PRIViLEDGE WORKSHOP REPORT

"Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions"
15. October 2020

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

Workshop Summary

This report provides a short summary of the recent workshop "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions" hosted by H2020 project PRIViLEDGE. The workshop took place on the October 15th, 2020 at 11:00-13:00 CEST and was held virtually via Zoom Webinar tool.

This event brought together the R&D, industry and policy stakeholders that are involved in developing and advancing blockchain and DLT technologies, with the aim of facilitating cooperation through explaining the different research advances, policy initiatives and by discussing on how to build mutually beneficial collaboration paths. This workshop was attended by 54 people from 15 different countries.

The workshop was organized in accordance with the PRIViLEDGE communication and dissemination plan and was delivered as planned - exploiting the technological advancements and generated knowledge of PRIViLEDGE to engage stakeholders from policy and industry into data security and privacy related issues. The workshop was announced through PRIViLEDGE website and social media channels and related information was disseminated by all project partners, workshop presenters, their institutions and extended internal and external networks.

This report has been prepared for circulation to participants but is also intended as a resource for those interested in the workshop content but who were unable to attend.

Workshop website: https://priviledge-project.eu/events/priviledge-virtual-workshop

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

Workshop Objectives and Programme

Background

From contact tracing apps to economic forecasting, 2020 has seen a range of innovative new uses for data – and also re-ignited long-standing debates on data sharing, data protection, privacy and public interest. Concurrently, in the recent years, the European Union has put a strong emphasis on data privacy and security issues and related BC and DLT solutions, through supporting many strategic initiatives and funding (since 2017) over 40 DLT-related research and innovation projects from H2020 programme.

As of now, many research activities and strategic initiatives on blockchain and DLT are maturing. For example, the European Blockchain Partnership was signed in 2018 by all EU Member States and members of the European Economic Area to work together towards realising the potential of blockchain-based services for the benefit of citizens, society and economy. Additionally, the European Commission has supported public-private cooperation. In April 2019, the International Association for Trusted Blockchain Applications (INATBA) was launched.

As the first EU-funded research projects and the political initiatives are maturing, and as many initiatives are being undertaken in parallel, project PRIViLEDGE took on the challenge and opportunity to unite the different parties (policymakers, industry and R&D representatives) within a 2-hour virtual workshop and facilitate exchange of ideas through exploring the current data sharing "climate" and explaining the different research advances and policy initiatives.

The primary goal of the "Data Sharing and Privacy – What Has Changed in the Era of COVID? A Deep Dive into Policy Dilemmas and New Technological Solutions" workshop was designed to facilitate discussions between R&D community, industry and policy stakeholders, in order to:

- explore how political and policy priorities around data and privacy have evolved since the beginning of 2020.
- present insights and new techniques for data security and privacy from Horizon 2020 projects.
- reflect on how the European Union's strategies for data and blockchain will support further innovation in coming years.

Programme (Annex 1)

The workshop was built up in two sections. The first part focused on setting the scene with key-note panellists speaking about data sharing and privacy from governmental, public and industry perspectives. The key-note messages were delivered by prof. Dimosthenis Anagnostopoulos (Secretary General of Information Systems of Public Sector of the Greek Ministry of Digital Governance), Paul-Olivier Dehaye (Board Member of the MyData movement) and Jade Nester (Director of Consumer Policy at GSMA).

The second section of the workshop explored novel data sharing and security avenues emerging from R&D results from four H2020 projects focused on enhancing DLT, blockchain or alternative solutions: PRIViLEDGE project (represented by Toon Segers), CUREX project, (represented by prof. Christos Xenakis), FENTECT project (represented by Francisco Gala) and CHARIOT project (represented by Konstantinos Loupos).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

Additionally, the European Commission (represented by Helen Köpman) reflected on how the European Union's strategies for data and blockchain will support further innovation in coming years.

The workshop was moderated by prof. Ivan Visconti (University of Salerno) and dr. Ain Aaviksoo (Guardtime OÜ).

***

Main messages from keynote speakers

Speaker: Prof. Dimosthenis Anagnostopoulos (Secretary General of Information Systems of Public Sector of the Ministry of Digital Governance, Greece)

Things done at the Greek Ministry of Digital Governance to mitigate COVID:

- Gov.gr portal for the citizens is offering more than 700 electronic services.
- Numerous applications of governmental services that helped the citizens to stay at home and get access to the services remotely that have more than a million visits.
- Launching new live environment for taxation for municipality offices based on Microsoft Teams that allows the officers to arrange for virtual meetings with public bodies and serve citizens virtually.

