid, 20.
[85] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 315.

 Copyright © 5GhOSTS Consortium 2019-2023

to or use of personal data and the equipment used for the processing".[86] Controllers must refrain from processing any excessive personal data not required for their purposes and avoid collecting irrelevant data from the data subjects. Some researchers suggest various techniques aimed at the implementation of data minimization principle with regard to privacy-disruptive technologies, such as 'minimizing model accuracy loss' technique applicable to machine learning solutions.[87] It is important to ensure that the roll-out of virtualized 5G networks is accompanied by privacy-preserving technologies and techniques.

Accuracy

The principle of accuracy is defined in Article 5(1)(d) and requires controllers to keep the data up to date and rectify or erase the inaccurate and incomplete data.[88] This principle is linked to Article 17 GDPR which guarantees the right to erasure (or the 'right to be forgotten'). Article 17(1) states that *"[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay […]".*[89] Data controllers in 5G networks will have to take "*account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data*" as stated in Article 17(2) GDPR. Considering the technological novelties brought by the new generation of mobile networks and complications related to processing huge amounts of data it is unclear how exactly this principle will be implemented in virtualized 5G networks. In practice it may be virtually impossible to rectify or erase personal data from the technological perspective. Another technical problem is to keep detailed records of data processing activities and track the flow of personal data. Such records may require substantial resources, and their implementation can be complicated.

The Figure 2 visualizes the structure of principles relating to processing of personal data as described in Article 5 GDPR.

[86] Recital (39) GDPR.
[87] Goldsteen, A., Ezov, G., Shmelkin, R., Moffie, M., & Farkash, A. (2020). Data Minimization for GDPR Compliance in Machine, 3.
Learning Models. arXiv preprint arXiv:2008.04113.
[88] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 317.
[89] Article 17 GDPR.

 Copyright © 5GhOSTS Consortium 2019-2023

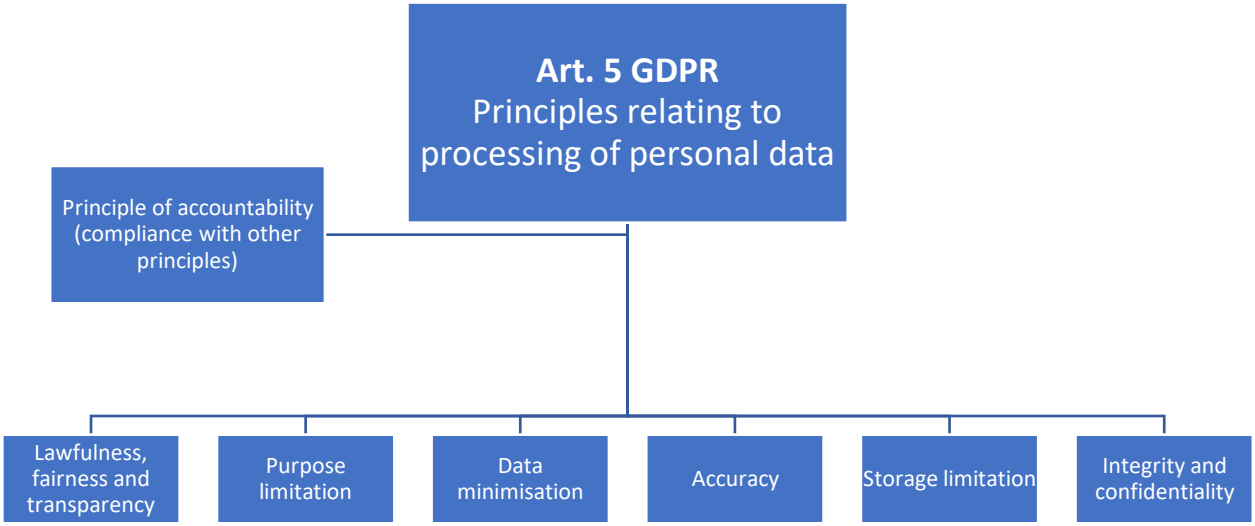

FIGURE 2. GDPR Principles relating to processing of personal data

Storage limitation

The storage limitation principle is specified by Article 5(1)(e) of GDPR. This principle requires controllers to clearly indicate the specific and adequate timeframe for storing personal data. It is prohibited for data controllers to retain gathered personal data beyond the timeframe necessary to process data according to the purposes for such processing.[90] Controllers in 5G will need to apply privacy-preserving techniques, like in the case of data minimization principle. Possible techniques may include so-called data 'pruning' considered for use in relation to blockchain technology.[91] While assessing the risks posed by blockchain

[90] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 318.

[91] Data pruning was mentioned by European Parliamentary Research Service (EPRS) as a possible GDPR-compliant privacy risk-mitigating technique while implementing blockchain technology. Specifically the EPRS states that "*[p]running could be a solution to the problems the indefinite storage of data creates from the perspective of key data protection principles such as that of data minimisation and storage limitation. Pruning enables for data to be removed from blockchains when it is no longer needed or wanted. As all solutions, pruning however comes with considerable trade-offs, and it has also been stressed that although the size of the archival node can be reduced through pruning, all the information necessary to recreate the older state is still saved on each node, meaning that is it unlikely that this could qualify as an anonymisation measure from a GDPR perspective".* It is possible to draw certain similarities between privacy disruptions caused by blockchain and virtualized 5G networks. Some of the techniques recommended for privacy risk mitigation in blockchain may be used in 5G networks as well, after a careful and rigorous assessment. See European Parliamentary Research Service. (2019). Blockchain and the General Data

 Copyright © 5GhOSTS Consortium 2019-2023

Commission Nationale de l'Informatique et des Libertés (CNIL, French Data Protection Authority) stated that in exceptional cases some information can be stored without a retention period.[92] However, in such cases a data protection impact assessment (DPIA) is required. Certain exceptions are likely possible in 5G networks as well, but they are extremely limited and must be backed by legal obligations.

Integrity and confidentiality

Article 5(1)(f) GDPR lists 'appropriate security' (labelled as 'integrity and confidentiality principle') as one of the principles relating to the processing of personal data. It entails that processing of personal data is done "*in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".[93] The security principle is hence linked to technical and organizational measures ensuring compliance with GDPR, as well as risk analysis and privacy policies.[94] It is important to note that security under GDPR is not limited to cybersecurity but also covers physical security like processing paper-based personal data. 5G networks are designed to use SDN and NFV at a large scale and hence are important technological novelties compared to previous generations of mobile networks; yet, they also create new challenges to security. As mentioned above, multiple stakeholders will be responsible for different elements in 5G networks and may apply different security standards and tools. NFV and SDN contribute to efficiency but raise concerns regarding the security of data and the increased number of opportunities for possible attacks. Cloud-based networks together with NFV and SDN may be reconfigured in numerous ways to create various types of networks with different standards and solutions pertaining to privacy and security. Stakeholders such as SDN providers, CSPs, and third-party developers may be wary of sharing their architectural or IT solutions in order to ensure transparency and react to inquiries from individuals and regulatory bodies. Lack of formal requirements on transparency may result in different objectives in trust pursued by different stakeholders and causes a situation where users are unable to obtain reliable information on the security standards and tools used to protect their data. Another concern is related to the use of equipment and software from previous generations of mobile networks by 5G networks, namely that together with cutting costs and ensuring the interoperability of different generations of equipment 5G inherits their unresolved security vulnerabilities. These challenges emphasize the importance of understanding technical concepts and specific network parameters for the development of privacy requirements.

