D3.5 Risk and recommendations on cybersecurity services

Author(s)	CONCEPTIVITY
Status	Final
Version	V1.0
Date	19/03/2021

Dissemination Level

☒ PU: Public

□ PP: Restricted to other programme participants (including the Commission)

□ RE: Restricted to a group specified by the consortium (including the Commission)

□ CO: Confidential, only for members of the consortium (including the Commission)

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP – D3.5	
Deliverable lead	CONCEPTIVITY
Related work package	WP3
Author(s)	Mark Miller, Victoria Menezes Miller (lead & author) CPT; Paolo Balboni & Anastasia Botsi, ICTL; Nicholas Ferguson, Julie Arteza & Niccolò Zazzeri, Trust-IT; Paolo Modica, AON.
Contributor(s)	**Consortium:** ICTL, Trust-IT, AON **Webinar report contributions:** Roberto Cascella, ECSO Andrés Castillo, University of Brighton, DEFeND Panos Chatziadam, FORTH-ICS & Cyber Sure Mirjam Fehling-Kaschek, Fraunhofer & RESISTO Anna Georgiadou - DSS Lab, NTUA & Energy Shield Annarita Iodice, MATICMIND & DEFEND Aristeidis Farao, University of Pireaus & SECONDO Lucio Gonzalez Jimenez, SGS Sabina Magalini, Rome Catholic University School of Medicine (UCSC) & PANACEA Evangelos Markatos, FORTH-ICS & REACT Natalie Miller, Fraunhofer & RESISTO Orhan Ermis, EURECOM & PAPAYA Spyros Papastergiou – Maggioli & CyberSANE Andrea Praitano, MATICMIND & DEFEND Panagiotis Sarigiannidis, University of Western Macedonia & SDN-microSENSE Max Van Haastrecht, University of Utrecht & GEIGER Fabrizio De Vecchis, RHEA Group & PANACEA Eleni Veroni, University of Pireaus & CUREX Christos Xenakis, University of Piraeus & SEALED GRID & SECONDO Christos Xenakis, University of Pireaus & CUREX
Due date	30/04/2020
Actual submission date	19/03/2021
Reviewed by	Marina Ramirez, AEI; Paolo Modica, AON & Nicholas Ferguson, Trust-IT
Start date of Project	01/05/2017
Duration	51 months

Revision history

Version	Date	Authors	Notes
v0.1	02.03.2020	M. Miller, V. Menezes Miller	Draft
v0.2	26.06.2020	M. Miller, V. Menezes Miller	Outline for invitation of comments
v0.3	13.11.2021	M. Miller, V. Menezes Miller	Revision based on AON and TRUST-IT contribution
v0.4	01.02.2021	M. Miller, V. Menezes Miller	Concertation

v0.5	02.02.2021	M. Miller, V. Menezes Miller	Webinars (Sections 5.1, 5.3)
v0.6	08.02.2021	Paolo Balboni, Anastasia Botsi	Draft sections relating to privacy and data protection (Sections 2.1 , 3.1, 3.2.2. 3.2.3, 3.2.4., 3.2.5.)
v0.7	10.02.2021	J. Arteza	Webinars (Sections 5.2, 5.3, 5.4)
v0.8	12.02.2021	M. Miller, V. Menezes Miller	Restructure, full edit of Sections 1, 2, 3.1, 3.2, 3.3
v0.09	16.02.2021	M. Miller, V. Menezes Miller	Edit Sections 4.4, Survey, Webinar
v0.10	17.02.2021	M. Miller, V. Menezes Miller	Completion of Executive Summary, Introduction, Editing of the entire document
v.11	19.02.2021	M. Miller, V. Menezes Miller	Conclusions (Sections 7.1 and 7.2)
v.12	19.02.2021	M. Miller, V. Menezes Miller	Webinar (Section 6) and Conclusions related to Webinars (Section 7)
v.13	22.02.2021	P. Balboni, A. Botsi	Additions to Sections 2.2, 4.4.1, 4.5.1, conclusions
v.14	23.02.2021	M. Miller, V. Menezes Miller	Webinars (Section 6) updates on statistics
v.15	23.02.2021	N. Zazzeri	Cyber Risk Tool statistics and implementation/launch section
v.16	23.02.2021	M. Miller, V. Menezes Miller	Final Conclusion, Re-organization of topics in all webinar sections
v.17	25.02.2021	M. Ramirez, M. Miller, V. Menezes Miller	Changes following first reviewer's comments
v.18	26.02.2021	P. Modica, M. Miller, V. Menezes Miller	Changes following second reviewer's comments
v.19	26.02.2021	M. Miller, V. Menezes Miller	Webinar statistics
v.2	19.03.2021	N.Ferguson	Final review

Executive Summary

This deliverable presents the results of the analysis of the risk and recommendations on cybersecurity services from different angles, which include an **update on the European Union's privacy, data protection and cybersecurity compliance framework**, the **challenges of emerging technologies**, in particular, Artificial Intelligence (AI) and Internet of Things (IoT), the **challenges of privacy during Covid from a user perspective** and the **findings of the third concertation event thereby resulting in a set of key recommendations covering the cybersecurity services landscape**, with a particular focus on privacy and healthcare.

The Third Concertation event planned for the Cyberwatching.eu project was replaced by a set of four webinars. This replacement was required and agreed due to the challenges in having a further physical concertation event – it was felt that a series of webinars would have a more significant impact given the specific topics that were selected and relevant to the current environment. Thus, although clearly the COVID crisis actually affected the concertation event negatively in that a physical event could not take place, it also presented a unique opportunity to discuss and solicit input concerning the perceptions of the relevant stakeholders with respect to privacy and the change of work requirements and way of working during this unprecedented crisis period, as well as to address the challenges encountered during Covid in the healthcare system.

In this deliverable, the results of a COVID survey which was carried out during several months is quite interesting having been undertaken as an additional task outside of the normal expected planning of the Cyberwatching.eu project. The conclusions and recommendations are thus also reflective of the input and feedback from the relevant stakeholders giving even more credence to our approach. As such, this deliverable actually goes above and beyond the initial intentions and objectives, despite the fact that the COVID crisis significantly hindered our ability to accomplish this. We will continue to pursue further the feedback from the stakeholder community, especially within the planned roadmap deliverable due at the end of the Cyberwatching.eu project. We also note that this deliverable represents the current snapshot and analysis, which presents as well a moving target given the risk aspects concerned.

Table of Contents

Table of Tables

Table of Figures

1 Introduction

This deliverable provides a **global view of risk on cybersecurity services**. In order to examine the complexity of this view, an update is, first, provided on the European Union's privacy, data protection and cybersecurity compliance framework (Chapter 2). It is recalled that Deliverable D3.2 "European Cybersecurity Research and Privacy and Innovation Ecosystem" has already presented a whole chapter dedicated to the Risk Management Ecosystem, covering amply the cybersecurity risk management process and showcasing a number of EU-funded projects in the domain of risk management.

Given the pandemic situation of 2020/21, two important factors influence the content of this deliverable:

- The **pandemic situation** which related specifically to numerous concerns on privacy and data collection;
- The **third concertation event** which should have taken place physically was replaced by a **series of webinars.**

For ease of understanding, this deliverable contains the following in brief:

Chapter 2: A description of the European Union's (EU's) privacy, data protection and cybersecurity compliance framework.

Chapter 3: Cybersecurity Services and Emerging Technologies, which specifically addresses challenges related to Artificial Intelligence (AI) and Internet of Things (IoT).

Chapter 4: Covid Pandemic – A New Crisis in Privacy. This chapter looks at the specifically privacy issues which became more pronounced during the pandemic.

Chapter 5: Cyber Risk Temperature Tool. This chapter describes the Cyberwatching.eu initiative to create a useful tool for SMEs which assists in assessing cybersecurity readiness.

Chapter 6: Summaries of the four webinars which took place to replace the Third Concertation Event.

Chapter 7: Conclusions and Recommendations covering the numerous recommendations in this deliverable ranging from legal aspects, to cybersecurity services, user perspectives (SMEs, MSEs, healthcare providers), privacy issues arising from the pandemic.

Despite the challenges of the COVID crisis during this period, we have taken the opportunity to expand the task work to include **the additional survey on the stakeholder perception of privacy** and the change of work and the way of working during these difficult times of the pandemic.

In addition, it is important to note that the analysis presented is also the result of significant research efforts with respect to privacy, data protection and compliance.

The conclusions and recommendations, including the result of the survey analysis, represent also the concerns of the stakeholder community at large.

2 European Union's Privacy, Data protection and Cybersecurity Compliance Framework

2.1 EU Regulatory Framework

The interplay between the legislations of the European Union (EU), including the General Data Protection Regulation (GDPR), the Directive on Network and Information Security (NIS) and the ePrivacy Directive (upcoming ePrivacy Regulation) have been analysed in depth in previous deliverables of cyberwartching.eu, as indicated below:

- D3.2:European Cybersecurity Research and Privacy and Innovation Ecosystem, specifically, Chapter 2 "EU Cybersecurity Governance Ecosystem".
- D3.4:EU Cybersecurity Legal and Policy Aspects: Preliminary Recommendations and Road Ahead", specifically, Chapter 2 "Interplay Between GDPR and NIS Directive". That deliverable's objective was to support policy, regulatory standards & legal discussions that contribute to shaping global cybersecurity and the privacy landscape.
- D4.4:EU Cybersecurity and Privacy Interim Roadmap, Chapter 2.2 "The Evolving Legislation Landscape".

This deliverable will address updates of importance to the EU Privacy, Data Protection and Cybersecurity Compliance Framework, namely the "ePrivacy Regulation" and relevant updates from stakeholder bodies, namely, the European Cyber Security Organisation (ECSO).

2.2 ePrivacy Regulation Update

The ePrivacy Regulation remains under negotiations under the new Presidency of the Council, with another draft regulation published on 5th January 2021.[1] The Portuguese Presidency, which will remain for the next 6 months, until 30 June 2021[2] has several aims with regards to moving the ePrivacy Regulation forward.

The European Data Protection Board ("EDPB") issued a statement on the ePrivacy Regulation and the future of the Supervisory Authorities and the EDPB, calling for any proposed changes in the draft Regulation to complement the General Data Protection Regulation ("GDPR"), by providing "additional strong guarantees for confidentiality and protection of all types of electronic communication". [3]

Following this approach, the Presidency proposes "*to simplify the text and to further align it with the GDPR*", to ensure consistency and legal certainty for users and businesses – similar to the Commission's Proposal of 10 January 2017.[4] The draft

[1] 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), Brussels, 5 January 2021, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

[2] More information available at: https://www.consilium.europa.eu/en/council-eu/presidency-council-eu/

[3] Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB, Adopted on 19 November 2020, p.1, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf .

[4] 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), Brussels, 5 January 2021, p.2, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

specifies that the amendments "reflect the *lex specialis* relation of the ePrivacy to the GDPR", which, in practice means that the accountability principle will also apply to the providers of electronic communications services.

The Presidency points out that one of the most important amendments introduced is the possibility to process electronic communications' metadata.[5] In the same scope, another equally important amendment was made in Article 8(1(g)) of ePrivacy Regulation which aligns the ePrivacy Regulation with the further processing compatibility of the GDPR[6]. Specifically, this amendment allows providers of electronic communication services to use the collection of information from the end-user's terminal equipment, as well as the processing and storage capabilities of the terminal equipment, for further processing activities. This amendment appears to facilitate the providers of electronic communication services to rely on the purpose of "further use".

However, additional security measures seem to be expected in order for the electronic communications' metadata to be further processed, some of which are: the pseudonymisation of the metadata, excluding the use of the said metadata for profiling activities, excluding metadata that includes location data that reveal special categories of personal data. Having the above, **further processing of metadata of electronic communications has a high benchmark** according to the new draft of the ePrivacy Regulation.

In addition, the new draft reinstates the ability for **third parties to share *anonymised* statistical metadata**. This is in line with the proposal of the EDPB which emphasized that electronic communications' metadata "can be processed without consent after it has been genuinely anonymised".[7] Prior to sharing of anonymised metadata, the draft requires additional safety measures, including the carrying out of a Data Protection Impact Assessment (DPIA) and possibly the need for a prior consultation with the Supervisory Authority (as stated in Articles 35 and 36 of the GDPR), thereby informing the end-user of the envisaged processing operations of data, respecting his or her right to object, and implementing technical and organisational measures.[8]

Furthermore, the new draft recognises **the "performance of a contract" as a legal basis** for the processing of metadata and other permitted processing activities (for example, billing, calculating interconnection payments, detecting or stopping fraudulent or abusive use of / subscription to electronic communications' services).[9] The new draft also retains the possibility for obtaining end-user consent to the specific

[5] Article 6c and Recital 17aa 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), Brussels, 5 January 2021, p.2, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

[6] Specifically, Articles 5 (1(b)) and Articles 6 (4) of the General Data Protection Regulation.

[7] Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB, Adopted on 19 November 2020, p.2, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf .

[8] Article 6b (2 (a) to (c)) 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), Brussels, 5 January 2021, p. 73, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

[9] Article 6b (1 (b)) 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), Brussels, 5 January 2021, p. 70, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

processing of communications' metadata. Meanwhile, similar to the previous version of the Regulation, the ability to rely on legitimate interests as a lawful ground to process metadata remains absent. Nonetheless, being able to rely on the ground of the performance of a contract is a valuable addition to the ePrivacy Regulation, as it offers electronic communications providers another legal basis other than consent for this processing activity.

Another more minute but nevertheless noteworthy amendment made was the **update of the 'location data' definition**, which was absent from the previous version of the ePrivacy Regulation. [10] The inclusion of this definition to the ePrivacy Regulation is instrumental, as it will help ensure legal certainty and consistency for electronic communications providers.

It is worth noting a concern underlined by the EDPB which has not been directly tackled in the new draft of the ePrivacy Regulation. Namely, that the **oversight of the compliance with the ePrivacy Regulation** should be the same supervisory authorities which are responsible for the enforcement of the GDPR, as initially proposed by the European Commission.[11] Furthermore, the EDPB suggests that the future ePrivacy Regulation should be "*formulated to improve its procedural situation instead of adding complexity*". [12] This is a topic that is yet to be clarified in the current state of the legislation and could potentially create many inconsistencies and procedural uncertainty among electronic communication providers.

In the last days before the submission of this deliverable, the Council of the EU has agreed on the revised proposal of the Portuguese presidency, which is a positive development towards the final text.[13] However, due to the lack of sufficient time for a proper analysis, and in order to respect the due process of the review of deliverables within the consortium, the proposal of February 10th will be further analysed in the final White Paper around legal compliance and policy statements (D3.7).[14]

In conclusion, it is clear that the new Presidency aims to further align the ePrivacy Regulation with the GDPR. The inclusion of the further processing possibility in alignment with the GDPR, the addition of the legal basis of performance of a contract for the processing of metadata, and the ability to share anonymised metadata with third parties (under the implementation of additional security measures) are all advancements towards a more cohesive legal framework for electronic communication

[10] Article 4 (3 (j)) 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), Brussels, 5 January 2021, p. 65, available at: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf .

[11] European Commission, 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), Brussels, 10 January 2017, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[12] Statement on the ePrivacy Regulation and the future role of Supervisory Authorities and the EDPB, Adopted on 19 November 2020, p.3, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201119_eprivacy_regulation_en.pdf.

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

[14] 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), Brussels, 10 February 2021: available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

providers. However, the topic of the oversight of ePrivacy compliance is yet to be clarified in the current state of the legislation and could potentially create many inconsistencies and procedural uncertainty among electronic communication providers. The consortium will continue to track the progress of the ePrivacy Regulation in the following months and note any updates to Deliverable D3.7 - Regulating Frameworks.

3 Cybersecurity Services and Emerging Technologies

Through several webinars and the annual **Concertation Meetings**, the Consortium was able to engage in constructive discussions with the community regarding the future of research projects in the sectors of cybersecurity and privacy. The feedback from surveys undertaken in **D3.3 (White Paper on Cyber Security Gap Analysis)** and **D3.4 (EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead)** was crucial to obtain a practical reflection of the current situation from the **perspective of gap analysis** and practical feedback on standards and certification and recommendations directly from the community involved in ongoing H2020 projects and experts in the future of Horizon Europe and the Digital Europe Programmes.

It also became apparent through the **European Project Radar**[15], as well as webinars and workshops carried out by Cyberwatching.eu and representative Horizon 2020 projects in previous months[16], that **many cybersecurity services continue to need guidance on the application and implementation of different legislations**. Deliverable D3.4 only briefly touched upon some of the challenges posed to **Artificial Intelligence** and **Internet of Things** with some initial recommendations recalled below from Deliverable D3.4:

Recommendations on Artificial Intelligence

a) Guidelines on AI/machine learning and data minimisation
b) Solutions to address complexity of processing in the context of AI and principle of transparency:
c) Guidelines on methodology for risk analysis specifically related to AI.
d) User-friendly instruments to disseminate Ethics guidelines for AI.

Recommendations on Internet of Things:

a) Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments.
b) Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR.

Table 1: Recommendations on AI and IoT from D3.4 (Executive Summary)

[15] European Project Radar: https://www.cyberwatching.eu/technology-radar

[16] Webinar on Security and Privacy by Design for Healthcare, Webinar on Cybersecurity for Healthcare: Human and Legal Perspectives, Workshop on Financial Sector Infrastructure Cyber-physical security and Regulatory Standards Workshop.

The above recommendations remain current and the following details a number of **challenges posed to cybersecurity services concerning both sectors of AI and IoT** and the means to overcome them.

3.1 Emerging Technologies

Cybersecurity services increasingly rely on the use of emerging technologies, such as AI and IoT. However, **new EU legislation** often comes with a challenging implementation period, during which **European Member States** must, efficiently and coherently, **adapt their national laws** to the requirements of the new piece of EU legislation.[17] An example of such a challenge and changing environment is provided in Section 2.2, regarding the difficulties of the COVID contact tracing apps to comply with the GDPR. Due to this acknowledged challenge, EU institutions and agencies have looked into **how these difficulties can be overcome**. One example is through enforcement: consider the designated national authorities responsible for enforcing the terms of the GDPR[18] and the Directive on Network and Information Security (NIS-D).[19] However, both the GDPR and NIS-D provide additional challenges which are inherent to their domains of regulation, in particular where they are considered as applicable to **innovative fields of technology, such as Emerging Technologies** – the complexities and intrusive nature (in terms of personal data collection and further processing) of AI and IoT-based products and services **create theoretical and practical issues when looking to enforce the obligations of the GDPR or NIS-D** against technology service developers/providers and users.

Since the GDPR and NIS-D have different scopes,[20] the concerns raised when they are considered vis-à-vis the Emerging Technologies are also different. Generally speaking, the main concerns related to the GDPR revolve around understanding **which GDPR obligations are relevant to developers/providers and users of Emerging Technologies**, and which need to be adapted so that they can remain relevant, and whether any conflicts so intensely with the particularities of the Emerging Technologies that they cannot regulate their use to any degree of usefulness. In contrast, the main concerns related to the NIS-D lie in the **implications around injecting Emerging Technologies into the operations of the Operators of Essential Services (OESs) and Digital Service Providers (DSPs)**, and to what extent this can be done without sacrificing security, usability and traceability of networks and information systems.

3.1.1 Ethics and Trustworthy AI

One particular problem raised by Emerging Technologies, which seemingly cannot be offset by way of current regulations alone, is seen in its relationship with **transparency and ethics**. Consolidating this connection, in 2019, the European Commission High-Level Expert Group on AI (AI HLEG) published their "**Ethics guidelines for trustworthy AI"** that would aid in the development of trustworthy AI in the European context. [21] In addition, a practical tool has been developed by the Commission in July

[17] European Parliament, *in the implementation of EU law at national level* (November 2018), available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/608841/IPOL_BRI(2018)608841_EN.pdf

[18] Arts. 51 *et seq.* GDPR.

[19] Art. 8 NIS-D.

[20] See Section 2 and Section 2.2, above.

[21] High-Level Expert Group on Artificial Intelligence*, Ethics Guidelines for a trustworthy AI* (8 April 2019), available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

2020, with the aim of supporting and revising the guidelines.[22] According to the AI HLEG, 'Trustworthy AI' is comprised of **three major elements** which "*be met throughout the system's entire life cycle*:

1. *it should be **lawful**, complying with all applicable laws and regulations;*
2. *it should be **ethical**, ensuring adherence to ethical principles and values; and*
3. *it should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm*."[23]

The AI HLEG Guidelines provide with a useful framework, based on **seven requirements** for artificial intelligence in order for it to be considered **to be trustworthy**.[24] Trustworthiness can be seen as a necessary prerequisite for the ultimate success of the Emerging Technologies as, in absence of trust, the Emerging Technologies may not see widespread use. These requirements include (1) the involvement of human agency and oversight, calling for AI to empower individuals and promote their fundamental rights; (2) technical robustness and safety, ensuring that AI is both secure and resilient; (3) privacy and data governance, guaranteeing compliance with law and also fostering acceptable data governance mechanisms; (4) transparency, with respect to the data used, the system itself and the actual business model of the AI; (5) diversity, non-discrimination and fairness, circumventing bias and promoting diversity; (6) societal and environmental well-being which calls for AI to positively contribute to society; and finally, (7) accountability, which calls for the implementation of mechanisms that ensure AI systems are accountable and responsible.

On 17 July 2020, AI HLEG published "The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment"[25], which is a tool that supports the afore-mentioned "Ethics Guidelines for Trustworthy Artificial Intelligence" (AI) and the seven key requirements of trustworthy AI). Through an accessible and dynamic checklist provided in this web-based tool[26], businesses and organizations, developers and deployers of AI, can self-assess through concrete steps their systems under development, in order to ensure that their users can benefit from AI without being exposed to unnecessary risks.

3.1.2 Risk Assessment for Emerging Technologies

The public sector outside of Europe, as exemplified by the Canadian Government, has also made efforts in order to provide a solution to the difficult nature of carrying out risk assessments on Emerging Technologies, through the development of an **Algorithmic Impact Assessment (AIA)**.[27] The AIA was designed in order to assess and manage

[22] European Commission, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 17 July 2020, available at: https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[23] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), p. 5, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[24] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 14-20, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[25] *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* available at https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[26] Web-based self-assessment AI tool available at https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence

[27] Government of Canada, *Algorithmic Impact Assessment (AIA)*, available at:

risks related to **automated decision-making**, and was borne from the Canadian Directive on Automated Decision-making, aiming to "*ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law*".[28] In this way, the Canadian Government has demonstrated its commitment to the principles of "*transparency, accountability, legality, and procedural fairness*", [29] principles which are also enshrined in European legislation.

Another kind of risk assessment that could be developed and carried out by market operators is one that specifically takes into consideration the rights of individuals, potentially inspired by the already-used fundamental rights impact assessment. The **fundamental rights impact assessment** is a product of the **Charter of Fundamental Rights of the European Union's implementation**, and their relative Operational Guidance was adopted by the European Commission in 2010. [30] It provides an assessment method that allows for the analysis of the influence a specific policy may have on the fundamental rights of EU citizens, thereby seeking to ensure the compliance of that policy with the Charter.[31] The development of a risk assessment framework for industry that is based on the EU's fundamental rights risk assessment, taking into consideration the real and potential risks to the rights and freedoms of individuals that are implicated in AI systems, could help mitigate such risks and ensure the development of transparent and ethical Emerging Technologies.

The **EDPB** has also issued **relevant Guidelines** on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data[32] and a toolkit,[33] from which inspiration could also be taken for the development of an **Emerging Technologies risk assessment** (as well as the ALTAI tool as described in Section 3.1.1). This assessment could evaluate both necessity, through the identification of the fundamental rights and freedoms potentially impacted, looking clearly at the objectives of the system and the relevant interests behind it, and ensuring that the system is the least intrusive in order to avoid negatively affecting rights and freedoms; and proportionality, insofar as a balancing test should be carried out, ensuring that the results of the system are actually in line with its objectives, that the

https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html.

[28] The Government of Canada implemented the Directive on Automated Decision-Making, which took effect on 1 April 2019 and of which compliance is mandatory from 1 April 2020. The Directive can be accessed here: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

[29] Government of Canada, *Directive on Automated Decision-Making* (1 April 2019), available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

[30] See also European Commission, Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (19 October 2010), available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0573.

[31] European Commission, Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments (6 May 2011), p. 3, available at: https://ec.europa.eu/info/sites/info/files/opperational-guidance-fundamental-rights-in-impact-assessments_en.pdf.

[32] European Data Protection Supervisor, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19 December 2019), available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[33] European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, (11 April 2017), available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

data processing is evaluated in terms of scope, extent and intensity, and that adequate safeguards are in place to improve proportionality if needed.[34]

3.2 Artificial Intelligence (AI)

Artificial intelligence (AI) is increasingly becoming an integral part of technology and cyberspace. AI can be implemented in systems, software and devices of varying sectors, to similar degrees of effectiveness.[35] From the data protection perspective, AI is typically used as a tool for automated decision-making and profiling, by leveraging algorithms to process large volumes of data.[36] In terms of AI being implemented in critical infrastructures, countries are putting AI to use in order to offer better and faster telecommunication services to citizens, run trade and stock markets by algorithms, or even create governmental procedures for voting, and managing administrative complaints.[37] In this context, **the main challenges arise when the processing activities carried out by means of AI are capable of leading to automated decisions** which produce legal, or similarly significant effects on data subjects.[38]

3.2.1 Challenges of Data Minimisation

One of the typical assumptions around the use of AI is that a large (potentially, a progressively expanding) dataset will be needed, so that the AI's algorithm can generate accurate and useful results, or even further develop (in the case of machine-learning algorithms). Considering that such large datasets may also include personal data, questions immediately come to mind: **Is it feasible for an AI-based system to work effectively without resorting to large volumes of (personal) data?** How can the principle of data minimisation be adhered to by AI-based systems?

This challenge is at the heart of the data protection issues that arise from the use of AI, because it seemingly places a core GDPR principle against the purposes and functions of AI itself. The incentive is to collect as much data as possible in order to render the AI operational, which may not factor in any considerations for the principle of data minimisation[39] – particularly because **AI algorithms will not only rely on data which is strictly relevant** to reach a desired output, given that AI must also learn to identify and discard data which is irrelevant to that goal, in order to increase its effectiveness after deployment (and avoid inaccurate or discriminatory results).[40] This

[34] This methodology is based on the European Data Protection Supervisor's *Quick-guide to necessity and proportionality*, available at: https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_q9uickguide_en.pdf.

[35] For more on this, see Consultative Committee of the Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Artificial Intelligence and Data Protection* (25 January 2019), available at: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8.

[36] For more on this, see UK Information Commissioner's Office, Big *data, artificial intelligence, machine learning and data protection* (4 September 2017), available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[37] European Commission, *Statement on Artificial Intelligence, Robotics and* 'Autonomous' *Systems* (9 March 2018), available at: https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf.

[38] See Art. 22(1) GDPR.

[39] Please note that this issue arises typically only for long-term AI projects, which integrate the data collected during the service or product lifecycle. If an AI is being developed as a one-off exercise, then once the training of the algorithm has occurred, there is no longer a conflict with the data minimization principle (as the storage and processing of large training datasets is no longer required).

[40] For more information on this, see European Parliament, Understanding *algorithmic decision-making: Opportunities and challenges* (March 2019), available at:

shows that even contextual data can be important for AI.[41] Therefore, the requirements for data minimisation – processing only personal data which is "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*",[42] cannot be upheld in the traditional form of the GDPR. Furthermore, given the difficulties in predicting the training speed or accuracy of a given AI model, AI developers may not be capable of correctly predicting just how much data (necessary or contextual) an AI algorithm will need in order to deliver the expected output.

In order to tackle this concern, it would be **recommended that further research be carried out on how the concept of data minimization can be tackled when mass data collection is necessary, in order to train algorithms within AI models**. It appears relevant, in this context, to distinguish between the data minimization during (1) the training of the model algorithm (original training data), and (2) once the AI is actually running on real-time data, which would be needed to ensure fairness, accuracy and lack of discrimination in AI decision-making. Furthermore, when assessing the adequacy, necessity or relevance of a given dataset for AI-based processing activities, due consideration should be given to the complexity of the problem or processing that the AI model is targeting, as well as the complexity of the learning algorithm. Considering the complexity of the problem/processing in question can help **define the underlying functions which the algorithm is meant to achieve**, providing insight into the input variables (i.e., types and volumes of data) that the algorithm will require; considering the complexity of the learning algorithm can help to understand how such data will be 'parsed' through the algorithm, allowing for a more precise identification of types of (personal) data which could be considered as adequate, relevant and necessary for the AI model to meet its intended purpose.

3.2.2 Challenges of Purpose Limitation

Under the GDPR's principle of purpose limitation,[43] personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".[44] As noted by the Article 29 Data Protection Working Party, "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility.*"[45] This notion of 'compatibility' is further explored in Art. 6(4) GDPR, which lays down criteria to be assessed by a controller in order to establish if a further processing purpose is compatible with the

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf.

[41] For simplicity's sake, consider the following example: if a developer is building an AI-based system to visually recognize fruit, the AI's training dataset may also need to include not only images of fruit, but also of any other objects or materials that may be mistaken for fruit, so that the AI learns what input to reject (and not just what input to accept).

[42] Art. 5(1)(c) GDPR.

[43] Art. 5(1)(b) GDPR.

[44] On this point, see Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf), p. 15: "*Personal data must be collected for specified purposes. The controller must therefore carefully consider what purpose or purposes the personal data will be used for, and must not collect personal data which are not necessary, adequate or relevant for the purpose or purposes which are intended to be served*".

[45] Article 29 Data Protection Working Party, *Opinion 03/*2013 *on purpose limitation* (2 April 2013), p. 21, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

initial purpose for data collection:[46] (1) whether there is any link between these purposes; (2) the context in which the personal data was collected;[47] (3) the nature of the personal data in question;[48] (4) the possible consequences of the intended further processing for data subjects; and (5) the existence of appropriate safeguards, such as encryption or pseudonymisation.