The Secretariat promotes interoperability i.e., electronic exchange of data between public bodies. Early 2020, more than 7 million interoperability calls were made through the Secretariat's Interoperability Centre. Prof. Anagnostopoulos brought out the central governments' cloud system (GCloud) meant for the whole administration system of Greece. Currently the Greek governmental cloud system is the biggest one in South-East Europe. By 2022 all central information of public bodies will reside in GCloud improving data security supported by the central management of multiple and comprehensive maintenance and providing advanced security policies. Prof. Anagnostopoulos noted that, in the near future, Greece will need two separate GClouds for health and education. These processes are largely enabled by the change enforced in the near future where Greek citizens will receive one unique personal identification number applicable throughout all information systems (whereas now they might have several).

Prof. Anagnostopoulos emphasised the further need to investigate DLT/blockchain applications in operational use of digital governance, like for example it is done in Estonia. Greece intends to expand blockchain capabilities in many spheres. So far steps have been made in the areas of:

- traceability of tobacco products,
- traceability and integrity of invoicing systems,
- identification and administration of public property registries.

Last but not least, Prof. Anagnostopoulos noted that the legislation and regulations must develop in correlation with the new technological advancements and solutions in DLT and blockchain.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

Speaker: Paul-Olivier Dehaye (Founder, PersonalData.io; Board Member, MyData Global)

In his key-note speech Dehaye focused on COVID-19 and the related the digital solutionism. He highlighted that the pandemic itself was layered with another pandemical wave on top of it - doing Bluetooth-based contact tracing.

Inherently, there is a clear conflict embedded into contact tracing (CT) where information is communicated between different actors and information about others is revealed, which makes privacy risks inescapable. This pushed security researchers to come up with systems and protocols that would have been unthinkable pre-pandemic. The main approach: announce continuously through a smartphone some short-lived identifiers so that in case of a positive test for the virus whoever received those signals can evaluate a risk score. Dehaye explained that this sort of system is very insecure and that security researchers would have never considered deploying it months before COVID-19 hit. This marker is important to notice because it illustrates the dynamics between individual privacy and larger public interest.

Hindrance for CT platform/app adoption:

- Current contract tracing solutions offer "after the fact" notification and no useful additional features for the citizens.
- Limitations by Google and Apple (most CT apps are built on them) justified by privacy concerns with respect to governments potentially interested in mass surveillance programs.
- Smart phones are wrong platforms to do peer to peer contact tracing because they are derived by capitalistic/business interests.

Overdispersion is one of the defining features of COVID-19, meaning that the best predictor of (getting infected with COVID) risk is not anchored in an individual but it is anchored in an exposure event. We should be looking for dispersion events. This would mean that the current trend of deploying perspective tracing (index case and looking for what it has affected) would need to switch to venue centric tracing of infections (finding out where the infected person got infected, in order to find much more infected people). Tracing becomes simpler because you will trace an individual in relation to a place or event rather than in relation to another individual. This also eases the privacy issue complexity.

Main changes that COVID has brought into discussions around privacy:

- The issue of personal data is clearly seen as public interest.
- Governments now understand the unexpectable power of Google and Apple in this ecosystem.

In conclusion, Deyahe stated that a lot of the data we need already exists and we should push for the opportunity where GDPR enables us to get to that data through the portability requirements to serve the public interest.

Jade Nester (Director of Consumer Policy, GSMA)

In her keynote speech Nester focused on GSMA's AI for Impact initiative and big data for COVID-19 response.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

- GSMA's mobile big data project "AI for Impact" defines the technical, commercial and ecosystem requirements to deliver viable data-driven products and services that adhere to principles of privacy and ethics. This is done in the space of aggregated anonymized location mobile data.

- Privacy preservation and accountability are very important for GSMA and key elements of "AI for Impact" and have established a code of conduct designed to ensure all their activities adhere to the privacy and security standards. Additionally, GSMA is very supportive of the EU's GDPR. Nevertheless, Nester noted that for mobile operators the "Privacy Directive" is even more restrictive when it comes to privacy issues.

- In connection to COVID research, Nester highlighted a recent development where 14 mobile operators worked with European Commission's research centre and e.g., they came to a high-level conclusion that mobility alone can explain the initial spread of the COVID virus in Italy, France and Spain. This helped other countries (like Norway) to be prepared, looking into mobility before the first COVID case hit them, and predict the scale of hospitalizations, for example.