Protection Regulation. Can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[92] "*If justified by the purpose of the processing and if a data protection impact assessment (DPIA) has proven that the residual risks are acceptable, personal data may exceptionally be stored on the blockchain, in the form of a traditional fingerprint (without a key) or even in cleartext. Indeed, some data controllers may have the legal obligation to make some information public and accessible, without a retention period: in this particular case, the storage of personal data on a public blockchain can be envisaged, provided that the DPIA concludes that the risks for data subjects are minimal*." Commission Nationale de l'Informatique et des Libertés. (2018). Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[93] Information Commissioner's Office. (2020). Guide to the General Data Protection Regulation (GDPR). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

[94] Ibid.

 Copyright © 5GhOSTS Consortium 2019-2023

Accountability

The final principle is principle of accountability and is defined by Article 5(2) of GDPR. This principle is essentially an obligation to ensure compliance with all principle listed in Article 5(1) of GDPR. Article 29 WP referred to 'data deluge' effect "*where the amount of personal data that exists, is processed and is further transferred continues to grow*".[95] The principle of accountability requires data controllers to adopt measures to effectively comply with the data processing principles and demonstrate such compliance. Technological developments contribute to the growth of the amount of data being processed, and so the impact of data breaches and data leaks as well as risk of misuse of personal data increase.[96] Legal certainty was also mentioned by Article 29 WP as one of the challenges towards the implementation of principle of accountability since the requirements of the principle are not detailed.[97] The ways and instruments to assess the level and effectiveness of compliance with the principle of accountability may differ and are flexible. According to the Opinion of Article 29 WP, "*[f]or larger, more complex and high risk processing, internal and external audits are common verification methods*".[98] There is no list of verification ways or authorized methodologies, but the Opinion of Article 29 WP mentions voluntarily certification as one of the instruments of achieving compliance. The accreditation of certification programs is usually regulated by EU and national legislation. Since 5G networks definitely fall withing the category of 'complex and high risk processing' and may contribute to 'data deluge' effect mentioned by Article 29 WP, it is likely that the compliance of vendors and actors processing data through 5G networks with the principle of accountability will be subject to scrutiny by national DPAs.

The Table 1 below summarizes possible disruptions, risks and conflicts posed by technological solutions introduced in 5G networks as identified in Section 3.3 (top row) to principles indicated in Article 5 of GDPR (left column).

[95] Article 29 Working Party 'Opinion 3/2010 on the principle of accountability', 00062/10/EN WP 173', 4. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[96] The EDPB maintained that *"[…] nature, sensitivity, and volume of personal data increases the risks further, because the number of individuals affected is high, as is the overall quantity of affected personal data[…]"* and "*[a]s usual, during risk assessment the type of the breach and the nature, sensitivity, and volume of personal data affected are to be taken into consideration*" linking volume of data to the impact of data breaches. See: EDPB 'Guidelines 01/2021 on Examples regarding Data Breach Notification', 12-19. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf; With regard to surveillance technologies the EDPB noted that "*[t]he amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use […] or even the risks of misuse*" linking the amount of generate data to the risks of inappropriate use (not conforming to the original purpose) or misuse. See: EDPB 'Guidelines 3/2019 on processing of personal data through video devices', 4. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

[97] Article 29 Working Party 'Opinion 3/2010 on the principle of accountability', 00062/10/EN WP 173', 14. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

[98] Ibid, 15.

 Copyright © 5GhOSTS Consortium 2019-2023

	New stakeholders in 5G networks (including SDN providers)	SDN and NFV - enabled architectural network flexibility and high-speed rates	Usage of cloud and edge computing technologies	Amount of 5G-enabled sensors and devices	Increased volume of processed personal data	Precise geolocation and identification
Lawfulness, fairness and transparency of data processing	X	X	X	X	X	X
Purpose limitation	X			X		X
Data minimisation				X	X	X
Accuracy	X			X	X	
Storage limitation	X				X	
Integrity and confidentiality (security)	X			X		
Accountability	X			X		

TABLE 1. Correlation between technological solutions and principles relating to processing of personal data

Data protection by design and by default

Article 25 of GDPR established principles of data protection by design and by default, which require all controllers to implement technical and organizational measures "*[t]aking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*" in order to protect the rights of data subjects both at the time of the determination of means for processing and during the processing itself.[99] The implementation of technical and organization measures is needed to ensure that 'by default' only personal data which is necessary to achieve purposes according to purpose limitation is processed.[100] Recital 78 of GDPR provides additional requirements in this regard such as "*the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default*" and "*minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and*

[99] Article 25(1) GDPR.
[100] Article 25(2) GDPR.

 Copyright © 5GhOSTS Consortium 2019-2023

processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features".[101] In some discussions a term 'Privacy by design' is used as an equivalent to 'Data protection by design'.

Recital 78 also imposes substantial obligations on the developers of applications and services namely "*[w]hen developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders*". The last sentence explicitly links the adherence to data protection by design and by default principles to competition in public tenders, which is particularly relevant for 5G vendors.

The principle of data protection by design and by default requires developers of applications, services and products to consider privacy and data protection principles early at the development of their respective goods and services. The belief is that incorporation of privacy and data protection requirements early substantially improves the privacy and data protection resilience and compliance of applications, services and products.[102] These legal provisions are aimed at ensuring the high efficiency of protection of data subjects' rights. The data controllers have a legal duty to implement technical and organization measures to ensure compliance with data protection principles. These measures go beyond the security and reliability of software and include business practices, organizational principles etc.[103] Using the wording of EDPB Guidelines on data protection by design and by default technical and organizational measures "*can be anything from the use of advanced technical solutions to the basic training of personnel*".[104] The commonly mentioned examples include pseudonymization of personal data, providing access to data to data subjects, ensuring security of data, training employees of the data controller and data processor on the principles and practices of handling personal data, contractual obligations of data processors to implement a certain level of compliance with data minimization practices.[105] There is no exhaustive or definite list of such measures, however. Effectiveness is the most important criteria when assessing the

[101] Recital (78) GDPR.

[102] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 573.

[103] Ibid, 577.