In light of this, a separate issue, which may arise more commonly with **machine-learning algorithms**, is the possibility for such algorithms to, **autonomously** (and in unexpected or unpredictable ways) **process (personal) data for purposes different**, or incompatible with, the original purposes for which the algorithms were set up. Machine-learning-based algorithms can - not only learn to achieve the goals they are programmed for - but they can also reinterpret their goals, shifting the focus from achieving their original goals to achieving the feedback they would receive if they had done so.[49] Where this occurs the result is that **personal data is processed for a purpose not originally disclosed to data subjects** (i.e., not specified or explicit), and which may potentially be incompatible with the purposes for which personal data was originally collected. Such a result would inevitably collide with the principle of purpose limitation.

Such a concern can seemingly only be addressed by **imposing limitations or further requirements on the use of personal data within AI-based systems.** Algorithms (and, in particular, machine-learning algorithms) should be carefully developed so that they will not, autonomously or beyond the control of the relevant controller, process personal data collected for purposes beyond the scope of their collection (or, at least, not without a proper compatibility test, under Art. 6(4) GDPR, having been performed by the relevant controller) – **any guidance which can be offered by policy-makers and competent authorities in this regard would prove invaluable.**

Controllers should carefully analyse the systems that they wish to implement and ensure that they are able to provide clear and adequate information to data subjects on how those systems will work and, in particular, the purposes for which they will use personal data – here, **guidelines or templates on how to disclose such information in a digestible way for individuals (consumers), considering, where relevant, the requirements of Art. 13(2)(f) and 14(2)(g) GDPR,[50] could be of great benefit to AI developers and users.**

3.2.3 Challenges of Transparency and Lawfulness

Under the GDPR's principle of transparency,[51] **controllers are required to provide data subjects with information as to their activities involving the processing of personal data**, under, e.g., Arts. 13 and 14 GDPR. This information must include, in particular and where automated decision-making is concerned, "*the existence of*

[46] Note that Art. 6(4) GDPR generally allows further processing to take place, even in the absence of compatibility with the original processing purposes, where consent is relied on as a legal basis for the further processing, or where the further processing is authorised by Union or Member State law.

47 Under Art. 6(4)(b) GDPR, the relationship between data subjects and the controller must be considered, in particular.

48 Under Art. 6(4)(c) GDPR, whether or not special categories of personal data, or personal data related to criminal convictions and offences, are processed is an important consideration in this regard.

49 For more on this, see, e.g., Casey Chu et al, CycleGAN, a Master of Steganography, available at: https://arxiv.org/pdf/1712.02950.pdf.

50 See Section 3.1.3, below.

[51] Art. 5(1)(a) GDPR.

automated decision-making, including profiling, (...) and (...) meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".[52] This seeks to ensure that data subjects understand exactly how their personal data will be used by a given controller, and what the consequences for them may be.

When AI-based systems are used to process personal data, **difficulties arise in the provision of clear information to data subjects**, not only because such systems are often very complex (and, so, hard to explain in a concise and intelligible manner to data subjects, as required by Art. 12(1) GDPR), but also because the purposes for which such systems may handle personal data may evolve over time.[53]

According to the AI HLEG, the requirement of transparency in AI "*is closely linked with the principle of explicability and encompasses transparency of elements relevant to an AI system: the data, the system and the business models*".[54] As the Ethics Guidelines for Trustworthy Artificial Intelligence establish, traceability,[55] explainability[56] and communication[57] all play fundamental roles in transparency.

One particular specification of this issue, which involves also the principle of lawfulness, is the **selection of an appropriate legal basis for the use of AI**. As noted above,[58] controllers wishing to use AI to carry out automated individual decision-making will not only have to identify a legal basis, under Art. 6 GDPR, but also ensure that an exception, under Art. 22(2) GDPR, applies to their specific case. In particular,

[52] Art. 13(2)(f) and 14(2)(g) GDPR. For more information on this, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (6 February 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, and Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[53] See Section 3.1.2, above. It should be noted that data subjects must be informed by controllers of the purposes for which personal data are to be processed, under Arts. 13(1)(c) and 14(1)(c) GDPR; this is also a result of the need for purposes to be explicit, under the principle of purpose limitation, reflected in Art. 5(1)(b) GDPR. For more on this, see Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation* (2 April 2013), available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, and Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[54] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 18, 28-29, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[55] Traceability, in this context, calls for the datasets that contribute to the AI's decision-making to be traceable, and that the algorithms used by the AI are adequately documented. This requires the establishment of procedures and methods that concretely ensure traceability, ensuring that all possible outcomes of the decisions made by the AI are known and traceable, as well as hypothetical decisions that the AI could make. See High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), p. 18, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[56] Explainability, on the other hand, requires an assessment of how decisions made by an AI are understood, how much AI-made decisions can affect its own decision-making processes, why the system was deployed and what the business model of the system is – in other words, AI-based systems must be designed in a manner which allows them to be explained to the individuals concerned. See High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI (8 April 2019),* p. 29, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[57] Communication, the third requirement for transparency, entails the use of a disclaimer, allowing individuals to understand that they are interacting with an AI as opposed to a human being, also communicating the risks inherent to the AI. See High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI (8 April 2019),* p. 29, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[58] See Section 2.1, above.

in the absence of Union or Member State law authorising the use of AI in this manner, controllers will be met with a choice: either Art. 22(2)(a) GDPR[59] is applicable, and therefore, they must rely on Art. 6(1)(b) GDPR,[60] or Art. 22(2)(c) GDPR[61] is applicable, and therefore, they must rely on explicit consent from the data subjects concerned.

However, both of these options represent particular challenges: Art. 6(1)(b) GDPR requires the processing in question to be objectively necessary for either the performance of a contract with a data subject, or to take pre-contractual steps at the data subject's request – if realistic and less intrusive options can be relied on to do so, this legal basis cannot be relied on;[62] consent, in turn, must be informed, which requires a minimum amount of information to be provided to data subjects about the processing to which they are consenting – naturally, if the processing purposes change, or other substantial parts of the information provided change, the validity of the consent itself may be called into question.[63] Outside of the scope of Art. 22 GDPR (such as where the decisions made do not create a legal or similarly significant effect on individuals, including, e.g., for the performance of analytics which are not used to make decisions on individuals,[64] or where there is substantial human intervention in an AI-based decision-making process[65]), controllers may consider other legal basis, including the pursuit of legitimate interests under Art. 6(1)(f) GDPR – this, however, will require a comprehensive legitimate interests assessment, as noted above.[66]

[59] Art. 22(2)(a) GDPR allows the processing of personal data in connection with automated individual decision-making if this is "*necessary for entering into, or performance of, a contract between the data subject and a data controller*".

[60] Art. 6(1)(b) GDPR allows the processing of personal data, in general, if this is "necessary 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".

[61] Art. 22(2)(c) GDPR allows the processing of personal data in connection with automated individual decision-making if this is "*based on the data subject's explicit consent*".

[62] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (8 October 2019), p. 8, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[63] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (10 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051), p. 18: "*(...) controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged*" and p. 21: "*There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, then new consent needs to be obtained*".

[64] For more examples of decisions which may, or may not, produce a legal or similarly significant effect on data subjects, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (6 February 2018), pp. 21-22, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[65] Note that, where such substantial human intervention exists, the decision-making process can arguably be excluded from the scope of Art. 22 GDPR (as it is no longer fully automated). On this, see Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (6 February 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053), p. 30: "*The controller can still envisage a 'model' of decision-making based on profiling, by significantly increasing the level of human intervention so that the model is no longer a fully automated decision making process, although the processing could still present risks to individuals' fundamental rights and freedoms*", and p. 27: "*Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all the relevant data, including any additional information provided by the data subject*".

[66] See Section 2.1, above.

The challenges faced by AI in terms of transparency and lawfulness can be seen as sharing **similarities with the processing of personal data for scientific research purposes** – as noted by Recital 33 GDPR, *"[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research*". This Recital goes on to suggest that "*[d]ata subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*".[67] Inspired by this Recital, an innovative suggestion would be to **develop guidance and/or means for AI developers and users to provide dynamic information notices (using illustrations, flowcharts, videos, etc.) to data subjects, seeking to inform them about the key aspects of how their personal data will be used, walking them through the AI's process step-by-step and, where relevant, asking for their consent to the parts of the processing which are known at the time** – this information and consent request could then be updated/renewed in the case of any foreseen substantial changes at a later stage. However, in order for this to function in a manner similar to the possibility foreseen by Recital 33 GDPR, it is important that the renewal of consent is asked prior to the further processing which relies on it being carried out;[68] this would **require developers to design AI so that it does not automatically proceed with incompatible further processing of personal data**, unless it is confirmed – by the developer or user – that a legal basis for this exists.

Other issues arise specifically around the use of consent, such as the need to **allow for consent to be withdrawn**.[69] Developers must bear this in mind, and design AI-based systems to allow data pertaining to specific individuals to be extracted from a dataset and not further considered by the system in question. **Guidance and further research on how this can be attained in practice – in particular, considering that, where automated individual decision-making is concerned, Art. 22(2)(c) GDPR is, as our practical experience has shown, the most likely exception to be relied on – would be welcomed.**

3.2.4 Challenges of Security

Security of datasets used in AI-based systems is a key concern.[70] There are several ways in which these **datasets can be maliciously compromised**, such as proprietary

[67] For more on the applicability of Recital 33 GDPR to the use of consent in connection with scientific research purposes, see Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (10 April 2018), pp. 28-30, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[68] On this, note the position stated in Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679* (10 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051), pp. 17-18: "*In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed. WP29 has consistently held in previous opinions that consent should be given prior to the processing activity. Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording 'has given' in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity.*"

[69] Art. 7(3) GDPR.

[70] For more on this, see, e.g., Jake Saper, *How to* Hack *Your Way Into a Proprietary Data Set* (17 July 2018), available at: https://www.forbes.com/sites/insights-intelai/2018/07/17/how-to-hack-your-way-into-a-proprietary-data-set/.

hacking of datasets, or even use of datasets against the AI in order to disrupt its decision-making.[71] Where machine-learning is concerned, the fact that such systems can autonomously deviate from their originally programmed goals can lead to the choices and predictions generated by such systems being misled by an attacker. The **impact of an integrity attack** on a dataset, or on an AI processing such a dataset, **can be massive, and could trigger public interest concerns** – consider, for example, where hacking a connected vehicle could put people's lives at risk. Security measures applied to AI must consider the direct risk that attacks on AI or its dataset may create for individuals.

In order to determine and implement appropriate security measures, AI developers and users must necessarily assess the relevant risks involved, so that they can select those measures deemed most adequate to address them. This refers to the risk-based approach promoted by the GDPR (in particular, for this case, Art. 32 GDPR), but which is also addressed in the NIS-D – as mentioned above,[72] the NIS-D expects OESs and DSPs (including those using AI) to manage the risks posed to their networks and information systems, through the implementation of appropriate security measures. If proper risk management is not carried out, then both the GDPR and NIS-D are breached. Once more, the manner in which it appears best to resolve this issue is **the development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures,[73] at varying levels of sophistication (to account for developers and users of different sizes, types and economic capabilities), which may be considered in order to properly address identified risks.**

3.3 Internet of Things (IoT)

While the opportunities created for society and, in particular, the economy of having an ecosystem of interconnected services and devices are considerable, **the amount of data** (including personal data) **required by IoT devices/services** – collected through a variety of sensors – **is both large and intrinsically intrusive** for the individuals concerned.[74] Considering that the European Union Agency for

[71] For more on this, see, e.g., Florian Tramèr et al, *Stealing Machine Learning Models via Prediction APIs* (August 2016), available at: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf.

[72] See Section 2.2, above.

[73] Concerning use of AI and the NIS-D, one key reference to make is to the concept of SIEM (security information and event management), which indicates a model of approach to risk management combining two fundamental functions: (1) SIM (security information management) and (2) SEM (security event management). The key principle underlying any SIEM software solution is the ability to aggregate significant data from multiple sources, so as to identify deviations/anomalies from the norm, and then trigger appropriate actions to solve the security problem (e.g., when a potential critical event is identified, a SIEM solution can gather additional information, generate alarms and indicate additional security controls to block the progress of that event). By collecting and aggregating information from, e.g., servers, physical/virtual storage resources, PCs and smartphones, SIEM solutions essentially help to keep the various security measures which may be at a developer or user's disposal manageable. SIEM software can use heuristic algorithms that contemplate the probability of addressing cyber-attacks of various types, such as zero-day exploits, distributed denial of service (DDOS) attacks and brute force attacks. The system exploits a baseline, a basic model that allows it to perform pattern matching operations, log aggregation and analysis to locate anomalous activities. A solution of this importance can only be considered fundamental, in combination, in the most complex realities or more compliant with the requirements of the NIS-D, with the presence of a SOC (Security Operation Center).

[74] See, e.g., European Data Protection Supervisor, *Opinion 4/2015 – Towards a new digital ethics* (11 September 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf), p. 7: "*How this information is handled could affect the privacy not only of the users of the devices, including where used in the workplace, but also the rights of others who are observed and recorded by the device. While there is little evidence*

Cybersecurity (ENISA) has identified IoT as a technology which is "*at the core of operations for many Operators of Essential Services […] especially considering recent initiatives towards Smart Infrastructures, Industry 4.0, 5G, Smart Grids*",[75] ensuring that appropriate security measures can be defined for IoT systems is a matter of particular concern.

3.3.1 Challenges of Data Minimisation

As noted above,[76] **IoT devices and services**, as they are generally currently designed, inherently require the processing of large amounts of data (including personal data).[77] In particular, these devices and services are **often configured to allow for communication with other IoT-connected devices and services by default**, without needing the intervention or awareness of the data subjects concerned,[78] which ties this problem into the problem of **individuals' potential lack of control** over the data which is sent and received by these devices. Just as is the case with AI,[79] this creates a **conflict with the GDPR's principle of data minimisation**. As noted by the Article 29 Data Protection Working Party, "*[]some stakeholders consider that the data minimisation principle can limit potential opportunities of the IoT, hence be a barrier for innovation, based on the idea that potential benefits from data processing would come from exploratory analysis aiming to find non-obvious correlations and trends*".[80]

One solution which could be considered by IoT developers/providers is to **more comprehensively design IoT devices and services with the principle of data minimisation in mind**, incorporating the concepts of data protection by design and by default into the development process.[81] In particular, as has been noted by the Article 29 Data Protection Working Party in the past, the principle of data minimisation "*specifically implies that when personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to*

of actual discrimination, it is clear that the huge volume of personal information collected by the 'Internet of Things' is of great interest as a means for maximising revenue through more personalised pricing according to tracked behaviour, particularly in the health insurance sector. Other domain-specific rules will also be challenged, for example where devices involving processing of health data are not be technically categorised as medical devices and fall outside the scope of regulation". See also, e.g., Mark Hung, *Leading the IoT: Gartner Insights on How to Lead in a Connected World*, available at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

[75] European Union Agency for Cybersecurity, *Good Practices for Security of IoT* (19 November 2019), p. 7, available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1.