- GSMA has specific COVID-response privacy guidelines that put trust into the centre while working with mobile data sets. The guidelines are available on GSMA webpage.

- Last but not least, Nester highlighted that the biggest obstacle is the governments' capacity on some markets to know how to use mobile big data effectively. Thus, GSMA has developed a capacity building course to help the governments out.

***

Main advances made in H2020 project to address data privacy and security concerns

Speaker: Toon Segers (H2020 project PRIViLEDGE, Researcher)

According to Toon Segers' presentation "Privacy advances in DLT by PRIViLEDGE partners", PRIViLEDGE project has made significant privacy improvements in transaction, computation and storage techniques for DLTs.

Segers highlighted the following advancements from PRIViLEDGE project:

- In the area of private transactions, a notable achievement is the publication of the privacy-preserving Proof-of-Stake based ledger*, Ouroboros Crypsinous*.

  Segers explained that typically the transaction ledger is a public resource and thus information about the way the transaction issuers operate may be leaked to an adversary, but *Crypsinous* ensures privacy for transaction issuers, ensuring that the proof of stake leadership election can run with a provably secure, privacy-preserving transaction scheme.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

- In the area of private computation, notable progress has been made in zero knowledge proof systems (*zk-SNARKs)*.

  SNARKs are what have accelerated privacy advances in DLTs. The succinctness and efficiency of verification are what make zk-SNARKs popular. They don't require a lot of resources for the verifier, while they offer a very powerful functionality. PRIViLEDGE makes a particularly efficient recent SNARK construction, by Groth et al., available to the Hawk blockchain project by proving it in the formal UC security model.

- In the area of storage, Segers discussed an improvement in bulletin board security that is particularly relevant for verifiable e-voting systems.

- Furthermore, another key contribution by the PRIViLEDGE team, together with colleagues from the Electric Coin Company and University College London is the Sonic zk-SNARK: A new zk-SNARK for general arithmetic circuit satisfiability. Sonic requires a trusted setup, but unlike conventional SNARKs the structured reference string supports all circuits (up to a given size) and is also updatable, so that it can be continually strengthened.

- PRIViLEDGE team introduces the first cryptographic security definition for e-voting bulletin boards capturing 'liveness' and 'persistence'. The main idea is that malicious peers are forced to either reveal themselves in which case they can be ignored, or to behave benignly.

Speaker: Prof. Christos Xenakis (H2020 project CUREX, Coordinator)

In his presentation "Electronic Health Data Exchange considering Security & Privacy" prof. Xenaxis emphasized the need to reinforcing the security level of healthcare infrastructures and pointed to some key healthcare challenges and threats to data privacy, while offering responses from CUREX Consortium. These are as follows:

- Healthcare challenge no 1. Data exchange introduces new types of threats.

  CUREX responds to this with (a) Asset Discovery Tool (ADT) & Vulnerability Discovery Manager (VDM), these bind the system and resources that discovered in the domain with possible vulnerabilities; (b) Threat Intelligence Engine (TIE) & Knowledge Extraction Analytics (KEA) - binds the discovered vulnerabilities with potential known threats. May identify new and unknown threats by detecting abnormal behaviours; (c) Cybersecurity Assessment Tool (CAT) & Optimal Safeguards Tool (OST) - based on the cybersecurity risk assessment results, optimal safeguards are proposed to the decision makers towards enhancing the cyber strategy of the healthcare organization.

- Healthcare challenge no 2. Privacy violations are more likely to occur when exchanging data.

  CUREX responds to this challenge with (a) Privacy Assessment Tool (PAT) - assesses the degree of compliance of the healthcare organization with the GDPR, by providing an indicative privacy score. (b) Health Professional & Patient Applications (HPA & PA) - handles the transactions between the CUREX Private Blockchain and the hospitals that wish to exchange medical records, respecting GDPR rules and enabling consent management; (c) Private Blockchain (PrB) - using smart contracts to comply with the GDPR and record the risk assessment reports in the network.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

- Healthcare challenge no 3. The lack of a collectively accepted and auditable exchange record leads to reduced trust between parties.

  To this concern CUREX offers its Private Blockchain (PrB) that acts as a distributed database, where the scores of the CAT and the PAT tools will be recorded, which also facilitates the traceability and auditability of the data.
- Healthcare challenge no 4. The lack of human-centric strategies and methodologies for raising cybersecurity and privacy awareness in a healthcare institution.