[104] EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0', Adopted on 20 October 2020, 6. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[105] See Information Commissioner's Office. (2020). Guide to the General Data Protection Regulation (GDPR). ICO, 167. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/; Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 577; EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0', Adopted on 20 October 2020, 6. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

level of compliance with the principle of data protection by design and by default.[106] The controller is required to document the implementation of technical and organizational measures and may determine certain effectiveness indicators.[107]

These principles might prove to be particularly challenging to comply with in 5G networks, especially when considering SDN, NFV, NS and cloud technologies used as well as the number of vendors and actors in the value chain.

3.4. ePrivacy Directive

Specific rules on privacy in telecommunications, initially adopted in 1997,[108] have been modernised in 2002[109] and 2009,[110] and may be replaced in the near future by the ePrivacy regulation.[111] Directive 2002/58/EC (ePrivacy Directive) was adopted in 2002 as a sector-specific piece of legislation with the intention to ensure the protection of privacy, personal data (including location data) and confidentiality of electronic communications.[112] The ePrivacy Directive's scope also includes the regulation of 'cookies' – small files storing data in user's browser. The ePrivacy Directive defines communications as "*any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service*", and includes information transmitted as a broadcasting service if such

[106] "*Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller […] Article 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk*" via EDPB 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0', Adopted on 20 October 2020, 7. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[107] Ibid.

[108] Directive 97/66/EC was adopted in 1997 and referred to ECHR and national constitutions as the basis for the protection of confidentiality: "*Whereas confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States*" (Recital 2). The Directive 97/66/EC was aimed at harmonization of national legislation of Member states related to the protection of the right to privacy with respect to the protection of personal data in telecom sector and create conditions for the free movement of such data. See: Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997, OJ L 24, 30.1.1998, p. 1–8.

[109] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, OJ L 201, 31.7.2002, 37–47.

[110] Directive 2009/136/EC of the European Parliament and of the Council of 25 November, OJ L 337, 18.12.2009, 11–36.

[111] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final.

[112] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

 Copyright © 5GhOSTS Consortium 2019-2023

transmission contains no data which may lead to identification of the subscriber.[113] The term 'value added service' means any service processing traffic or location data, excluding when it is necessary for transmission or billing purposes.[114]

Much of attention was given to the protection of location data in ePrivacy Directive. The analysis of the provisions relation to location data is dictated by the fact that geolocation is one of the key privacy-disrupting technologies, as explained in paragraph 2.2.3. of this deliverable. According to Article 9(3) of the ePrivacy Directive, "*Processing of location data other than traffic data […] must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service*." This provision applies to any third parties involved in processing personal data through 5G networks as well, such as CSPs, SDN service providers etc.[115]

The provisions of the ePrivacy Directive make it clear that communication taking place in 5G networks in general and the use cases in particular fall within the scope of the Directive, specifically with regard to the electronic communications and location data.

There have been calls by the European Data Protection Board (EDPB) for amending the ePrivacy Directive and replacing it with a more comprehensive legislative instrument, especially in light of the adoption of the new GDPR in 2016.[116] The ePrivacy Directive does not apply to Internet-based communication services while EDPB considers such services "*functionally equivalent*" to traditional telephone communications infrastructure.[117] The European Commission published a Proposal for the new ePrivacy Regulation (the

[113] Article 2(d) of the ePrivacy Directive.
[114] Article 2(g) of the ePrivacy Directive.
[115] Article 9(3) of the ePrivacy Directive.
[116] See for example Statement 3/2019 on an ePrivacy regulation adopted on 13 March 2019 by the European Data Protection Board available at: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_en.pdf; and Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, adopted on 25 May 2018, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.
The EDPB continuously stated that new ePrivacy Regulation must not lower the level of protection offered by ePrivacy Directive, and must complement the GDPR namely with regard to consent rules. The EDPB stated that "*the ePrivacy Regulation is necessary to ensure a level playing field and legal certainty for market operators*" (Statement 3/2019) and "*consent should be obtained systematically in a technically viable and enforceable manner before processing electronic communications data or before using the storage or processing capabilities of a user's terminal equipment. There should be no exceptions to process this data based on the 'legitimate interest' of the data controller, or on the general purpose of the performance of a contract*" (Statement on 25 May 2018) which is especially relevant for 5G networks due to the challenge of obtaining consent before the processing actually takes place.
[117] European Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, adopted on 25 May 2018, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf

 Copyright © 5GhOSTS Consortium 2019-2023

Proposal) replacing ePrivacy Directive in 2017.[118] In February 2021 the Council of the EU confirmed its position on an updated ePrivacy Regulation.[119] The updated Proposal changed the wording on confidentiality in Recital 1 of the Proposal directly linking it to the right to privacy.[120] The Proposal also uses the definitions established by the European Electronic Communications Code (EECC), namely the definition of electronic communications services, noting that the new definition of the EECC includes not only services provided via internet but also 'interpersonal communications services' such as voice over IP (VoIP), messengers and email services.[121] This definition covers a substantial number of actors and use cases in 5G networks. With regard to the use cases used in this deliverable, the Proposal specifically mentions that "*transmission of machine-to-machine or Internet of Things services regularly involves the conveyance of signals via an electronic communications network and, hence, constitutes an electronic communications service*"[122] potentially covering the massive amount of M2M communications data.

Additionally, potential challenges may arise due to the restrictive nature of the provisions of the Proposal related to automated processing of electronic communications data. The Proposal indicates that 'any interference of electronic communications data' is prohibited, and interception is qualified as essentially any action performed with the communications data 'for purposes other than the exchange of communications'.[123] The user consent will be required for scanning and storing the content of the electronic communications including metadata. While telecommunication providers in 5G networks may obtain this consent for the purpose of providing the service of exchange of communications, it might potentially be a challenge for other actors in 5G networks (e.g. CSPs, SDN service providers etc.) to obtain the same consent for their operations with data, since it is unclear whether such operations may qualify as required for purposes of exchanging communications.

3.5. Open Internet Regulation

In practice in 5G networks network slicing technology may cause different network 'slices' to get different priorities meaning that data of certain consumers may be processed with preference. The implementation of network slicing must comply with EU net neutrality rules established by Regulation 2015/2120 (Open

[118] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD)

[119] Council of the EU. (2021, February 10). Confidentiality of electronic communications: Council agrees its position on ePrivacy rules [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

[120] "*Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") protects the fundamental right of everyone to the respect for private and family life, home and communications. Respect for the confidentiality of one's communications is an essential dimension of this right, applying both to natural and legal persons*", Recital 1 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003(COD) (Proposal for the ePrivacy Regulation).

[121] Recital 11 of the Proposal for the ePrivacy Regulation.

[122] Recital 12 of the Proposal for the ePrivacy Regulation.

[123] Recital 15 of the Proposal for the ePrivacy Regulation.