[76] See Sections 1 and 3.2, above.

[77] See, e.g., European Commission, *IoT Privacy, Data Protection, Information Security* (available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753), p. 1.

[78] See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[79] See Section 3.1.1, above.

[80] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 16, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[81] See the Mauritius Declaration on the Internet of Things, issued at the 36th International Conference of Data Protection and Privacy Commissioners (14 October 2014, available at: https://edps.europa.eu/sites/edp/files/publication/14-10-14_mauritius_declaration_en.pdf): "*Data processing starts from the moment the data are collected. All protective measures should be in place from the outset. We encourage the development of technologies that facilitate new ways to incorporate data protection and consumer privacy from the outset. Privacy by design and default should no longer be regarded as something peculiar. They should become a key selling point of innovative technologies*".

use the service anonymously".[82] The **EDPB has produced recent guidelines which can act as a helpful checklist in this regard**, particularly concerning the principle of data minimisation.[83] One of the ways in which this could be done, which would also address the problem of individuals' lack of control over IoT data flows, would be for developers to consider **creating 'privacy dashboards'[84] or 'privacy interfaces' for individuals[85]** – these dashboards/interfaces, which could be available on specific devices (such as an individual's mobile phone), could act as a control centre for that individual's IoT devices and services, offering information and options concerning data receipt and transmission for each device or service. By default, all data transmissions which are not strictly needed for the device or service to function (regardless of IoT functionalities) should be turned off, and only activated upon an action of the data subject which would meet the GDPR's requirements for consent.[86] **This is also a problem which could be addressed by policy and regulation, where stricter requirements on data collection and transmission could be enforced on IoT developers. These could include an obligation to build in 'do not collect' switches or permissions into IoT devices and services, so that individuals can disable or limit collection and transmission of data before even activating the device or service.[87]**

Other privacy enhancing technologies could be considered, in this respect – consider, for example, the use of 'attribute-based credentials' or 'anonymous credentials' in the IoT context, by which individuals could selectively authenticate themselves in relation to IoT devices/services, **allowing only the collection/transmission of selected data which they find to be appropriate.**[88]

[82] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), pp. 16-17, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[83] See European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019), in particular pp. 19-20. See also, e.g., UK Information Commissioner's Office, *Data protection by design and by default*, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

[84] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227), pp. 20-22.

[85] See, e.g., Jennifer Kashatus, *Building Privacy into the Internet of Things* (4 August 2015), and Andy Crabtree et al, *Building accountability into the Internet of Things: the IoT Databox model* (27 January 2018), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6560684/.

[86] In particular, as defined by Art. 4(11) GDPR, consent must be an "unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". For more information on this, see Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (10 April 2018), pp. 15-18, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[87] See, e.g., Gilad Rosner et al, Privacy and the Internet of Things: Emerging Frameworks for Policy and Design, available at: https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf.

[88] See European Data Protection Supervisor, *Opinion 5/2018 – Preliminary Opinion on privacy by design* (31 May 2018), pp. 16-17, available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

ENISA has developed a methodology for assessment of privacy enhancing technology maturity, which can be relevant for technology service providers and users looking to implement such measures to address privacy concerns; see European Union Agency for Cybersecurity, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies* (31 March 2016), available at: https://www.enisa.europa.eu/publications/pets.

3.3.2 Challenges of Data Processing Roles

The processing of personal data through IoT-connected devices or services is often carried out by machines managed by different organisations, each of them using computational capacity provided by cloud service developers/providers and that can also involve analytic software programmes supplied by the related vendors.[89] This **exponentially increases the number of parties involved in the data processing activities** and the difficulties in clearly allocating data processing roles (controller or processor) to each one; failure to do so correctly may result in misallocation of respective duties and obligations towards the data subjects and towards the competent supervisory authorities.[90]

Given the variety of data processing roles which these stakeholders may play (which may vary per activity),[91] the contractual tools offered by the GDPR, in isolation, arguably do not suffice to address this problem, even if stakeholders would agree to use them to regulate their data processing relationships: joint controllership arrangements, under Art. 26 GDPR, would only cover instances of joint controllership[92] between stakeholders, whereas data processing agreements, under Art. 28(3) GDPR, would only cover instances where one stakeholder can be qualified as acting as a processor on behalf of another. In particular, the **GDPR does not provide any express obligations to contractually regulate instances where stakeholders may be acting as autonomous controllers**,[93] which may lead to the creation of "grey areas" where each stakeholder feels that the responsibility for compliance lies with

[89] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 11, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. See also European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015), p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

[90] Different supervisory authorities have advanced different models for assigning data processing roles to these stakeholders. See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), pp. 11-13, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, and European Data Protection Supervisor, *EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy* (16 December 2015), p. 5, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

[91] A data processing role should be defined for each specific data processing activity or operation performed by an organisation, and not merely adopted wholesale. Our practical experience has shown that many service providers, particularly in the digital and cloud domains, tend to qualify themselves generally as processors on behalf of their clients (which may be correct, concerning processing activities performed on clients' behalf, such as those needed to provide the service in question), when in fact they also perform processing activities for their own purposes (such as running analytics on use of their service, for service development purposes) or for those of third parties (such as engaging in programmatic advertising exchanges within their service). On this, see Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (16 February 2010, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf), p. 25, and European Data Protection Supervisor, *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725* (7 November 2019, available at: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf), p. 11.

[92] Under Art. 26(1) GDPR, "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".

[93] Autonomous controllership exists, generally, where two controllers engage in a processing relationship, each one for their own specific purposes and in a manner that renders them unable to influence the purposes of which the other will further process personal data (as opposed to joint controllership, where the purposes and means of processing are jointly defined by the controllers involved).

another, and thus feels free to process personal data in any ways deemed convenient or beneficial, to the detriment of the individuals concerned. To address this, **stakeholders could (and should) consider engaging with each other through more complex contractual frameworks** (which we would conventionally call "**Data Management Agreements**"), identifying the specific data processing activities/relationships which take place between them and their respective roles for each one,[94] and agreeing on different sets of terms to regulate each category of activity/relationship: (1) controller-to-processor terms, including the minimum obligations of Art. 28(3) GDPR,[95] (2) joint-controllership terms, including the minimum requirements of Art. 26 GDPR,[96] and (3) controller-to-controller terms, regulating aspects such as the provision of information to data subjects on data transmissions performed, responsibility for ensuring lawful collection and transmission of data, restrictions on further processing of data received, cooperation in the event of personal data breaches or supervisory authority requests, etc. Through these data management agreements, stakeholders could establish a level playing field for IoT-collected and -shared data, create greater certainty between them as to the extent to which such data may be used by themselves and others, and thereby create greater assurances of lawful processing for data subjects.

In this respect, **any guidance or further research into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), would be welcomed, to provide tools for stakeholders to effectively self-regulate**.

3.3.3 Challenges of Purpose Limitation

Given the interactions possible between different IoT-connected objects and services, multiple data flows may be generated that will, frequently, be left outside of individuals' control. As noted by the Article 29 Data Protection Working Party, "*[i]n the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep*".[97] The European Data Protection Supervisor has also noted that "*[t]he interaction between IoT and big data may pose risks to data protection among others, because it allows establishing connections between seemingly isolated and unrelated information. In*

[94] This builds upon the recommendation made by the European Data Protection Supervisor in its EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (16 December 2015, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf), p. 5.

[95] Art. 28(3) GDPR lays down various minimum obligations which must be included in written data processing agreements entered into between controllers and processors, including the need for processors to handle personal data under controller instructions (Art. 28(3)(a) GDPR), implement appropriate security measures (Art. 28(3)(c) GDPR), respect the GDPR's rules on engagement of further processors (Art. 28(3)(d) GDPR), delete or return data processed on behalf of the controller upon termination of the processing (Art. 28(3)(g) GDPR) and, in general, assist the controller in the performance of the controller's obligations (Arts. 28(3)(e), (f) and (h) GDPR).

[96] Art. 26(1) GDPR requires joint controllers to determine their respective responsibilities for GDPR compliance in a transparent manner (particularly where the provision of information to data subjects, and the addressing of data subject requests, is concerned) by means of an arrangement between them, unless this is already legally and specifically regulated.

[97] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. See also European Commission, *IoT Privacy, Data Protection, Information Security* (available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753), p. 2.

addition, generating knowledge from trivial data or even data previously thought to be 'anonymous' will be made easier by the proliferation of sensors, revealing specific aspects of individual's habits, behaviours and preferences".[98] In this sense, similarly to AI,[99] personal data may be **further processed by the different stakeholders** involved in the development and provision of IoT devices and services, **for purposes which may be incompatible with the original purposes** motivating the collection of personal data.

Here, again, **the imposition of limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services, seems to be a reasonable solution. Providing individuals with control over which data may be collected and transmitted, through the use of dashboards, privacy centres or other privacy enhancing technologies,[100] would already be a large step to achieve this goal**. However, one core difference between the AI systems previously analysed and the problem faced with IoT is the multiple different stakeholders which may be involved in the data collection and sharing process, without necessarily having agreed to any specific terms on how data shared with and received from other stakeholders should be used. In this respect, **imposing contractual limitations between stakeholders (through Data Management Agreements)[101] on the further processing of received personal data could be a key step to ensuring that appropriate limitations are in place, particularly in the absence of stricter and clearer policy on IoT data collection, sharing and repurposing**.

3.3.4 Challenges of Transparency and Lawfulness

The pervasive nature of IoT data processing can effectively lead to situations where **individuals** (whether or not they are the end-users or owners of IoT-connected devices) **find themselves under third-party monitoring**, regardless of whether they are aware of this or not.[102] Moreover, where decisions can be taken by IoT-connected devices automatically, **individuals will effectively lose control of their personal data** in the absence of clear information on the processing activities undertaken by such devices.[103] In more complex IoT systems, there may be no clear and comprehensive point of information where individuals can understand the terms under which their personal data are processed. This, in turn, can affect the validity of legal bases relied on by IoT developers, such as consent[104], as well as the ability for individuals whose data is processed to exercise their rights under the GDPR[105] (as, without knowledge that a processing activity is going on, this becomes impossible). As

[98] European Data Protection Supervisor, EDPS response to the Commission public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (16 December 2015), p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/15-12-16_online_platforms_en.pdf.

[99] See Section 3.1.2, above.

100 See Section 3.2.1, above.

101 See Section 3.2.2, above.

[102] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014), p. 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[103] European Commission, *IoT Privacy, Data Protection, Information Security*, p. 4, available at: available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753.

[104] As noted in Section 3.1.3 above, consent, under Art. 4(11) GDPR, needs to be informed, requiring the provision of a minimum amount of information to the consenting individual in order to be reliable as a valid legal basis.

[105] See Section 2.1, above.

noted above,[106] this runs afoul of the GDPR's principle of transparency, and of the concrete obligations to provide information to data subjects within the GDPR.[107] The GDPR requires information on data processing to be served to individuals before processing happens,[108] thereby reinforcing traditional and time-bound conceptions of notice.[109]

Nevertheless, controllers can explore several possibilities that will allow them to ensure that their users understand the processing that takes place and remain informed throughout the entire lifecycle of the IoT deployments. **Two suggestions to help comply with the principle of transparency are the use of just-in-time notifications[110] and periodic notifications,[111] which may allow developers to deliver specific and relevant information to individuals at times when they are most likely to be able to apprehend such information.[112]** Furthermore, as noted above, [113] **the development of privacy dashboards or control centres for individuals may be fundamental in this respect**, as it can allow not only the creation of a central point where information on the processing activities undertaken may be accessed, but also where individuals may set their preferences in regards to data collection/transmission and, potentially, also exercise their rights under the GDPR directly (e.g., accessing, rectifying, deleting or exporting personal data captured by IoT-connected devices). In any case, **further research and guidelines on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by) – would be welcomed.**

3.3.5 Challenges of Security

An additional concern of relevance to the use of IoT is **the ensuring of end-to-end security during the entire data lifecycle**. This is of particular importance given the

[106] See Section 2.1 and 3.1.3, above.

[107] Arts. 12, 13, 14, 15 and 34 GDPR.

[108] Art. 13(1) GDPR. Art. 14(3) GDPR, which applies only to data collected indirectly (i.e., from sources other than the data subject itself), allows the provision of this information at a later date – information must be provided within a reasonable period after the personal data have been obtained, but at the latest within one month, unless the data is used for communication with the data subject (in which case, information should be provided at the moment of communication, if sooner than the one-month deadline) or for transmission to another recipient (in which case, information should be provided at the moment of first transmission, if sooner than the one-month deadline). For more on this, see Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018), pp. 15-16, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[109] Michael Moran et al, *IoT and GDPR: A Data Convergence that Pits Against the Cautious* (February 2018), available at: https://microshare.io/wp-content/uploads/2018/02/GDPRWhitepaperFeb2018.pdf.

[110] Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation 2016/679* (11 April 2018, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227), p. 21.

[111] Jennifer Kashatus, *Building Privacy into the Internet of Things* (4 August 2015), available at: https://www.technologyslegaledge.com/2015/08/building-privacy-into-the-internet-of-things/.
Periodic notifications are more persistent and regular reminders about the ongoing data collection that occurs; these are referenced also by the Article 29 Data Protection Working Party in their *Opinion 2/2010 on online behavioural advertising* (22 June 2010, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf), p. 18.

[112] For example, during updates of the IoT device, or other major processes occurring during the lifecycle of the device.

[113] Section 3.2.1, above.

multiple stakeholders which may be involved, resulting in IoT-connected devices performing **data processing under the control of different organisations**, without an overarching orchestration and control over the data.[114] This raises several concerns not only under the GDPR's principle of security, but also under the NIS-D.

First and foremost, it is particularly difficult to ensure the carrying out of regular monitoring, auditing and testing activities where a large number of IoT devices are involved in the processing of information within a system.[115] Auditing may become impractical and unrealistic when considering smart infrastructures, made up of hundreds or even thousands of IoT-connected devices within a certain region; however, failing to audit creates a great amount of exposure to risk, as an attack on one device may result in an attack on the entire IoT-connected network or system. One of the most significant and unfortunately continuously expanding attacks of the IoT ecosystem is DDoS (Distributed Denial of Service), which exploits the vulnerabilities of the protocol related to IoT to perpetrate, more often, systemic attacks.[116] There are also new vulnerabilities found that are related to the use of the Constrained Application Protocol (CoAP). **In light of this, further research and the development guidelines and procedures to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices, would be welcomed.**

IoT devices, in addition to being hard to monitor, have the ability of communicating with each other. This machine-to-machine communication (M2M) allows them to share certain data in order to improve the IoT and its functionality. However, these **M2M capabilities also introduce privacy and cybersecurity concerns** across multiple products and services that may be offered, both by OESs and DSPs.[117] Essentially, the interoperability of the M2M can make the entire infrastructure of IoT-connected devices vulnerable.