  CUREX offers Cyber Hygiene (CH) as a survey tool that engages different healthcare employee groups, addressing them a series of targeted questions to extract knowledge and understand the group-specific gaps and needs with regards to raising cybersecurity and data privacy awareness.

Speaker: Francisco Javier González Gala (H2020 project FENTECT, Coordinator)

Gala presented FENTEC's approach developing new Functional Encryption (FE) - an efficient alternative to the all-or-nothing approach of traditional encryption. In his presentation "FENTEC: Increasing Trustworthiness of ICT solutions with Functional Encryption" he highlighted that FE helps to create the balance between privacy and information that needs to be shared.

Essential FE enables partial views over encrypted data and effectively enhances security of complex systems by compartmentalization of data or computation over data. FENTEC's three use cases, which depict real problems, are vehicles to produce tangible advantages for the whole ICT industry and for stakeholders that need to operate in environments where data confidentiality and privacy is needed, but partial access to the data through external parties is unavoidable.

The security, efficiency, expressiveness and versatility of the new FE approach was showcased by Gala within presenting the project's three use-cases:

- Privacy-preserving digital currency, enforcing flexible auditing models: providing customer privacy and tools to audit the payment system itself.
- Privacy-Preserving Statistical Analysis: enabling Wallix clients to be able to perform analytics about their clients' data while providing guarantees as to the privacy of those data.
- Data Collection and Local Decision Making: detecting motion at the gateway level on an encrypted video stream coming from security cameras.

Speaker: Konstantinos Loupos (H2020 project CHARIOT, Coordinator)

In his presentation "Blockchain as an enabler in the CHARIOT Integrated approach to Industrial IoT Safety, Privacy and Security" Loupos emphasized that CHARIOT provides a design method and cognitive computing platform supporting a unified approach towards Privacy, Security and Safety of IoT Systems.
In relation to blockchain CHARIOT offers:

- Combined authentication solution of blockchain with PKI - a privacy and security protection method building on state-of-the-art Public Key Infrastructure (PKI) technologies to enable the coupling of a pre-programmed private key deployed to IoT devices with a corresponding private key on a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

blockchain system. This includes the implementation of security services utilising a cryptography-based approach and IoT security profiles all integrated to the CHARIOT platform.
- Blockchain aided encryption between all IoT network endpoints. Fog-based decentralised infrastructures for Firmware Security integrity checking leveraging blockchain ledgers to enhance physical, operational and functional security of IoT systems, including actuation and deactivation.
- Mobile application for sensor provisioning in the IoT network utilizing four-eye principle.
- Blockchain-based state management for sensors.
- CHARIOT sensors (WIFI and BLE) with high processing capabilities that support encryption and blockchain.

Industrial IoT gateways operate a real time operating system in comparison to the traditional operating systems. Thus, CHARIOT has chosen the ARTIK device integrated into the getaway. And in this approach CHARIOT has created:

- Blockchain Keypair: A tool for generating the appropriate CHARIOT compliant keypairs for interacting with the CHARIOT blockchain
- Blockchain Keypair API: A RESTful API for generating the appropriate CHARIOT compliant keypairs for interacting with the CHARIOT blockchain
- Blockchain Deployment: Deployment scripts for properly initiating all services of the CHARIOT system, including the blockchain component
- Distributed PKI Smart Contracts: Smart contracts implementing the logic of a non-authoritarian PKI system using state-of-the-art cryptography, nonce-based systems & a pseudo-language for assessing instructions
- ARM-based Blockchain Runtime: A blockchain compilation of the Hyperledger Fabric suited for the ARMv8, or aarch64, architecture which hadn't been conducted in the past
- Blockchain Service: A RESTful API for interacting with the blockchain instance and generally handling all operations of the underlying smart contract

Speaker: Helen Köpman (European Commission, Deputy Head of Unit for Digital Innovation & Blockchain)

Köpman stated in her presentation "Reflections on the EU Data Strategy and Policy and Funding Priorities for Blockchain and DLT" that the new EU strategy for blockchain builds upon the three main EU priorities:

- sustainability - support for the blockchain to be sustainable and for the blockchain to create more sustainability in the economy at large, e.g. the Green Deal where one uses blockchain to roll out solutions to push for digital transformation.
- scalability - to be useful for Europe's industry blockchain technology has to be low latency and interpretable to achieve the scale and scope needed.
- privacy - since blockchain includes immutability of data and records which is important in creating trust; EC encourages technical solutions that are reconcilable with immutability concept and compatible with GDPR. Köpman noted that the projects presented at the workshop are already advancing in this area, so there are solutions emerging that are able to tackle this.
- cyber-resilience - blockchain needs to be resilient to hacking and tampering, EC wants European industry to benefit from the safest solutions to be compete world-wide.