 Copyright © 5GhOSTS Consortium 2019-2023

Internet Regulation) and BEREC Net Neutrality Guidelines.[124] These guidelines clarify the implementation of EU net neutrality rules on equal treatment of traffic. Moreover, in light of the recent judgment of the CJEU in joined cases C-807/18 and C-39/19 on open internet access, the compliance of NFV and SDN with principles of technology neutrality and internet neutrality as stated in Regulation 2015/2120 must be taken into account during the implementation of these technologies. Implementation of SDN and NFV must not hinder the data protection and privacy standards of the EU and ensure the compliance with innovation principle and principles of technology and net neutrality and contribute to enhancement of infrastructure competition.

3.6. European Electronic Communications Code

Another relevant European legislation that governs digital networks and services is the European Electronic Communication Code (EECC), which directly mentions 5G and underlying technology of SDN. The EECC was adopted in 2018 to replace the previous generation of EU directives on electronic communications[125] and governs the activities of ECS providers, including the implementation of SDN. The EECC deals primarily with legislative harmonization, competition and protection of end-user interests and is aimed at the implementation of internal market in electronic communications networks and services.[126] Important concepts defined by the EECC and relevant for 5GhOSTS project research include 'Electronic communications service', 'Electronic communication network', 'Associated service' and 'Security of networks and services'. According to Article 1 EECC it "*establishes a harmonised framework for the regulation of electronic communications networks, electronic communications services, associated facilities and associated services, and certain aspects of terminal equipment. It lays down tasks of national regulatory authorities and, where applicable, of other competent authorities, and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Union.*"

Electronic communications service (ECS) is defined as a paid ('for remuneration') service provided via electronic communications networks and includes 'internet access service', 'interpersonal communication service' and 'services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting'.[127] The interpersonal

[124] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015, OJ L 310, 26.11.2015, 1–18; BEREC. (2020). BEREC Guidelines on the Implementation of the Open Internet Regulation. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation.

[125] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108, 24.4.2002, p. 33–50.

[126] Article 1(2)(a) EECC; See also: Serge Gijrath. (Re-)Defining Software Defined Networks under the European Electronic Communications Code. (2019). ELaw, 2019/007.

[127] Article 2(4) EECC. 'Internet access service' is defined as "*a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used*" by Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

 Copyright © 5GhOSTS Consortium 2019-2023

communication service (ICS) is defined as "*a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service*".[128] ICSs include traditional voice calls, emails, messengers, chats etc.[129] The addition of ICS is particularly important since it broadens the scope of the ECS.[130] The exact legal status of ECS is of high importance for 5GhOSTS research because of the possibility of bestowing the status of ECS providers upon SDN and NFV providers. The EECC does not directly qualify the NFV and SDN providers as ECS providers; however, such possibility is not excluded by the researchers.[131]

Electronic communication network (ECN) according to the EECC is any transmission system "*whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed*".[132] The governance of ECNs is still largely vested with national regulatory authorities (NRA) and the BEREC.[133] The overlap between different legal obligation stemming from the EU and national legal frameworks may affect the compliance and roll-out of 5G networks due to the need to comply with different national jurisdictions. The overall legal harmonization at EU level in relation to privacy and data protection mitigates the risk, but the issue of governance of ECNs remains.

Associated service is any service "*associated with an electronic communications network or an electronic communications service which enables or supports the provision, self-provision or automated-provision of services via that network or service, or has the potential to do so, and includes number translation or systems offering equivalent functionality, conditional access systems and electronic programme guides (EPGs), as well as other services such as identity, location and presence service*".[134]

Security of networks and services is defined as "*the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or*

[128] Article 2(5) EECC.
[129] European Commission. (2016). Review of the Electronic Communications Regulatory Framework - Executive Summary 2: Services, End-users' rights. https://digital-strategy.ec.europa.eu/en/library/review-electronic-communications-regulatory-framework-executive-summaries, 2.
[130] Serge Gijrath. (Re-)Defining Software Defined Networks under the European Electronic Communications Code. (2019). ELaw, 2019/007, 10.
[131] Ibid, 31.
[132] Article 2(1) EECC.
[133] Serge Gijrath. (Connectivity & Interoperability in Society 5.0. Technological principles for network regulation: a new lease of life for network operators? (2019). ELaw, 2019/008, 3.
[134] Article 2(11) EECC.

 Copyright © 5GhOSTS Consortium 2019-2023

of the related services offered by, or accessible via, those electronic communications networks or services".[135] The security characteristics of availability, authenticity, integrity and confidentiality are particularly important with regard to communications privacy and data protection in 5G.

4. Privacy, security, and data protection risks in virtualized 5G networks

As was described in Section 2 of this deliverable virtualized 5G networks bring a wide range of privacy-disrupting technological novelties, which include virtualization, edge computing and precise geolocation among others. The combination of SDN, NFV, edge and cloud computing may potentially cause a plethora of privacy, security and data protection challenges.[136] The use of VNFs provides a larger amount of possible attacks such as spoofing, sniffing, and denial-of-service and vulnerabilities, such as configuration errors which may affect the security of personal data.[137] Device-to-device (D2D) communication in 5G allow devices in the networks to communicate directly without the need for the cellular core network, devices to communicate directly without the need for the cellular core network, allowing to offload some of the traffic from the nodes in 5G networks but posing substantial risks with regard to security and privacy of data.[138]

The following is the non-comprehensive list of potential privacy, security and data protection risks in 5G networks:

- **Precise user geolocation –** 5G uses a larger number of base stations, IoT devices and sensors than previous generations of mobile networks. Precise geolocation of data subjects (users of 5G networks) under such conditions becomes much easier. As was mentioned before, location data and online identifiers are defined in Article 4(1) of GDPR as personal data, since such information may lead to the identification of the data subject.[139] Huge amount of personal data allows the identification of persons with higher precision which causes concerns regarding profiling and automated decisions. Article 29 WP suggested to consider location data and online identifiers personal data in its Opinion 08/2012 providing further input on the data protection reform discussions.[140] In its Opinion 13/2011 on Geolocation services on smart mobile devices

[135] Article 2(21) EECC.

[136] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF), p. 2. https://doi.org/10.1109/5gwf.2018.8516981.

[137] Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, 2(1), 3. https://doi.org/10.1109/mcomstd.2018.1700063.

[138] Zhang, A., & Lin, X. (2017). Security-Aware and Privacy-Preserving D2D Communications in 5G. IEEE Network, 31(4), 70–77. https://doi.org/10.1109/mnet.2017.1600290.

[139] Article 4(1) GDPR.