The European Telecommunications Standards Institute has developed guidelines on cybersecurity in IoT for consumers, which lay out key security concepts which IoT device/service developers and users may consider, in order to address such concerns.[118] Furthermore, an additional consideration would be the **implementation of end-to-end encryption regarding all data collected and**

[114] See, e.g., Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p.9. On this matter, it is relevant to consider the work performed by ENISA in mapping existing security standards against the IoT landscape: see European Union Agency for Cybersecurity, *IoT Security Standards Gap Analysis* (17 January 2019), available at: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis.

[115] In such a scenario, the heterogeneous connections determine what in information security is technically defined as an "increase of the exposed surface", with an exponential extension of the hardware and software vulnerabilities, connected to potential risks of exploitation by cyber criminals. In such cases, it is not uncommon for IoT devices to be used as proxies and, therefore, the compromise of a device connected to a network inevitably makes all other internal and external resources vulnerable.

[116] DDoS attacks, which can be performed through an increasing proliferation of malware-infected botnets and vulnerable servers that automatically generate further attacks against vulnerable targets, are aimed precisely at disrupting services, which – in the case of essential or digital services – is exactly what the NIS-D seeks to prevent.

[117] Ellyne Phneah, *M2M Challenges Go Beyond Technicalities* (19 June 2012), available at: http://www.zdnet.com/article/m2m-challenges-go-beyond-technicalities.

[118] European Telecommunications Standards Institute, ETSI TS 103 645 v1.1.1 (2019-02): CYBER; Cyber Security for Consumer Internet of Things (2019), available at: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

transmitted by and between IoT-connected devices and services.[119] Further security measures and best practices which should be considered include those within **ENISA's guidelines on Good Practices for Security of Internet of Things.**[120]

4 Covid-19 Pandemic – A New Crisis In Privacy

The 2020 pandemic created a **hitherto unforeseen environment where the dependency on digital information, data privacy and IT security were of paramount importance**. Whilst physical human contact was reduced, the usage of digital communications and exchange of data exploded at an unprecedented rate. People were forced to work from home without much prior notice. Business and organization data was migrated from IT secure systems to personal devices. Families relied on digital means of communication to maintain social ties. The elderly found themselves needing to adapt to such means of communication to keep in contact with loved ones. Government struggled between controlling the pandemic, enforcing measures to protect citizens but faced with the issues surrounding data privacy. **The combination of these requirements and behaviours led to paradigm shifts which raised weakness and threats which thus far did not exist.** With sudden limits on personal movement, work-place shifts, health reporting, health tracking, data privacy became an even more sensitive and important topic to address.

4.1 Survey on Privacy Risks Related to Covid-19

In July 2020, in the early stages of the pandemic, Cyberwatching.eu partners generated an online survey in the context of Covid-19 on Cybersecurity and Privacy, in order to understand the change in social interactions and at the same time understand the society's opinions on the risks of sacrificing some of their privacy for the public interest,[121] which also focused on the Covid-19 contact tracing apps. The survey is attached as Annex 1.

Through this survey, Cyberwatching.eu was also able to collect information relating to the society's acceptance of the sacrificing of their privacy, and whether they deemed it as a justified approach. The fact that cybersecurity services in the health-care sector are directed towards citizens cannot be ignored, thus the response of individuals will be used as an indicator of the risks of cybersecurity services from the perspective of citizens. **In Covid-19, citizens realised that our ability to exist relies on electronic communications and it has been insightful to analyse the responses**.

4.1.1 Dissemination of the Survey

The survey was widely distributed as follows:

[119] Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things* (16 September 2014, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf), p. 9. See also, generally, European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* (19 November 2018), p. 37 (PS-10), available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

[120] European Union Agency for Network and Information Security, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing* (19 November 2018), available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

[121] The survey can be found at the following link: https://cyberwatching.eu/online-survey-cybersecurity-and-privacy-Covid-19 or in Annex 1.

- AEI sent the survey to 210 email addresses from 196 different Cyber and ICT clusters
- AEI sent to their 70 members.
- AEI through twitter (+3100 followers)
- Digital SME through their social network
- CONCEPTIVITY to ECSO partners to ± 230 companies via their newsletter
- CONCEPTIVITY through LinkedIN, ± 7000 contacts
- CONCEPTIVITY to EOS - published in the EOS newsletter
- CONCEPTIVITY through personalized messages
- Cyberwatching.eu web site's portal contained the survey for 8 months
- ICTLC through their social network channels (Twitter, and LinkedIn)
- ICTLC through their newsletter and news blog
- TRUST-IT to the Concertation list (± 43 contacts)
- TRUST-IT to the contacts from H2020 projects database, some ± 150 project contacts

4.1.2 Response to Survey

A total of **83 citizens responded to the survey**. As seen in Figure 1, the survey responses covered not only many European Member States, but also international responses from countries like Japan, the United States of America and Saudi Arabia. This can be interpreted as a positive attitude and interest of stakeholders, both in Europe and internationally, to understand how societal perceptions have changed as a result of Covid-19.

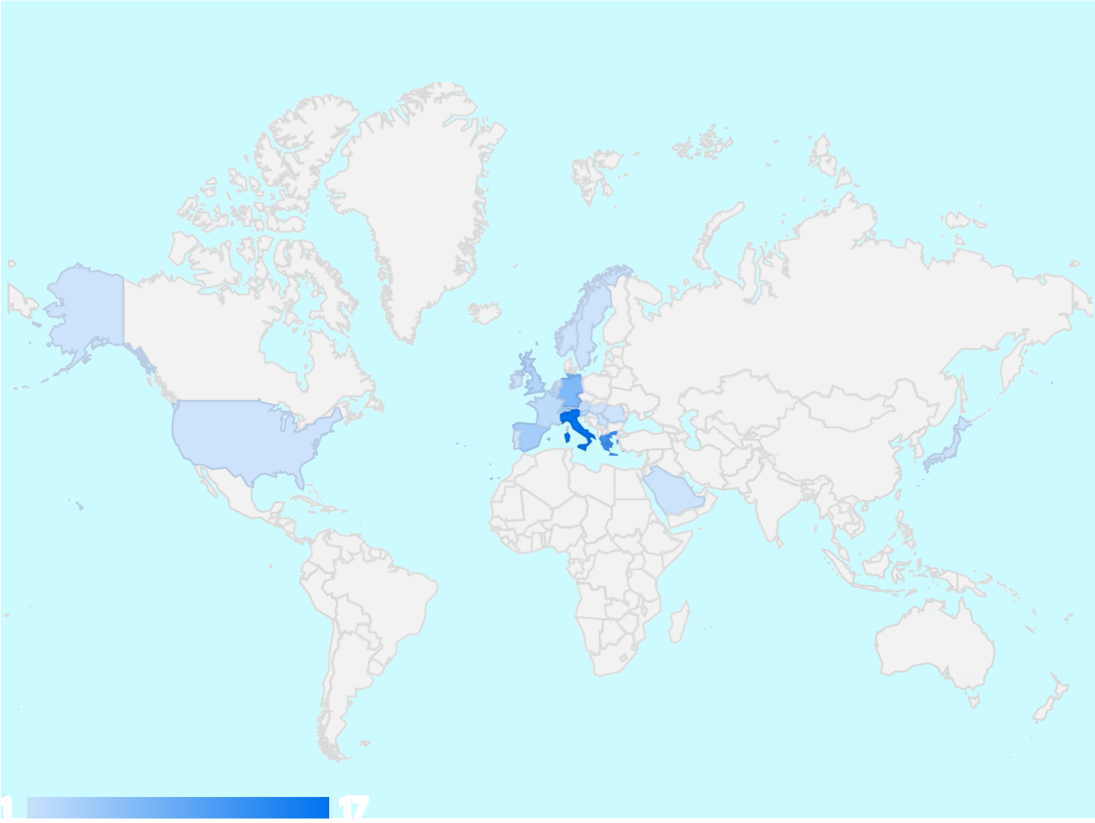


Figure 1: Response to survey by country

4.2 Challenges of Covid, Contact Tracing Apps and Privacy

Largely, the positive and wide response was also reflected in the results of the survey. It was easy to observe openness and flexibility towards the idea that, during Covid-19, privacy is relative. The following addresses the findings from the survey, with conclusions or recommendations, as applicable.

4.2.1 European Landscape on Contact Tracings Apps and Privacy

According to the European Commission, **twenty one out of the twenty-seven European Member States have deployed a contact tracing app in their country**.[122]. According to the latest publicly available information two more countries are currently developing a contact tracing app, while four countries are not foreseeing the deployment of a contact tracing app.

These facts emphasize that contact tracing apps have become the norm, considering that the pandemic continues to evolve in the European continent. Therefore, **this deliverable's scope has been slightly re-targeted in order to support the European cybersecurity services to understand what the risks are in the current situation, and what recommendations can arise in order to improve**. The Cyberwatching.eu consortium approached these risks by trying to understand the citizens' perspective towards contact tracing apps in order to identify the risks that remain unclear or important from the perspective of society.

Based on research, there are several protocols that can be found in the current digital contact tracing app market.[123] Although many kinds of contact tracing apps exist this research illustrates three different protocols.

Protocol 1 consists of the app recording its own location, and once a user is reported as being infected, their trajectory is sent to the authority.[124] The authority in hand would then share the pseudonymous trajectories of all infected users with every user, which would require each user to check whether they were in close contact with an infected individual. **The second protocol** relies on the broadcasting of a unique identifier through Bluetooth, so that when two phones are in close proximity, they can exchange identifiers. If a user is infected, the authority would contact all users that came in close proximity through their unique identifier. Lastly, **the third protocol** considers a similar broadcasting of a unique identifier via Bluetooth which is reset every hour. In this case, if two phones came in close proximity, they would exchange identifiers; and if one user was infected, all identifiers that they have used would be sent to the authority. The authority would then share the identifiers of all infected users with every user, and users would check if they encountered one of these identifiers. This research was used

[122] Specifically, that includes Austria, Belgium, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Slovenia, Spain. More details could be found here: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en.

[123] Yvyes-Alexandre de Montojoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin, *Evaluating Covid-19 contact tracing apps? Here are 8 privacy questions we think you should ask,* available at: https://cpg.doc.ic.ac.uk/blog/pdf/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask.pdf.

[124] Yvyes-Alexandre de Montojoye, Florimond Houssiau, Andrea Gadotti, Florent Guepin, *Evaluating Covid-19 contact tracing apps? Here are 8 privacy questions we think you should ask,* available at: https://cpg.doc.ic.ac.uk/blog/pdf/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask.pdf, p.2.

as an example in order to question the extent to which data protection can be guaranteed during the development and deployment of such apps. It is an interesting approach that could be further enhanced in order to help app developers and stakeholders create contact tracing apps according to data protection by design and by default. In addition, **the EDPB has published useful guidelines for contact tracing applications, which can be used as a baseline for the developing of cybersecurity services in this context**. [125]

According to independent research on contact tracing apps[126] requested by the Dutch Ministry of Health, one of the main conclusions was that all of the contact tracing apps available in the Dutch market struggle to comply with the GDPR.[127] The Dutch Ministry of Health required for solutions to meet the principles including: anonymity (untraceable to individuals) of the data processed, accuracy (minimizing false positives), data minimization, disclosure (strict data sharing policy), purpose limitation (process of source and contact tracing is the sole purpose or processing), transparency (including the ability for users to report errors and vulnerabilities), security, deletion (when the contact tracing app is no longer needed, the data should be deleted), and lawfulness (GDPR compliance).

The **results of the research** both identified gaps for contact tracing apps, but also confirmed their (potential) compliance with several principles. On one hand, the **principle of anonymity could not be guaranteed** by any of the apps, and the **principle of accuracy seemed to be dependent on the strength of Bluetooth connections as well as on whether the user and their device were in the same location**. On the other hand, **data minimization and purpose limitation were both respected** by storing minimal information of the device and for the envisaged purpose (of contact tracing). The disclosure of the data had a tendency to be based on the user's consent, and the legal basis of apps processing pseudonymized data was Article 9 (2) of the GDPR and Dutch requirements of the Public Health Act. Lastly, all **contact tracing apps had the potential to meet both the transparency principle and the principle of data deletion**.[128]

The above conclusions indicate that although contact tracing apps in the Dutch market have potential to be compliant with the GDPR, there are certain principles that must be more carefully evaluated and implemented, including the principle of anonymisation, and the principle of accuracy.

In congruency to the results of the Dutch Ministry of Health, **the need for guidance on contact-tracing apps has been recognised on the supranational level**. Several

[125] European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, p. 11.

[126] Specifically, the analysis was carried out on the responses to the Ministry of Health's invitation to the market for proposals for smart digital solutions for contact tracing during the Covid-19 pandemic.

[127] Juridische analyse - advies Autoriteit Persoonsgegeven inzake de DPIA van de CoronaMelde, available in Dutch at:
https://www.rijksoverheid.nl/documenten/publicaties/2020/04/19/samenvatting-privacy-analyse-contactonderzoeksapps.

[128] Note that the adherence of the security principle was left to be addressed by an independent report carried out by security experts.

international and EU institutions have published reports[129], guidance[130], guidelines[131], recommendations[132], best practices, conditions and obligations applicable to contact tracing apps. Nevertheless, since health-related data is a category of personal data that allows for further specifications and limitations [133] on the national level, many Data Protection Authorities have published their own set of conditions and guidance for providers of contact tracing apps to follow.

Data Protection Authorities of Europe have supplemented the European guidance in order to provide the national data protection requirements and best practices when processing personal data in the context of contact-tracing and tracking applications. In fact, the Consortium has collated the various guidance on processing of personal data during the Covid-19 pandemic, as well as on the topic of contact-tracing, in the News section of the website – which serves as a knowledge mapping of some of the main official resources,[134] and that includes many published reports not only from Europe but also from countries all over the world.

Nevertheless, it has been observed that the use of contact tracing apps is dependent on the people's perception of their risks and social preferences, rather than in the possible benefits to society and public health.[135] Several research initiatives have shown that, on the one hand, the widespread adoption, and on the other, the efficiency of the contact tracing apps remains relatively low.[136]

4.2.2 Findings from the Survey with respect to Contact Tracing

The online survey on Cybersecurity and Privacy also placed focus on the Covid-19 contact tracing apps, and results illustrated that when it comes to contact tracing / tracking applications, which are specifically introduced by the government or a public authority, **62% of the respondents' governments had a governmental tracing or tracking app**. The respondents with the highest positive responses came from countries including Italy, Austria, Germany, France, and Switzerland. Nevertheless**,**

[129] The European Data Protection Supervisor has published a Report #TechDispatch #1/2020 on Contact Tracing with Mobile Applications, which is available at: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en.

[130] The Organisation for Economic Co-operation and Development (OECD) has issued several recommendations on "Tracking and Tracing COVID: Protecting privacy and data while using apps and biometrics", available here: https://read.oecd-ilibrary.org/view/?ref=129_129655-7db0lu7dto&title=Tracking-and-Tracing-COVID-Protecting-privacy-and-data-while-using.

[131] The European Data Protection Board has published Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak, available here: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en.

[132] The European Commission has adopted a Recommendation to support exit strategies through mobile data and apps; and a Recommendation on apps for contact tracing, available here: https://eur-lex.europa.eu/eli/reco/2020/518/oj.