Köpman emphasized the importance of public and private cooperation, highlighting the following initiatives:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

- Cooperation through a European Blockchain Partnership harnessing national blockchain efforts into a pan-European approach.
- The European Union Blockchain Observatory and Forum that accelerates blockchain innovation and the development of the blockchain ecosystem within the EU.
- International Association of Trusted Blockchain Applications (INATBA) - global blockchain organization from members of industry with the mission to build global governance and interoperability frameworks across different blockchain producers and users. EC would like to see this association to federate the work in standardization and put that forward to international standardization bodies.

Finally, Köpman presented a number of new policy initiatives that will help to tackle the challenges in the area of blockchain:

- European Blockchain Services Infrastructure (EBSI) - during the budgetary period in the EU, the Commission would like to launch a new innovation procurement for European Blockchain Services Infrastructure. In combinations start-ups, SMEs and larger companies can bid for solutions that could roll out those services.
- One of the initiatives is also the establishment of a regulatory sandbox. Here, especially smaller players (SMEs and start-ups) that have solutions and applications that could be deployed, will be brought together with local regulators to discuss what potential the solutions have in real life. The aim is to help the SMEs and start-ups to roll out these applications in a compliant way.
- Additionally, EC is determined to support more research, especially subjects related to decentralized data usage, data privacy enhancements, data portability issues.
- There's a 600-million-euro fund for supporting start-ups in the area of Artificial Intelligence and blockchain. EC is looking for increasing this fund.
- Emerging new regulatory framework for digital assets - proposed regulation covers not only entities issuing crypto-assets but also firms providing services around these crypto-assets such as and firms operating digital wallets, as well as cryptocurrency exchanges.
- Boost support in skills in the blockchain area - skilled experts are needed in order to transform the blockchain solutions that are emerging.

***

Conclusions

The workshop helped to assess the privacy and security advancements within several mature H2020 projects that utilize blockchain, DLT or FE mechanisms along with advanced cryptographic tools. It brought into the light several nuances and caps in EU data sharing environment from technical and practical standpoints, but also offered many innovative solutions.

The workshop re-confirmed that research, industry and policy communities need to cooperate and communicate with each other even more closely in order to tackle the present and future challenges of big data, data sharing and security. There is significant overlap in interests between these communities and the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

many current and upcoming EC initiatives promise to boost and support the collaboration between these stakeholders to create sustainable solutions for data sharing and privacy.

Annexes

Annex 1. Workshop Programme

AGENDA

11:00 - 11:05

OPENING WORDS AND INTRODUCTION

Prof. Ivan Visconti
Scientific coordinator at University of Salerno, PRIViLEDGE

11:05 – 11:35

KEY-NOTE PANEL: PRIVACY & SECURITY ISSUES IN DATA SHARING AND BIG DATA USAGE

- **Prof. Dimosthenis Anagnostopoulos**, Secretary General of Information Systems of Public Sector of the Ministry of Digital Governance, Greece.
- **Paul-Olivier Dehaye,** Founder, PersonalData.io; Board Member, MyData Global
- **Jade Nester**, Director of Consumer Policy, GSMA.

In conversation with **Ain Aaviksoo**, Chief Medical Officer, Guardtime. Former Chief Digital and Innovation Officer for Health, Estonia.

11:35 - 12:50

NEW INNOVATIONS: CUTTING-EDGE INSIGHTS ON PRIVACY AND DATA SHARING FROM EU-FUNDED RESEARCH

- "**Privacy advances in DLT by PRIViLEDGE partners**"
  A.J.M. (Toon) Segers,
  PRIViLEDGE Researcher (Eindhoven University of Technology, NL)

- "**Electronic Health Data Exchange considering Security & Privacy**"
  Prof. Christos Xenakis,
  CUREX Coordinator (University of Piraeus, GR)

- "**FENTEC: Increasing Trustworthiness of ICT solutions with Functional Encryption**"
  Francisco Javier González Gala,
  FENTEC Project Director (ATOS, ES)

- "**Blockchain as an enabler in the CHARIOT Integrated approach to Industrial IoT Safety, Privacy and Security**"
  Konstantinos Loupos,
  CHARIOT Coordinator (INLECOM, GR)

- "**Reflections on the EU Data Strategy and Policy and Funding Priorities for Blockchain and DLT**"
  Helen Köpman,
  Head of Unit of Digital Innovation and Blockchain, European Commission (Belgium).