[140] "[I]dentification numbers, location data, online identifiers or other specific factors as such should as a rule be considered […] personal data […]". See Article 29 Working Party 'Opinion 08/2012 providing further input on the data protection reform discussions', 01574/12/EN WP199, 6. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

Article 29 WP stated that "*smart mobile device is very intimately linked to a specific individual*".[141] This statement explains the reasoning behind the attention to the protection of location data as personal data. It is further explained that the owner of the smartphone stores large amounts of personal data on the device and rarely gives it to another person, which makes a smartphone a sort of an equivalent to the unique identifier related to a specific individual. Anyone who gets lawful (location services providers, telecommunication providers, various applications) or unlawful (attackers) access to the geolocation data may as well deduce the home address, workplace, habits, and routine of the of the data subject. Geolocation data may be qualified as a special category of personal data if it reveals political opinions (e.g. attendance of political rallies, gatherings, meetings), religious beliefs (attendance of religious establishments or sites), trade union membership (attendance of trade union meetings) of the data subject as stated in Article 9(1) of GDPR.[142] It is important to mention that geolocation is possible not only via personal smartphones of data subjects but also using embedded sensors and devices. This creates an additional potential challenge of tracking the person without a smartphone or without their explicit and informed consent to such tracking. While geolocation was possible in 3G and 4G networks, 5G networks bring it on another level by enabling the high precision and speed of such geolocation not possible in previous mobile networks. As was mentioned before 5G also enables 3D positioning through MIMO.[143] Correspondingly, the requirements for the informed consent may be stricter since the impact of the data breach or data leak are higher. Various application developers and vendors may require user's consent for processing geolocation data in order to provide their services to the users. In such case vendors and app developers become data controllers to the extent they process personal data and must provide the necessary information to the user as described in paragraph 3.5. of this deliverable. Consent must be specific and linked to the specific purpose of data processing.

- **Profiling and automated decision-making –** Recital 71 of GDPR states that "*[t]he data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention*". Profiling and automated decision-making is regulated by Article 22 GDPR which states the right of the data subject not to be subject to a decision based exclusively on automated processing, unless such profiling: (a) is necessary for entering into or performing a contract between a data subject and a controller; (b) is authorized by EU or Member State law; (c) is based on an explicit consent of the data subject. In any case of profiling or automated decision-making the data controller is obliged to impose suitable measures to safeguard data subject's rights and freedoms and legitimate interests. The Article 29 WP in its Guidelines on profiling and automated decision-making stated that *"[a]dvances in technology and the capabilities of big data*

[141] Article 29 Working Party 'Opinion 13/2011 on Geolocation services on smart mobile devices', 881/11/EN WP 185, 7. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.
[142] Article 9(1) GDPR.
[143] 5G Italy. (2018). 5G Italy White Book: from Research to Market. https://www.5gitaly.eu/2018/wp-content/uploads/2019/04/5G-Italy-White-eBook.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms" which most likely includes 5G networks.[144] Profiling according to the Guidelines of Article 29 WP consist of three elements – (a) automated form of processing, (b) carried out on personal data and (c) the objective of the profiling measures is to evaluate personal aspects about a data subject. Automated decision-making is a related concept which can potentially overlap with or result from profiling. Data protection principles apply to both profiling and automated decision-making. The Guidelines specifically mentions that "*Complexity is no excuse for failing to provide information to the data subject*" referring to Recital 58 of GDPR.[145] The increase in the amount of personal data processed by vendors using 5G networks and the high speed of such processing contributes to the increase of precision and definiteness of identification of individuals, their personalities which creates a substantial risk to data subject's rights in terms of profiling and automated decision-making. Namely, this can affect employees' rights in Smart Office use case, patients' rights in Remote Surgery use case and drivers' and passengers' rights in Vehicle to Infrastructure use case. The EDPB provides a specific guidance with regard to privacy and protection of personal data in connected vehicles: "*[…] connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts or data collected by cameras may concern driver behavior as well as information about other people who could be inside or outside the vehicle*".[146]

- **Responsibility ambiguity –** as was mentioned before the architecture of virtualized 5G networks is complex and involves numerous actors and vendors processing personal data. At the same time a considerable technical, organizational and legal challenge is to clearly define roles and responsibilities with regard to processing personal data in 5G networks among various parties. This challenge is related not just to the liability of data controllers and data processors, but also to the potential loss of data ownership, dilution of responsibilities, and loss of control over the technology environment for processing data between the actors and vendors in 5G networks.[147] The CSPs, SDN providers, equipment manufacturers, software providers, application developers will almost surely have different uncoordinated privacy, security and data protection policies,

[144] Article 29 Working Party 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP251rev.01. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[145] Article 29 Working Party 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 17/EN WP251rev.01. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[146] EDPB, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications', 3. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[147] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF); Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

measures and objectives regarding processing personal data. Depending on their jurisdiction, these actors may potentially be required to provide personal data of EU citizen or access to communications by legislation, courts or law enforcement agencies.[148] This ultimately results in a whole range of legal challenges to privacy, security, and data protection and most importantly to the effectiveness of protection of data subjects' rights in 5G networks. Responsibility ambiguity affects all 5G use cases, but is especially relevant for Remote Surgery use case, since it involves special categories of data and various provisions on medical devices and healthcare.

- **Security standards, security architecture and inheritance of security and privacy challenges –** The lack of homogenous security standards and approaches among the actors and vendors creates a weak point in security and confidentiality of communications in 5G networks and may lead to data breaches, data leaks and greater number of access points for potential attackers. The reliance of 5G networks on IP-based architecture and cloud solutions leads to the increase in possibilities for hacking and other types of cyber-attacks. Access control, communication security, data confidentiality and data availability might also be affected.[149] 5G vendors are most likely to rely on the equipment and security architecture used by 3G and 4G networks, at least at the beginning of the roll-out of 5G. Such reliance reduces the costs of implementation of 5G but also means that 5G inherits the security vulnerabilities of previous-generation equipment and architecture. The use of SDN, NFV, and NS in new mobile networks creates a risk of data leak between functions shared among different slices.[150] SDN, NFV, NS, and cloud technologies also increase the reliance of 5G on software stability and software updates. This mean the greater vulnerability of core network of 5G to software bugs, system stability, back doors, malware, computer viruses and hacking.[151] Some of 5G vendors may be lagging in implementing updated and changes due to a range of technical and business reasons.[152] Some of the ECS providers and CSPs may not provide the sufficient information on their security measures and policies.[153] Vulnerabilities in Remote Surgery and Vehicle to Infrastructure use cases may cause severe consequences due to their impact on health, safety, and wellbeing of people.

- **Grounds for processing personal data and dilution of consent –** Ubiquitous presence of 5G-enabled sensors and devices makes possible the gathering of massive amounts of personal data which includes precise geolocation and identification of individuals. A huge amount of such sensors and devices along with the flexible architecture of SDN and NFV affects the application of

[148] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[149] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, 8, 108052–108061. https://doi.org/10.1109/access.2020.3000662.
[150] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[151] Ibid.
[152] Cybersecurity and Infrastructure Security Agency. (2019). Overview of risks introduced by 5G adoption in the United States. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
[153] Teatini, S., & Matinmikko-Blue, M. (2020). Privacy in the 5G World: The GDPR in a Datafied Society. Wiley 5G Ref, 1–13. https://doi.org/10.1002/9781119471509.w5gref173.