[133] Article 9 (4) GDPR, "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

[134] Note that due to the speed and number of updates or new publications on the topic, there is no presumption of completeness of this list.

[135] Yves-Alexandre de Montjoy, Tarun Ramadorai, Tomasso Valletti, and Ansgar Walther, *A simple Theory of Contact Tracing Applications*, Imperial College London, September 2020, p.8, available at: https://imperialcollegelondon.app.box.com/s/ojm4rryi15mua3p52zpas93heucd2qm0 .

[136] SensorTower, *Covid-19 Contact Tracing Apps Reach 9% Adoption in Most Populous Countries*, July 14, 2020, available at: https://sensortower.com/blog/contact-tracing-app-adoption, and Rodríguez, P., Graña, S., Alvarez-León, E.E. *et al. A population-based controlled experiment assessing the epidemiological impact of digital contact tracing*. Nat Commun **12,** 587 (2021). https://doi.org/10.1038/s41467-020-20817-6.

only 50% of the citizens that had an available contact tracing app actually used it. It is also worth noting that out of the 21 countries that have a contract tracing app currently, 20 have the **potential** to become interoperable but only 50% of them are actually interoperable. Interestingly, the majority of the respondents (79%) did not feel that they sacrificed their privacy during Covid-19 although only 21% of the respondents felt they had sacrificed their privacy, another 29% did not use the very app because it could potentially compromise their privacy. This means that even if they did not explicitly feel that their privacy was being sacrificed, a large proportion of the respondents did not actually use contact tracing app. It is worth noting that out of the respondents that felt they had sacrificed their privacy, **70% of them thought that this sacrifice was not justified.** The reasoning of those respondents was that privacy violations lead to violations to their freedom, and abuse of their personal data by enforcement or by the government.

Further, only 12% responded that the tracing app was mandatory to use, or that it was mandatory during the peak of Covid-19. At first glance, the voluntary nature of the application may be a non-privacy related reason for which the respondents did not use the tracing app. However, when asking participants the reasoning for not using the tracking app, the response was overwhelmingly that it **related to privacy and movement tracking concerns**. One participant even compared the contact tracing app with "big brother", which may be a hyperbole, but nonetheless, it emphasized the lack of trust of the participant towards the contact tracing app. The fact that 12% of respondents mentioned that the tracing app was mandatory, also goes against the recommendations given by the EDPB to ensure that the use of contact tracing applications should be voluntary.[137] Specifically, the EDPB notes that voluntary adoption is the only way with which systematic and large-scale monitoring of location and / or contacts, which is a “grave intrusion into their privacy”, can be legitimized.[138]

On the question of whether the respondents’ trusted that their government or public authority protected the personal data they shared or would share through the contact tracing app, the results were concerning. Almost half of the respondents, to be precise, **two in five (42%), did not trust that their government would protect their personal data**. As has been mentioned by the EDPB, data protection is “indispensable to build trust”, as well as to create the conditions for social acceptability of solutions such as contact tracing apps.[139] Therefore, the lack of public trust may also be reflected in the eventual success of these apps.[140] In addition, 38% of respondents were concerned that during the Covid-19 crisis their personal data would be controlled or monitored by the government. One participant mentioned that when tracking individuals, the linking of data sets should be ensured. For example, administrative data (such as age, or localization) should be separated from health-related data (such as other underlying diseases).

In conclusion, contact tracing apps may at the moment be widely available in Europe, however their **adoption remains doubtful (50%)**. In addition, although most did not

[137] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[138] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[139] Paragraph 3 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[140] Achieving Privacy by Design in Contact Tracing Measures - Global Privacy Assembly, available at: https://globalprivacyassembly.org/contact-tracing-statement.

feel like their privacy was sacrificed through the contact tracing app, those that did felt that it was not justified. This can be further explained by the fact that many respondents did not trust that their government would protect their personal data. Nevertheless, **there are steps that can be taken by service providers and developers to improve their compliance posture**. The EDPB points out that the principle of data minimization and data protection by design and by default should be carefully considered. [141]

4.3 Challenges of Covid, GDPR and Health Information

4.3.1 GDPR and Health Information

Health-related data under the GDPR is considered a special category of personal data, which requires a specific mandate in order for the processing to be compliant with data protection rules. Within the context of the legal grounds that are available, the processing of health data could be relied on the necessity for reasons of public interest in the area of public health, in accordance with the conditions of Art. 9 (2 (i)) GDPR, for healthcare purposes, under Art. 9 (2(h)) GDPR, and under certain conditions with explicit consent (Art. 9 (2(a)) GDPR). [142]

4.3.2 Findings from the Survey on Privacy of Health Information

As a result of the ongoing pandemic, the collection and use of health information became widespread [143]. For this reason, the survey contained questions related to the perception of citizens with regard to their health data during Covid-19.

From the results of the survey in this respect, **half of the respondents (52%) had concerns about the privacy of their health records**, while 38% did not have any concerns, and 10% did not know whether they had any concerns. It is clear that more respondents were worried about their health records, than not. In observing the number of individuals that had to provide health information to their employers, 70% did not have to. Although this is an encouraging percentage, there were different types of health information that employees had to disclose to their employer. On the one hand, some employees disclosed merely whether they were "fit for work". On the other hand, a number of employees stated that they had to disclose when they were infected by Covid-19, to provide a negative test of Covid-19, or to confirm that they are free of symptoms and had not been in contact with confirmed Covid-19 cases. While other respondents had to disclose their temperature or certain health information before entering the office. The most concerning privacy invasion observed was arguably the need to "report daily" their state of health, including fever, pains and Covid-19 related symptoms. In addition to the employment context, respondents were also asked whether they provided health information to other organisations. The majority of the respondents, and precisely 64%, did not provide health information to other organisations. Even so, the fact remains that **29% had to share health information with other organisations**.

[141] Paragraph 24 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[142] Paragraph 33 of European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak.

[143] World Health Organisation, Covid-19 significantly impacts health services for noncommunicable diseases: available at: https://www.who.int/news/item/01-06-2020-Covid-19-significantly-impacts-health-services-for-noncommunicable-diseases.

The most concerning aspect of this section was a question on whether their doctor had adequately informed them on their data's cybersecurity, in which **4 in 5 respondents answered negatively (79%)**. The reason for the lack of adequate information on the cybersecurity of the respondent's data is unclear. However, it **emphasizes a lack of awareness of data protection by health professionals, and a clear need for training that focuses on delivering adequate information to patients** when it comes to health-related data. It seems improbable that doctors would have appropriate security measures implemented and would not mention these to their patients, especially during distressful times when privacy is at stake. Therefore, it can be inferred that appropriate security measures may be lacking entirely. The second recommendation that can arise **from this feedback is for cybersecurity tools and services to allow for customisation by health institutions in order to guarantee data protection to special categories of personal data** (such as health data, biometric data, and genetic data).

These concerns were expressed further on a broader question on other concerns the respondents may have had regarding their health data. One of the main issues was that hospitals, doctors and medical practitioners "do not care" about privacy, and do not have any "knowledge about IT and data security". A very frequent concern was that their health data could be used for commercial purposes, for example to analyse their eligibility for health insurance. Throughout the responses, this recurrent trend that the practices of health personnel are not up to date with the legislations on data protection compliance is worrisome. One respondent noted that "in most case the [medical] systems are maintained by external service providers whose focus is on function and not security". This point goes hand in hand with the above recommendation **on the need for cybersecurity services that will have personal data as a main priority, by design and by default**. This will both support the health-care sector, by guaranteeing adequate security measures, as well as help raise awareness on the need to inform patients about the security of their data, and how they can exercise their rights.

The last concern, which wraps up the aspect of security in the health-care sector, is that of cybersecurity attacks. **Several participants in the survey mentioned ransomware attacks and that their repercussions are a major concern**. One participant from France mentioned that two months following surgery at a private clinic, they randomly found out that a hack had occurred in the clinic's network. The respondent demonstrated disappointment at not having been informed by the health-care clinic directly, instead of the newspaper. Another respondent complements this point by explaining that ransomware attacks are used as means to blackmail data subjects' data on psychological treatments.

4.4 Challenges of Covid, GDPR and Personal Data Collection

4.4.1 GDPR and Personal Data Collection

The responses to Covid-19 have varied across the world, however one similarity can be observed above all, that of “harnessing the power of data” to develop effective tools and measures.[144] Data collection has come at a turning point as both governments and private entities heavily rely on data access to ensure public safety and business

[144] OCED Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14 April 2020, available at: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ .

continuity, respectively. [145] The GDPR can help ensure that any personal data processed in the context of the pandemic is done in a compliant, and lawful way.[146] This extensive data collection may introduce challenges that impact citizens, their perception of their privacy (or lack thereof), and their feelings towards entities processing their personal data.

4.4.2 Findings from the Survey on GDPR and Personal Data Collection

Following on from the above, an open question was asked on what the respondents' concerns were regarding personal data collection in the context of Covid-19. The responses varied from ideological concerns, to cybersecurity and privacy concerns. Some respondents stated that **their concern was sharing data with third parties**. While several respondents' concern was **the use of their data for different purposes, the abuse of the initial purpose unintentionally, or further processing their data**. This concern is parallel to a violation of **purpose limitation**, whereby the GDPR states that any data controller must collect and process personal data for a specified, explicit and legitimate purpose. The voiced worries concerned both the legitimacy of the purpose - for example violations to a legal processing of their tracking data, as well as the specified and explicit criterions of the principle. These concerns can be grouped towards **a broader risk of privacy relating to tracking apps**.

Along those lines, there were also worries regarding the **use of the tracking information to record their associated habits, routines and interests**. This could be considered a concern against them being profiled by the government or public authority. It is important to ensure that the citizens understand that the transparency of their applications is of utmost importance. It is worth noting that it seems some citizens believe that statistics and aggregated data analysis may consist of personal data, which by default is not the case. Another common concern among respondents was **cybersecurity-related attacks** that could compromise their privacy, freedom and physical security, such as maliciously collecting and processing their tracking data. This is in line with the above recommendation in which cybersecurity services can offer guarantees, namely, by ensuring that **an appropriate management of cybersecurity attacks is available to the healthcare systems**.

A less common concern was relating to the **violations of liberality and freedom**, which was also expressed as the tracking of border crossings and app proximity tracing. This considers the more ideological, constitutional and human rights concern of citizens' regarding their general freedom of movement. Interestingly, participants overwhelmingly noted that they feel that other apps could be tracking their movements too, including Google Maps, Google, Facebook, WhatsApp, LinkedIn and Instagram.

When respondents were asked whether they felt an increasing need to have control of their personal data during this time, an overwhelming majority (78%) responded positively. In addition, **60% of the respondents felt greater appreciation of the laws on privacy and data protection after the Covid-19** pandemic rolled out.

[145] OCED Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14 April 2020, available at: https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/ .

[146] Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, p.1, available at: https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf .

A major concern was the sharing of information with a third party, the use or abuse of such data for malicious ends. These concerns could be grouped in a broader context relating to tracking apps. This is in line with the above recommendation in which cybersecurity services can offer guarantees, namely, by ensuring that **an appropriate management of cybersecurity attacks is available to the healthcare systems**.

4.5 Challenges of Covid, Privacy and Transparency

4.5.1 Privacy and Transparency

The principle that has significant impact to the data subjects' perception of their privacy is that of transparency.[147] As mentioned in Section 3.2.3, under the GDPR's principle of transparency,[148] controllers are required to provide data subjects with clear information as to their activities involving the processing of personal data, under, e.g., Arts. 13 and 14 GDPR. The EDPB has re-emphasised the need for data subjects to receive transparent information during the pandemic, including the main features of the processing, the purposes and the retention period of the processing.[149] However, in the Covid-19 pandemic, as a result of the urgency of processing data, complying with regulations and implementing protection controls for protecting citizens nationally was very challenging.

4.5.2 Findings from the Survey on Privacy and Transparency

Interestingly, **almost half of the respondents now have higher expectations from privacy policies, as opposed to the time prior Covid-19**. Out of the 43% that now have higher expectations from privacy policies, thought-provoking recommendations have been suggested with regards to their expectations.

The most repeated response **suggested a higher need for clarity on the steps to exercise data subject rights**, as well as more straightforward ways to track data flows. This point also relates to the abovementioned need for more **interoperability** between tracking applications (for example, if one is under quarantine in Italy, if they travel to France, they can transfer the relevant data to the application used in France). However, the concentration on these type of expectations among participants suggests that guidance and clarity by cybersecurity services on the techniques, technical means and tools for exercising data subject rights is integral during the extraordinary times of the pandemic. Along these lines, another expectation mentioned was the ability to customize privacy settings. Thus, the feedback received from respondents **further increases the necessity for cybersecurity services to focus on appropriate means for data subjects to exercise their rights in the field of healthcare applications, software, as well as embed privacy settings customization, where possible**.

The second most common response asked for **enhancement and explanations of the safety measures**. This is another concerning point since it can be interpreted as

[147] Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, p.6, available at: https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 .

[148] Art. 5(1)(a) GDPR.

[149] Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, p.2, available at: https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf .

a gap of comprehensible communications towards data subjects when it comes to the security of their data. As has been observed by the ENISA, malicious actors have been taking advantage of the pandemic to launch **phishing campaigns and ransomware attacks in the healthcare sector**.[150] One respondent specifically referred to the Covid-19 pandemic as a time where more private data was collected than before, and accordingly "a more sensitive handling of this data is required". The expectation of better explanations of the security measures may be due to the fact that data subjects consider the variable of Covid-19 as a reason for the collection of more sensitive type of personal data **and thus the need to understand the type of security measures is further highlighted.** In addition, another respondent pointed out that protection of the reputation of data subjects is integral during Covid-19, which further increases the expectations for appropriate security measures. More specifically, a respondent mentioned that the explanation of the "design of security measures" could be useful. Therefore, the mere inclusion of a list of security measures is not considered acceptable by data subjects during the pandemic. The recommendation that arises from this feedback is that **enhanced explanations of the implemented security measures within privacy policies is crucial**.

Another frequent response requested a **clearer explanation of privacy-related risks**. It can be observed that the risk-based approach of the GDPR remains important during the pandemic, also on the side of the data subjects. The privacy-related risks are exacerbated by the current pandemic, especially since the risks that could materialize could be unlike what the data subjects may be more familiar with, both in terms of their nature and consequences. One respondent expressed the need to protect the reputation of the data subjects. Linked with this concern is the expectation for "non-invasive privacy by default". The cybersecurity services can be of assistance, by offering privacy by default to the healthcare systems, software, and applications used. The recommendations towards the stakeholders are to ensure that **privacy-related risks are explicitly communicated to the data subjects**. In addition, cybersecurity tools and services can use privacy by default as a vehicle to both carry out a proper risk-assessment of the processing activities in the healthcare sector, as well as explaining the said privacy risks to the data subjects.