12:50-13:00

CONCLUSION

Prof. Ivan Visconti, Scientific coordinator at University of Salerno, PRIViLEDGE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

Annex 2. Biographies of Presenters

Speakers:

- **Prof. Dimosthenis Anagnostopoulos** is a Professor in the Department of Informatics and Telematics in the area of Information Systems and Simulation. From August 2019, he serves as Secretary General of Information Systems of Public Sector of the Ministry of Digital Governance. He served as the National Representative of Greece for ICT in Horizon 2020 (2014-2015). He has also served as Secretary General of Information Systems of the Greek Ministry of Finance and Economics (2004 - 2009). His research interests include eGovernment, Information Systems, Semantic Web and Web Services, Modelling and Simulation Methodologies and Applications (networks, transportation systems) and Business Process Modelling.

- **Paul-Olivier Dehaye** is the Director of PersonalData.IO, a non-profit focused on making data rights individually actionable and collectively useful. He has contributed to the uncovering of the Cambridge Analytica scandal. He is on the Board of Directors of MyData Global and co-founder of MyData Geneva.

- **Jade Nester** is Director, Consumer Policy, at the GSMA, a trade association representing the interests of mobile network operators worldwide. Jade has 14 years of experience working on technology policy issues. Prior to joining the GSMA, she was at Promontory Financial Group, an IBM company, where she advised clients on compliance with privacy and data protection frameworks. Between 2006 and 2014, she worked for the U.S. government, including as Senior Advisor for Internet Policy at NTIA in the Commerce Department and Director, Internet Public Policy at the State Department.

- **Toon Segers** is a PhD researcher in applied cryptography at TU Eindhoven, focusing on Secure Multi-Party Computation (MPC). Toon is head of product of Roseman Labs, a high-tech software company that delivers privacy solutions based on MPC. Prior, Toon was Partner at Deloitte, responsible for its Cyber Risk and Blockchain practices in The Netherlands. Toon worked 10 years at BCG, holds an MBA from Columbia and an MSc from TU Eindhoven in Applied Mathematics.

- **Prof. Christos Xenakis** is a faculty member of the Department of Digital Systems of the University of Piraeus. He has participated in numerous projects realized in the context of EU Programs (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie, Horizon2020) as well as National Programs (Greek).

- **Francisco J. G. Gala** works for Atos Research and Innovation (ARI) as Head of the Secure Societies and Societal Transformation Unit. He holds a master's degree in environmental sciences and an MBA. He has 17-year multidisciplinary experience in the UK and Spain, having worked in different key sectors such as ICT, engineering, environmental protection and utilities.

- **Konstantinos Loupos,** Head of R&D Program, holds an MBA (Hellenic Open University, GR), M.Sc. in Microelectronics Systems Design (University of Southampton, UK) with distinction and M.Eng. in Electronic and Electrical Engineering (University of Manchester, UK). He has extensive experience in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.

embedded systems and sensors and microelectronics systems, security systems, IoT technologies and Cybersecurity.

- **Helen Köpman** is Deputy Head of Unit for Digital Innovation & Blockchain, at DG Communications Networks, Content and Technology at the European Commission in Brussels. The unit elaborates EU policy initiatives to support digital innovation, blockchain and growth of startups and include Startup Europe, ICT standardisation and innovation procurement. The unit leads along with DG FISMA, the European Commission Task Force on Financial Technology.

Moderators:

- **Prof. Ivan Visconti** is a professor of computer science at the Computer and Electrical Engineering and Applied Mathematics Department of the University of Salerno. His research focuses on advanced cryptographic notions and tools and their applications to Blockchain Technology.

- **Ain Aaviksoo** is Chief Medical Officer at Guardtime. As the former Deputy Secretary General for E-services and Innovation at the Estonia Ministry of Social Affairs he oversaw the digital transformation and innovation of social security area in Estonia, including health, labour and social matters. He has working experience as a physician, senior level civil servant, researcher, service design consultant and entrepreneur.

Annex 3. Workshop Video

The workshop video is accessible through Guardtime YouTube channel.

- "PRIViLEDGE Workshop on Data Sharing and Privacy" (2:02:34)
  https://www.youtube.com/watch?v=n1rejiJ-Gp0

This report was compiled by Liis Livin (Guardtime OÜ, PRIVILEDGE project) and released in November 2020.
Contact: liis.livin@guardtime.com

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.