 Copyright © 5GhOSTS Consortium 2019-2023

consent rules and legitimate interest and grounds for processing personal data. Legitimate interest can be used as a ground for processing personal data in certain cases, but the data controller must perform a 'balancing test'. According to the Opinion on the notion of legitimate interests of the data controller of Article 29 Working Party such test consists of four elements: (a) assessing the controller's legitimate interest, (b) impact on the data subjects, (c) provisional balance and (d) additional safeguards applied by the controller to prevent any undue impact on the data subjects.[154] Data controllers must carry out and document the assessment to prove minimal impact on privacy before any processing of personal data takes place and it has to comply with the requirements of the principle of proportionality.[155] Legitimate interests of data controller must also meet the reasonable expectations of the data subjects.[156] However, the use of legitimate interest as a ground for processing personal data in 5G networks is not unlimited. According to EDPB Guidelines *"[…] location data collected from electronic communication providers may only be processed within the remits of articles 6 and 9 of the ePrivacy Directive. This means that these data can only be transmitted to authorities or other third parties if they have been anonymised by the provider or, for data indicating the geographic position of the terminal equipment of a user, which are not traffic data, with the prior consent of the users*" and "*information, including location data, collected directly from the terminal equipment […] the storing of information on the user's device or gaining access to the information already stored is allowed only if (i) the user has given consent or (ii) the storage and/or access is strictly necessary for the information society service explicitly requested by the user*".[157] The EDPB refers to ePrivacy Directive when discussing consent, but specifically notes that the notion of consent in ePrivacy Directive remain the same as the notion of consent in GDPR. According to Article 5(3) of the ePrivacy Directive "*the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller*".[158] The EDPB also considers that consent and not legitimate interest "*will likely constitute*" the grounds for storing and accessing data already stored on user's equipment and the processing of personal data in its Guidelines in on processing personal data in the context of connected vehicles and mobility related applications.[159] Each data controller in 5G value chain will have to show their own specific legitimate interest and provide full information

[154] Article 29 Working Party 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' 844/14/EN WP 217, 33. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[155] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 338.

[156] Ibid.

[157] EDPB 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', 5. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[158] Article 5(3) ePrivacy Directive.

[159] EDPB 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications', 6. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

on the purposes of processing personal data, explicit mention of legitimate interest in case it is the ground for processing, recipients of personal data, the period for which personal data will be stored, information on the right to erasure and rectification of personal data, and information on transfer of personal data to third parties.[160] Considering the amount of actors and the dynamic nature of 5G architecture the use of legitimate interest will not always be feasible. It is not possible to retroactively rely on legitimate interest as a ground for processing personal data if the data controller incorrectly or unlawfully obtained data subject's consent.[161]

A valid consent is a legal basis for processing of personal data and is mandatory in certain cases. According to Article 7 GDPR *"[t]he data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent*".[162] As was pointed out by Eleni Kosta, "*The role of consent in this era is reduced, as the control of the individual over his personal information is overcome by the facilitation of everyday activities in electronic communications and especially the internet, to the extent that the privacy of the individual is not infringed*".[163] It would be extremely hard to obtain an individual's valid consent for the processing by 5G IoT devices before such processing actually takes place because of the almost simultaneous transfer of substantial amounts of personal data. Extensive information about the devices and wearables of the data subject including sensitive health data such as pulse rate or fitness will be gathered and processed almost instantly without the possibility to obtain valid consent the moment such data subject is within the range of 5G-based IoT systems. According to 'A first assessment based on stakeholder inputs - Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem' by the Body of European Regulators for Electronic Communications (BEREC) there is a risk of inability to obtain a valid consent by multiple data processing actors in 5G value chain since such actors will not have a direct relation to end-users.[164] The dynamic and distributed virtualized architecture of 5G with implemented SDN, NFV, NS and reliance on cloud technologies hinders the exercise of the right to withdraw consent. Another significant challenge is the feasibility of verifying child's consent to data processing. According to Article 8 of GDPR "*Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child*" and "*The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*".[165] There

[160] Ibid, 17.
[161] EDPB 'Guidelines 05/2020 on consent under Regulation 2016/679', 25. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[162] Article 7(3) GDPR.
[163] Kosta, E. (2013). Consent in European Data Protection Law (Nijhoff Studies in European Union Law). Martinus Nijhoff, 399.
[164] BEREC. (2019). A first assessment based on stakeholder inputs - Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem. 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
[165] Article 8 GDPR.

 Copyright © 5GhOSTS Consortium 2019-2023

exists an obligation of the data controller to undertake 'reasonable efforts' to verify whether child's parents or caretakers indeed provided their consent to processing child's personal data.

- **Jurisdiction and cross-border transfer of data –** As was mentioned before, 5G vendors, actors and equipment and services providers may be subject to different laws depending on their country of origin and operation. Another challenge in this regard is the issue of jurisdiction over personal data leaks and the competence of DPAs regarding exercise of users' rights. The distributed and dynamic architecture of 5G networks enables the rapid processing of personal data transferring it to different physical locations in real time through edge computing facilities. The European Commission adopts 'adequacy decisions' which allow the transfer of personal data of EU citizen to non-EU states. Such decisions are adopted on the basis of Article 45 of GDPR which states that "*[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation*".[166] In July 2020 the CJEU invalidated the Privacy Shield Decisions which enabled the transfer of personal data to the US.[167] It caused a considerable effect since many of the largest cloud-services providers are located in the US. Cross-border transfers of personal data inevitably lead to questions of jurisdiction and applicable law. The recent decision by the CJEU in Case C-311/18 ("Schrems II") highlights the importance of proper regulation of the cross-border transfers of personal data and the need for legal certainty. In another judgement of the CJEU in Case C-623/17 ("Privacy International") the CJEU highlighted the importance of the principle of proportionality of EU law when regulating personal data processing, data retention, and forwarding of personal data by ECS providers to intelligence services. 5G technology enables the provision of highly customized network services, which also means that privacy requirements will wary.

- **Supply chain –** Cybersecurity and Infrastructure Security Agency of the United States mentioned a threat posed by manipulation of equipment or intentional insertion of vulnerabilities and malicious software by untrusted 5G equipment manufacturers.[168] The EU is not immune from such risk as well. Back doors, bugs, software and hardware deficiencies and vulnerabilities may be exploited by both state and non-state actors with the intention to undermine security of 5G networks and confidentiality and integrity of communications. Compromised piece of equipment may possess the capability to infect other devices and multiply the negative effect on the security of the network.[169]

[166] Article 45(1) GDPR.
[167] CJEU 16 July 2020, Case C-311/18, ECLI:EU:C:2020:559 ('Facebook Ireland and Schrems case' or 'Schrems II case').
[168] Cybersecurity and Infrastructure Security Agency. (2019). Overview of risks introduced by 5G adoption in the United States. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
[169] Ibid.