5 Cyberwatching.eu Initiative: Cyber Risk Temperature Tool

5.1 Description of the Cyber Risk Temperature Tool

In view of the updated EU Regulations requirements as explained in Chapter 2, followed by the challenges in emerging technologies as explained in Chapter 3, cyberwatching.eu initiated the creation of **a tool to assist SMEs in understanding the real situation about their cyber security environment**. The main objective of this tool is, therefore, to provide SMEs with a preliminary assessment of its cyber security readiness in a cost-effective manner. By means of a short but complete questionnaire, an SME may obtain a preliminary evaluation of its cyber security readiness in a cost-effective manner and thereby, consider undertaking actions that would be necessary in order to enable it to become more resilient. Ideally, the questionnaire should be completed by the person with the most technical skills within the company. The full questionnaire is provided in Annex 2.

[150] European Agency on Cybersecurity, Cybersecurity in the healthcare sector during Covid-19 pandemic.

5.2 Structure of the Questionnaire

The questionnaire consists of two main parts. In the first part, the respondent is asked to provide a personal assessment of the IT level of security within the company. In the second part, the respondent is asked questions of a more specific and technical nature. Through the attribution of a score, the SME is placed in one of the following profiles (in the order of *severity*):

- Low vulnerability;
- medium-low vulnerability;
- medium-high vulnerability;
- high vulnerability.

Thus, the evaluation is performed through a set of questions that are based on the need to analyse the company through different areas, such as:

- Specific knowledge of the cyber security readiness within the company;
- the methodologies followed within the company;
- the distribution of administrative fees on the systems;
- the information segmentation policy;
- authentication policies for access to corporate systems;
- other assessments previously carried out.

The afore-mentioned topics were selected because they were considered as the starting point and as essential for a careful analysis in terms of cyber security.

5.3 Methodology

As mentioned above, the interviewee is required to complete a questionnaire consisting of **two distinct parts**: the first part represents a **self-assessment** evaluating the cyber-risk vulnerability rate of the company, whereas the second part, based on few questions, seeks the **real data regarding that very rate**.

More specifically, the first three questions work on a rating system: the interviewee is required to provide a self-evaluation with a rating from 1 to 7, where 1 indicates the lowest value and 7 the highest.

For each answer:

- 4 points are assigned to interviewees who provided the values 1, 2 or 3;
- 8 points are assigned to those who provided the value 4;
- 16 to those who select 5;
- 20 points are assigned to the values 6 and 7.

The second part of the questionnaire consists of eleven questions, including some sub-questions, which represent a real and objective evaluation. In these cases, just one option is provided:

- for each answer, a value from 0 to 10 is assigned,
- rating the possible options from the best to the worst.
- In a particular situation, 15 is the value assigned to answers which reflect a notably severe situation.

Once the questions are completed, the tool calculates the final score, which is obtained by averaging the scores of each question in both parts of the questionnaire.

5.4 Explanation of Scores

For the **first part** of the questionnaire, four scoring ranges have been created, and for convenience **are numbered from 1 to 4**, where 1 indicates low confidence in one's computer security (1- |6) and 4 indicates high confidence in one's computer security (18- |20).:

Self-assessment	
Low confidence in your IT security (1-6),	1
Medium-low confidence (6-12),	2
Medium-high confidence (12-18),	3
High confidence (18-20).	4

Table 2: Cyber Risk Temperature Tool – Self-assessment score

The definition "*Confidence in own cyber security"* means how the respondent assesses their cyber security readiness. This is important because each person takes decisions regarding cyber security issues based on his or her individual assessment of corporate cyber security.

Although this is important, it does not mean anything on its own. It is included in a matrix with the results obtained from the answers to the questions in the **second part** (average of the scores obtained), also divided into 4 ranges:

Rating	
Low vulnerability (0 ≤ M ≤ 3),	1
Medium-low vulnerability (3 ≤ M ≤5),	2
Medium-high vulnerability (5 < M ≤ 7),	3
High vulnerability (7 < M ≤ 12).	4

Table 3: Cyber Risk Temperature Tool - Rating score

When crossing the two axes, the matrix returns a scale from -3 to 3.

		Rating			
		1	2	3	4
Self-assessment	1	-3	-2	-1	0
	2	-2	-1	0	1
	3	-1	0	1	2
	4	0	1	2	3

Table 4: Self-Assessment Matrix

The returned scale from the matrix indicates the coherence between the subjective evaluation of the respondent and the objective evaluation of the company, an indicator of the **perception of the company's cyber security.**

Very under-estimated	Under-estimated	Slightly under-estimated	Consistent with self-assessment	Slightly over-estimated	Over-estimated	Very over-estimated
-3	-2	-1	0	1	2	3

Table 5: Indicator of company's cyber security

5.5 Explanation of Results

While evaluating the vulnerability rate, the perception must be considered as an added factor.

The tool will return the description of **the vulnerability range and in addition the value of perception**. The possible combinations that can be obtained are the following:

Profile 1[151]**:** Congratulations, your company has **Low vulnerability** and your perception of cyber security […][152] The real situation:

> As a result of the carried-out assessments, your company has proved that it fulfils the main requirements demanded for adequate cyber security. You are recommended to keep updated on cyber security issues at all times.

Profile 2: Your company has **Medium-low vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company only partially meets the main requirements for adequate cyber security. You are recommended to keep updated on cyber security issues and consider contacting a cyber security expert for a more in-depth evaluation.

Profile 3: Attention! Your company has **Medium-high vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company does not meet most of the main requirements for adequate cyber security. You are recommended to contact an expert in the field who can provide you with adequate support to identify and mitigate the vulnerability.

Profile 4: Attention! Your company has **High vulnerability** and your perception of cyber security [...] The real situation:

> As a result of the assessments carried out, your company does not meet the main requirements for adequate cyber security. You are strongly recommended to urgently contact an expert in the field to mitigate your numerous vulnerabilities.

5.6 Testing and launch campaign

The Cyber Risk Temperature Tool was developed and implemented in August 2020. Before the official launch in October 2020, an internal testing phase was launched among the Consortium to spot possible bugs and improvements.

[151] Temporary name

[152] It is the value of your company's cyber security perception

The launch of the tool was accompanied by a promotional campaign which included the following:

- Landing page set up
- Promotion to Concertation mailing list (93 members)
- Social media promotion
- Newsletter to the cyberwatching.eu community (> 1000 members)

Another promotional campaign was launched in January 2021 (and is currently ongoing) with the help of the whole Consortium including a promotional article to be published on external sources and social media posts and images ready to be shared.

5.7 Analysis of results

As of now, the Cyber Risk Temperature Tool gathered 26 responses coming from the following countries:

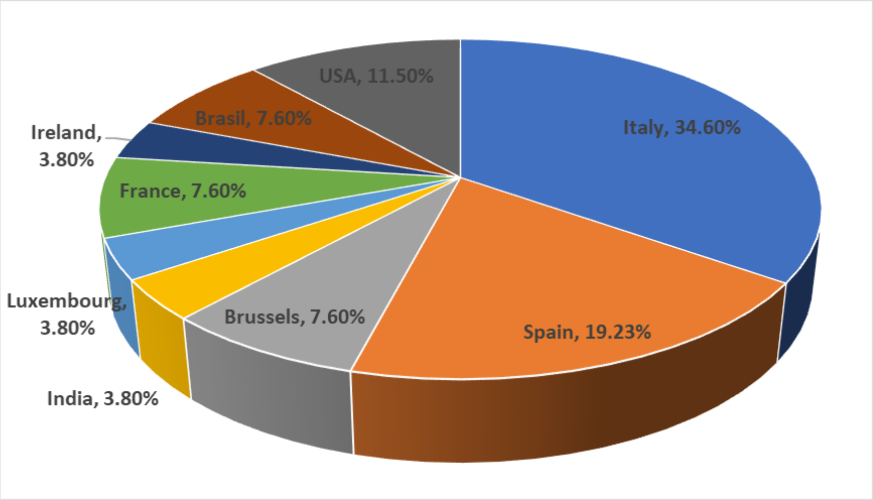


Figure 2: Cyber Risk Temperature Tool - Country breakdown

By analysing in depth, the responses of the questionnaires, the results show that the perception of companies concerning their cybersecurity assessment is for the vast majority that they are in a very good position with low vulnerabilities indicated, with 50% of companies indicating a slight underestimation and 26.6% indicating a perception in line with the assessment

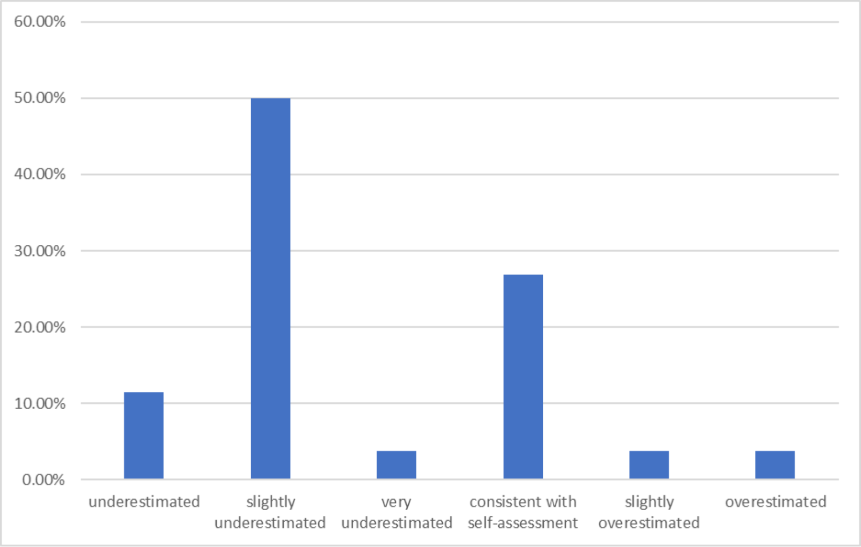


Figure 3: Cybersecurity perception analysis

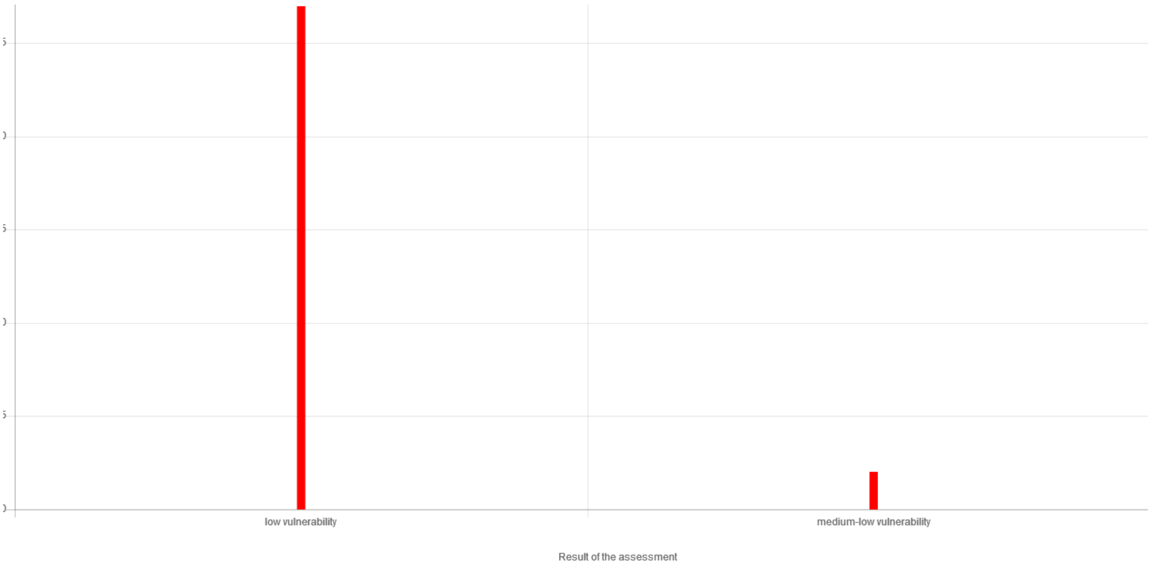


Figure 4: Cybersecurity vulnerability perception analysis

These findings are also backed up by the fact that the majority of respondents have a firewall in place to protect their devices and that they perform back-up of their data either every day (38%) or every week (18%).

It is important to note that 38% respondents indicated that their company is following best practices or frameworks (e.g. OWASP, NIST and COBIT) and also regularly carrying out training courses about cybersecurity.

6 Third Concertation Event

The Covid-19 pandemic led to many disruptions in 2020, and which continue in 2021. The third Concertation Event was originally foreseen in the second quarter of 2020. However, due to the pandemic and country-specific application of regulations, quarantine requirements and confinements, the Event was initially postponed until mid-Autumn 2020 with the hope that travel would resume normally in Autumn 2020. With the continued pandemic restrictions, and after several discussions within the Consortium on how best to resolve this situation, it was decided that the format of the Third Concertation Event would need to be virtual. Instead of holding a single virtual event, it was decided that a series of Webinars would be better suited and different topics could be addressed at intervals, thus avoiding the fatigue of continuous online concentration which has consumed the general method of work today. The following Webinars were, thus, organized:

- Effective Protection of Critical Infrastructures against Cyber Threats (29 October 2020)
- EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks (12 November 2020)
- Cybersecurity risk management: How to strengthen resilience and adapt in 2021 (23 November 2020)
- Security and Privacy by Design for Healthcare (10 December 2020)

6.1 Effective Protection of Critical Infrastructures against Cyber Threats

- Date: 29 October 2020
- Presentations & recording[153]
- Final report[154]

6.1.1 Summary

Critical infrastructure is a long-standing priority in Europe and globally. Critical infrastructure describes the physical and cyber systems and assets which are essential to maintain vital societal functions. This term has expanded over the years, originally from the transportation infrastructure to utilities, to include healthcare, energy and various manufacturers.

The threat landscape for critical infrastructure organisations is becoming more precarious with an increasing number of high-profile attacks taking place. This continues to evolve as the way in which people actually work changes, along with the number of connected devices increasing in many critical infrastructure environments. The situation has exacerbated with the Covid-19 pandemic with many workforces having to connect remotely. This development has, therefore, changed the definition of critical infrastructures by including also our personal equipment, in this arena, which magnifies the importance of supply chains, and the danger of its disruption, for instance, during the pandemic and the potential to cut all traffic.

Critical Infrastructures nowadays rely on advanced technologies and robust ICT components to efficiently manage the large amounts of data that are necessary for

[153] https://cyberwatching.eu/effective-protection-critical-infrastructures-against-cyber-threats
[154] https://www.cyberwatching.eu/publications/effective-protection-critical-infrastructures-against-cyber-threats

daily operations, communications, and in general, to provide different kinds of services depending on the specific sector of their activity such as energy, water, health, finance, transportation, among many others.

The high usage of technologies combined with the use of smart devices and different types of software and hardware makes critical Infrastructures a vulnerable target to every day more sophisticated attacks coming from hackers and cybercriminals. During September 2020, fourteen attacks were reported by the Centre for Strategic and International Studies (CSIS)[155] and all of them targeted critical Infrastructures not only from the European Member States but around the world (e.g. ransomware attack on a German hospital which may have led to the death of a patient; the French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks; and two sets of cyberattacks targeting emails of several members and employees of the Norwegian parliament and public employees in the Hedmark region).