 Copyright © 5GhOSTS Consortium 2019-2023

5. Implementing privacy, security and data protection risk mitigating measures in 5G networks

The privacy, security and data protection in virtualized 5G networks largely depends on actors operating in 5G value chain. Their decisions, management practices, procedures applied will have a decisive impact on the functioning of 5G networks.[170] Since some of the security and privacy requirements issued by 3GPP are not applied by default or are optional, the overall effectiveness of security depends on to what extent the operators of 5G networks will enforce these standards.[171] Anonymization, pseudonymization and implementation of data protection by design contribute to the GDPR-compliant security and privacy in 5G networks.[172] The personal data processed via 5G networks may prove to have a high commercial value. The new cloud, edge computing, virtualization and software-reliant generation of mobile networks is vulnerable to software bugs, data leaks, lack of coordination between different parties involved in the processing of personal data, and cyber attacks.

Implementation of effective privacy preserving technologies, data protection measures and security standards is not just a requirement of law but a necessity enabling the operation of 5G network as a whole. As was noted by S. Rizou, E. Alexandropoulou-Egyptiadou and K. E. Psannis "*[t]he 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*".[173] Adherence to GDPR requirements namely to principles relating to processing personal data, principle of data protection by design and by default is crucial for ensuring the privacy and data protection. Users must be able to easily obtain full and clear information on the processing of personal data, the data controllers, purposes of the processing, profiling and automated decision-making, and the ways to exercise their rights to rectification and erasure of data. Considering the use of edge computing and cloud services and the option of distributed processing of personal data in 5G networks, traceability mechanisms have to be implemented, which may prove to be a substantial challenge.[174] The fact that 5G contributes to the generation of an immense amount of personal data highlights the importance of effective data minimisation measures.

There is no exhaustive list of actions or privacy-preserving technologies necessary to achieve compliance with legal requirements. The privacy-disruptive novelties introduced by 5G networks require the development of new and efficient privacy enhancing and privacy preserving technologies to cope with the growing among of data and interoperability issues.[175] Researchers have proposed a number of technical

[170] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 11. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[171] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, 8, 108052–108061. https://doi.org/10.1109/access.2020.3000662.
[172] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, 8, 108052–108061. https://doi.org/10.1109/access.2020.3000662.
[173] Ibid.
[174] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 11. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[175] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF)

 Copyright © 5GhOSTS Consortium 2019-2023

and organizational measures as well as privacy risk mitigation techniques to enhance privacy, protection of data and security in 5G networks.

It has been noted that existing trust models may not be fully suitable for 5G networks, and the development of new models is required, which consider the presence of many novel actors and vendors providing various services in 5G.[176] Some of the network actors may use external cloud services and it is important to prevent unlawful cross-border transfer of data. Identity management in 5G would also change due to reliance on many small IoT devices that are not capable of bearing a standard identity module.[177] Identity management is important to protect the security of the network as well as personal data stored on the devices themselves. Compliance with principles of lawfulness, fairness and transparency will ensure that users' data is not processed and is not transferred to third parties without the user's informed consent. Researchers note the potential conflict between privacy and computing trust.[178]

Privacy protection models require substantial computing resources and demanding cryptographic operations not always possible or feasible in 5G networks.[179] It has been noted that there is an ongoing academic debate on what cryptographic algorithms are best suited for use in 5G networks since limited resources and aimed performance of 5G networks must be considered.[180] The guaranteed encryption of end-to-end communications in 5G networks and the continuous improvement of encryption models, especially when using edge computing, has been mentioned by AEPD.[181]

Researchers suggested categorization of regulatory approaches to achieving privacy objectives in 5G networks identifying the following types[182]:

- **Government regulation –** legislation developed by national, supranational (EU) and international (Council of Europe, United Nations) governmental bodies;

[176] Kumar, T., Liyanage, M., Ahmad, I., Braeken, A., & Ylianttila, M. (2018). User Privacy, Identity and Trust in 5G. A Comprehensive Guide to 5G Security, 267–279. https://doi.org/10.1002/9781119293071.ch12.
[177] Ibid, 277.
[178] Kumar, T., Liyanage, M., Ahmad, I., Braeken, A., & Ylianttila, M. (2018). User Privacy, Identity and Trust in 5G. A Comprehensive Guide to 5G Security, 267–279. https://doi.org/10.1002/9781119293071.ch12.
[179] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF)
[180] "*Summarizing, the literature is still divergent if adopting more traditional cryptographic algorithms, such as AES, RSA, PKI, or if moving towards more recent methods, such as ECC or Quantum Cryptography, or solutions based on blockchain. Probably, the well-suited approaches for 5G are those able to support the resources' constraints of end-devices as long as guaranteeing the robustness of the system and, at the same time, preserving the performance of the 5G network*" via Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G In the internet of things era: An overview on security and privacy challenges. Computer Networks, 179, 107345. https://doi.org/10.1016/j.comnet.2020.107345.
[181] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 11. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[182] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF).

 Copyright © 5GhOSTS Consortium 2019-2023

- **Industry self-regulation** – standards and regulations adopted by industry-specific standardization bodies such as 3GPP, NGMN (Next Generation Mobile Networks), and ETSI (European Telecommunications Standards Institute);

- **Market regulation** – many users are concerned about their privacy while using mobile networks. The consumer opinion is crucial and may influence the adoption of privacy, data protection and security policies and mechanisms in 5G.

SDN in itself contributes to disruption of privacy in 5G due to its dynamic and flexible nature. SDN allows the dynamic re-routing of user traffic to different data centers, and together with NFV it will enable the dynamic provisioning of new data processing functions, i.e., the network and its data processing facilities are not fixed once data is sent from the mobile device. In particular, privacy compliance cannot be certified once and for all, instead, the container orchestration process and network settings have to guarantee compliance with privacy, data protection, and security requirements. However, SDN can also be used to design privacy-aware mechanisms.[183] SDN service providers may define privacy-preserving data flow rules to ensure that data packets are routed exclusively within EU borders.[184] With regard to the Vehicle to Infrastructure use case, a technical privacy preserving authentication scheme was suggested to take advantage of SDN technology in 5G. Researchers claim that such a scheme may contribute to privacy without decreasing performance even in high vehicle density scenarios.[185] An improved privacy-preserving approach for enhancing security in Vehicle to Infrastructure use case utilizing edge computing is claimed to contribute to the network's confidentiality, integrity, and privacy elements.[186] The use of the 'hybrid cloud approach' may help to store critical data and special categories of data on the in-housed cloud while less sensitive data is processed in the public cloud.[187] Such an approach may lower the severity of data leaks and data breaches, but it doesn't mean that the protection of some data can be waivered in favor of other data.

The privacy and security risks may be mitigated by the adoption of business, management, and operational measures. Such measures include the fostering of development of services and equipment from trusted manufacturers, promoting open, transparent, and consensus-driven international telecommunications standards, limiting the use of 5G equipment with known vulnerabilities, public-private cooperation

[183] Ibid.

[184] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF).

[185] Huang, J., Qian, Y., & Hu, R. Q. (2020). Secure and Efficient Privacy-Preserving Authentication Scheme for 5G Software Defined Vehicular Networks. IEEE Transactions on Vehicular Technology, 69(8), 8542–8554. https://doi.org/10.1109/tvt.2020.2996574.

[186] Rasheed, I., Zhang, L., & Hu, F. (2020). A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing. Computer Networks, 176, 107283. https://doi.org/10.1016/j.comnet.2020.107283

[187] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G Privacy: Scenarios and Solutions. 2018 IEEE 5G World Forum (5GWF).

 Copyright © 5GhOSTS Consortium 2019-2023

regarding countering security and privacy vulnerabilities, and continuous robust assessment and evaluation of the efficiency of applied measures.[188]

Encryption is a technical measure contributing to overall security of processing personal data and is a major element of privacy requirements for 5G networks as a risk mitigation measure.[189] Encryption is listed alongside anonymization of data as an appropriate safeguard while processing personal data on the grounds other than user's consent, which is particularly relevant for 5G networks.[190] Article 32 GDPR requires to implement technical and security measures to ensure the secure processing of personal data *"[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing"* explicitly mentioning encryption and pseudonymization as possible tools.[191] Implementation of encryption also relieves data controllers of the obligation to notify users affected by the data breach.[192] The EDPB requires data controllers to use effective encrypting mechanisms in case of transferring data to third countries for storage or backup purposes or in case of transit of data.[193] The encryption key must be kept separate from the personal data it may re-identify or decrypt.[194] CNIL provides the following recommendations regarding the implementation of encryption mechanisms for processing personal data[195]:

- Use of recognized and secure algorithms (e.g. SHA-256, SHA-512, SHA-3, AES etc.) and refraining from using obsolete algorithms (e.g. DES, 3DES and hash functions SHA1 and MD5);
- Use of appropriate key sizes for hash functions;
- Ensure the protection of secret keys;
- Create a procedure on managing secret keys and actions in case of a loss of the secret keys;
- Use software and cryptographic libraries audited and/or certified by third parties with proper expertise;
- Use of VeraCrypt software for encrypted containers, which is especially relevant for container orchestration involving personal data in 5G networks;
- Checking the validity, consistency, and certification chain of received certificates.

[188] Cybersecurity and Infrastructure Security Agency. (2019). Overview of risks introduced by 5G adoption in the United States. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
[189] Recital 83 GDPR.
[190] Article 6(4)(e) GDPR.
[191] Article 32(1)(a) GDPR.
[192] Article 34(3)(a) GDPR.
[193] EDPB 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', 22-24. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
[194] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 135.
[195] CNIL. (2018). Security of personal data. https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.

 Copyright © 5GhOSTS Consortium 2019-2023

Encryption also contributes toward the implementation of the principle of data protection by design.[196] While non-personal data is out of the scope of GDPR and there is no legal obligation to encrypt it, some non-personal data may also constitute attribute data and contribute to the re-identification of the data subject if paired with other sets of data. It is essential to consider attribute data in V2I and SO use cases, since large sets of M2M data or information gathered by IoT sensors can in many cases be linked with other data and lead to identification of data subjects.[197]

Data Protection Impact Assessment (DPIA) is an important instrument and requirement devised in the GDPR. According to Article 35(1) of GDPR, "*[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*" (DPIA).[198] Recital 84 provides additional information on DPIA: "*In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing*".[199] Data controllers in 5G value chain will most likely be obliged to perform a DPIA since a number criterions required for such assessment are present in 5G networks:

- New technologies – 5G networks introduce a whole plethora of new privacy-disrupting technologies;

- Nature and scope – 5G networks will be ubiquitous and rely on a large number of sensors and IoT devices continuously gathering data;

- High risk – a list of potential risks to privacy, security and data protection was provided in section 4 of this deliverable.

[196] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 578.
[197] Spindler, G., & Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation. Journal of Intellectual Property, Information Technology and E-Commerce Law, 168. https://www.jipitec.eu/issues/jipitec-7-2-2016/4440.
[198] Article 35(1) GDPR.
[199] Recital 84 GDPR.

 Copyright © 5GhOSTS Consortium 2019-2023

Data controllers perform DPA based on the advice of their Data Protection Officer.[200] It is possible that in some cases providers of services in 5G networks will have to request an opinion of the respective Data Protection Authority.[201]

It is possible to use privacy threat modelling methodologies to conduct a systematic and extensive assessment of a software system's design as a step towards compliance with the principle of data protection by design and by default such as LINDDUN methodology.[202]

[200] Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, 672.
[201] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 11. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[202] Wuyts, K., Sion, L., Joosen, W. (2020). LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling, International Workshop on Privacy Engineering 2020, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

 Copyright © 5GhOSTS Consortium 2019-2023

6. Conclusion

This deliverable provided an overview of the state of the art of privacy-disrupting technologies introduced in 5G networks, listed and analyzed the challenges to privacy, data protection, and security posed by these novel technologies, and outlined the applicable EU legislation.

5G networks highlight the importance of the development of authorized and regulated certification mechanisms envisaged by GDPR. The success of 5G networks depends on its ability to guarantee security, privacy and protection of personal data.[203]

While there is a need to balance compliance with legislative provisions and over-protection of the network, it is essential to apply rigorous assessment of any privacy-preserving technologies and techniques to ensure the protection of users' rights. The GDPR was designed as a risk-based future-proof legislation to tackle not-yet-known threats to privacy and data protection. 5G however, poses a substantial privacy-disruption threat if not implemented in the correct way, namely by applying the principle of data protection by design and by default in all steps, including research, standardization, development, deployment and operations of the 5G network." Some researchers argue that GDPR may prove inadequate to address the threats to privacy and users' right posed by the Internet of Everything and an 'always connected' society led by the commercialization of personal data.[204] The deployment of 5G infrastructure will likely require a re-assessment of trust relationships within the network, which then leads to the development of new, comprehensive, and use-case-sensitive trust models which would be the technical basis for DPIA. While the latter issue is beyond the scope of this deliverable, the 5GhOSTS project will focus on relevant trust and threat models in deliverable D1.3.

[203] Agencia Española de Protección de Datos. (2020, May). Introduction to 5G technologies and their risks in terms of privacy, 11. https://www.aepd.es/sites/default/files/2020-06/nota-tecnica-privacidad-5G-en.pdf.
[204] Teatini, S., & Matinmikko-Blue, M. (2020). Privacy in the 5G World: The GDPR in a Datafied Society. Wiley 5G Ref, 10. https://doi.org/10.1002/9781119471509.w5gref173.

 Copyright © 5GhOSTS Consortium 2019-2023