The European Commission understands the importance of effectively protecting these infrastructures which provide essential services to citizens, hence their investment in innovative systems contributes to tackling this situation.

The Cyberwatching.eu webinar focused on how better cybersecurity is essential for protecting critical infrastructures and making them more resilient. The EU projects CyberSANE[156], CYBERWISER.eu[157] and ReACT[158], and the European Cyber Security Organisation (ECSO)[159] presented their ambitions and approaches to providing critical infrastructures with advanced systems for timely detection, monitoring, handling and treating different risks and attacks. Several recommendations were provided by the four speakers with an overview of what the cybersecurity challenges are in critical infrastructures, and some answers on how team-leading experts in Europe are collaborating, thanks to funding from EC to ensure that Europe's critical infrastructures remain resilient to cyberattacks. 233 participants joined the webinar and details on them will be included in D3.6 Report on Concertation activities.

6.1.2 Webinar programme

The outline of the seminar and the speakers is given below:

- Cyberwatching.eu Introduction and welcome note- Nicholas Ferguson, Cyberwatching Project Coordinator & Trust-IT Services
- Towards a trustworthy and resilient digital Europe - Roberto Cascella, ECSO
- CyberSANE: Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures - Spyros Papastergiou - CyberSANE & Maggioli
- Building cybersecurity training environment to protect ICT systems - Niccolo Zazzeri, CYBERWISER.eu & Trust-IT Services
- ReAct: REactively Defending against Advanced Cybersecurity Threats - Evangelos Markatos, REACT & FORTH-ICS

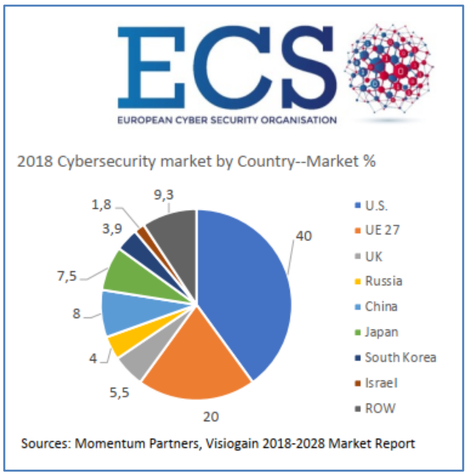
[155] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
[156] https://cyberwatching.eu/projects/1690/cybersane
[157] https://cyberwatching.eu/projects/963/cyberwisereu
[158] https://cyberwatching.eu/projects/1053/react
[159] https://ecs-org.eu/

6.1.3 Towards a trustworthy and resilient Europe

Roberto Cascella, ECSO
https://ecs-org.eu/

The global cybersecurity market is fast-growing with an estimated growth rate of €115 billion per market growth rate of more than 13% by 2022, based on the ECSO 2018 market analysis.

Europe is a market that is highly dominated by global suppliers from North America (40% as shown in **Error! Reference source not found.**), also in Asia such as China, Japan, etc., as most of the IT hardware and software products are built outside the European Union (often by European companies).



Sources: Momentum Partners, Visiogain 2018-2028 Market Report

Figure 5: ECSO 2018 Cybersecurity market analysis by country

One of the challenges is an important consideration of **how the IT hardware and software products that are built outside Europe are integrated.** This is because the non-EU products are integrated with the critical infrastructure in the European supply chain. Based on the ECSO market analysis the **European market** is quite large with €25 billion made up of about 12,000 supplier companies (74% of them are Micro and SMEs).

In another analysis carried out by the ECSO Working Groups, in Europe there are innovative solutions produced by SMEs and different companies, but **Europe still has a fragmented market**.

At the same time, there is an issue linked to the **growing sovereignty** (in particular after COVID) and the need for Europe to acquire digital autonomy. This is very important when looking at all the situations in Europe, also with respect to products and solutions that are coming from the third-party countries.

Given this complex scenario, different aspects need to be considered which are at stake, such as

1. Citizen privacy
2. Society
3. European values
4. Democracy
5. Awareness
6. National security sovereignty.

In terms of the economy, there is a need to have a clear economic recovery and digital autonomy to ensure that there is competitiveness in Europe. Finally, the increasing crime in Europe is mentioned in a press release[160] published by ENISA[161] in October 2020, identifying and evaluating the top cyber threats in Europe with an increase in Phishing, Identity Theft, Ransomware, Monetisation as the top motivations for cybercriminals, and the COVID-19 environment has increased the fuelling of attacks on homes, businesses, governments and critical infrastructure.

6.1.4 New challenges and objectives in Europe

6.1.4.1 Digital transformation

Cybersecurity is continuously evolving. Digital transformation[162] is the integration of digital technology into all areas of a business, fundamentally changing how a company operates and delivers value to its customers. It is also a cultural change that requires organizations to continually challenge the status quo, experiment, and become comfortable with failure.

In particular at the end of 2019, ECSO considered **digital transformation as one of the main issues in cybersecurity**. Digital transformation has made an impact both on society, not only on the economy but also on the infrastructure and how it operates, and for the democratic process here in Europe.

In February 2020, the European Commission published its digital strategy "A Europe fit for the digital age"[163]. The EU's digital strategy defines an ambitious approach towards digital technological development, as well as how technology will be used to meet the climate-neutrality objectives. It also shows the different aspects that should be taken into considerations, such as the European Industrial strategy link to the data strategy of SMEs and all the different technologies that will be key such as Artificial Intelligence (AI), Cybersecurity, High Performance Computing (HPC) and connectivity.

6.1.4.2 Green Deal

In December 2019, the European Green Deal (EGD)[164] set out Europe's new growth strategy that will transform the Union into a modern, resource-efficient and competitive economy. Its ambition is to overhaul many of Europe's economic sectors, most notably energy, transport, agriculture, goods production and consumption, and the housing stock. This initiative has an impact in looking for research, technology and industrial deployment of the cybersecurity solutions that are more energy featured.

6.1.4.3 Next Generation EU

In July 2020, the European Commission, the European Parliament and EU leaders agreed on a recovery plan that will help the EU emerge from the crisis and lay the foundations for a more modern and sustainable Europe. This initiative is known as the "Next Generation EU (NGEU)[165]" and is unprecedented as for the first time in its

[160] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020
[161] https://www.enisa.europa.eu/
[162] https://enterprisersproject.com/what-is-digital-transformation
[163] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en
[164] https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
[165] https://ec.europa.eu/info/strategy/recovery-plan-europe_it

history, it will support in repairing the economic and social damage caused by the coronavirus pandemic.

The Covid-19 pandemic has seen simultaneous disruptions to both supply and demand not only in Europe but also in an interconnected world economy. With this, there is a need for digital transformation to ensure that a resilient infrastructure in Europe has been accelerated even more by the Covid-19 situation.

While this is the case, the attack surface in terms of cybersecurity has changed as there are several workforces connected remotely and at the same time have integrated new technologies that pose brand new and possible threats with vulnerabilities.

6.1.5 Challengers ahead

6.1.5.1 Cyber resilient digital infrastructures

Complex scenario	Some challenges ahead
• High-availability and controlled performances in highly complex/heterogeneous technologies (HW/SW, real/virtual) • Presence of legacy systems/components and need to ensure security and privacy over mixed legacy and innovative technologies • Complex digital infrastructures lifecycle management process across all stakeholders (supply chain w/o central authority) • Heterogeneous regulatory scenario	• Real-time & situational awareness, automating mitigation / detection / response / recover • Securing the whole digital infrastructure lifecycle, including training, education and safety aspects • Innovation based on the integration of existing security/privacy components in legacy systems • Distributed decision making and collaboration solutions, e.g., orchestration services. • Secure virtualization technologies that are transversal to verticals

6.1.5.2 Deploying resilient digital infrastructures in the field

Complex scenario	Some challenges ahead
• Complex and cross-platform cyber-attacks / Threat management • Integrity and trustworthiness of communications and services • Virtualization and softwarisation of networks and network functions and the interconnection of different technologies • Complex trust models to address M2M interaction and to manage complex 5G infrastructures	• Increase trust in information sharing mechanisms through control and formal analysis of data and sensors • Design and implementation of new security mechanisms and automation of attack response mechanisms • Realistic, open-source and configurable tools and simulators to evaluate new security solutions

• Impact of current cryptographic schemes and migration to quantum-safe ones	

6.1.5.3 Main ECSO recommendations to the European Commission and Digital Europe Programme for a Cyber Resilient Europe

ECSO sent the recommendations to the Asian-European parliament because it is important to strengthen the cyber resilience in Europe at all different aspects.

- Support and protection of the European digital transformation – there is a need to support and have an EU vision for a European cybersecurity ecosystem based on EU values. Having a comprehensive EU cybersecurity strategy and approach in implementing the industrial policy by looking at the education, training, skills and awareness.
- There are issues that are linked to sovereignty recovery, socio/economic development, and Next Generation public private cooperation so there is a need to increase the digital economy. The above-mentioned needs to have clear support from the EU Legislations and Regulations, Private and Private Investments in Research, Capability Development and Capacity Building, and Strategic Alliance and Partnership for Trusted Supply Chains in Europe.

Concerning the activities that ECSO carries out, there is a particular ECSO WG that looks in particular at the cybersecurity challenges and trying to establish a new cybersecurity EU R&I roadmap with a vision to strengthen and build a resilient EU ecosystem, analysing the challenges of digitalisation of the society and industrial sectors to sustain EU digital autonomy by **developing and fostering trusted technologies.**

- **European R&I priorities**. ECSO has provided some scenarios and suggested priorities to the European Commission with respect to Horizon Europe and Digital Europe Programme (ECSO 2021-2027 technology vision of the future shaping society and industry).
- **Trans continuum (link across techno sectors with other PPPs).** Joint initiatives with other cPPPs in Europe (ETH4HPC, 5G, IA, BDVA, etc.) by looking the digital contingent, in the sense that nowadays there are emerging technologies such as IoT, AI, Blockchain, HPC, 5G that are pushing towards digital transformation, and are critical elements that are integrated into the critical infrastructures to identify global challenges and need to address them in a transversal and coordinated way.

Collaboration. Coordination with other PPPs, Jus, Pilots on Competence Centres, EC projects and other initiatives to monitor the evolution of the cybersecurity ecosystem and understand the gaps. Cooperation with EDA on cybersecurity for dual-use technologies.

6.1.6 CyberSANE: Cyber security incident handling, warning and response system for the European critical infrastructures

Spyros Papastergiou, Maggioli & CyberSANE
www.cybersane-project.eu

Over the past decade, Critical Information Infrastructures (CIIs) have been operating upon robust and reliable ICT components, complex ICT infrastructures and emerging technologies which are interconnected through complex networks, providing a high level of flexibility, scalability, and efficiency on the provided services and the supported processes. However, the increased usage of information technology in modern CIIs means that they are becoming more vulnerable to the activities of all kinds of malicious entities and individuals (e.g., hackers, terrorist groups, criminal gangs).

The above landscape puts the CIIs operators are under pressure to detect ongoing attacks and to combine and analyse all the threats related information and evidence effectively and accurately. However, the lack of appropriate tools to anticipate and handle complex cyberattacks in a way that takes into account the heterogeneity and complexity of their environments raise the need for improved monitoring approaches.

CyberSANE aims to contribute towards the emerging need to improve the level of prevention, preparedness, reaction and resilience to cyber incidents and threats of the CIIs. In order to meet its objective CyberSANE will introduce an innovative, Incident Handling and response system which support, the security officers and operators and guide them to recognize, identify, model, dynamically analyse, forecast, treat and respond to advanced persistent threats and handle daily cyber incidents utilizing and combining both structured data (e.g., logs and network traffic) and unstructured data (e.g. data coming from social networks and dark web).

6.1.6.1 Recommendations on cybersecurity priorities for the critical infrastructure domain

The Critical Information Infrastructures should incorporate:

- Security Monitoring and Analysis capabilities for preventing and detecting any kinds of anomalies, threats, risks.
- Social Information Mining capabilities to extract data from distributed online web sources offering to the security operators' information on activities and situations that can become a threat to the infrastructures.
- Data Fusion and Event Management capabilities to provide the intelligence needed for an effective and efficient analysis of a security event.
- Risk Evaluation capabilities to thoroughly assess the vulnerabilities of their interconnected cyber assets and to continuously estimate the probability of all possible cyber-attacks.
- Threat Intelligence capabilities to facilitate and promote the secure and privacy-aware sharing of incident-related information.

6.1.7 Building cybersecurity a training environment to protect ICT systems

CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity

Niccolo Zazzeri, Trust-IT Services & CYBERWISER.eu
www.cyberwiser.eu

This part of the webinar began with an overview of how COVID-19 pandemic has changed the way many businesses operate, compelling them to find different solutions, shifting working environments and amplifying a lot of the challenges organisations were already facing.

As organizations around the world struggled to adapt to a strictly remote workforce, cyber-criminals intensified their attempts at gaining access to sensitive and valuable data by using different techniques such as social engineering techniques, malware, phishing etc. This context continues to drive a rapidly growing need for well-trained cybersecurity professionals. Yet supply is not meeting the demand for skilled professionals in this field. This reflects a shortage of cybersecurity professionals worldwide which is expected to grow to 3.5 million in 2021.

While the provision of training and educational courses is increasing, it is not sufficiently available to fill entry-level cybersecurity vacancies in the market, both in terms of non-technical preparation and technical training for specialist cybersecurity positions. On top of this, IT teams are overwhelmed by the sheer number of threats and issues they have to deal with on a daily basis.

This is where CYBERWISER.eu comes into play. CYBERWISER.eu delivers a flexible, risk-centred, capacity-building platform, combining a theoretical and practical approach to cybersecurity with innovative features including a cutting-edge cyber range. CYBERWISER.eu implements customisable training pathways in cybersecurity to fit a broad range of needs and capacity building targets, from juniors like a threat and vulnerability analysts all the way up to information security risk manager and CISOs can all benefit from using it.

The CYBERWISER.eu Platform has been validated by three full-scale Pilots covering three different domains (FSP#1 higher education, FSP2# transport and FSP#3 energy) who have used it to increase their students' or employee's skills on specific topics such as SQL Injection, Cross-Site Scripting, Phishing, Session Hijacking etc.

CYBERWISER.eu is also offering the opportunity to test the Platform for free to SMEs, Research & Academia, Large Companies and any interested organisation who can apply to join the Open Pilot Stream[166] and start a dedicated training path.

6.1.7.1 Recommendations

From a training perspective, the Critical Infrastructure sector could benefit from being able to:

- Simulate a complete corporate environment with real-world attacks/threats. The staff of Critical Infrastructure should have the opportunity to play both attacker and defender roles in order to better understand how vulnerabilities can be exploited and how to handle cyber-attacks and defence in real life.
- Train both technical and non-technical staff as people at all levels contribute to the risk and protection of an organization's cybersecurity practice. Organisations should consider a systematic delivery of awareness training programs as well as further development and practical training for staff in cybersecurity specialist roles.
- Easily access secure online tools for training and upskill their employees. In accordance with most of the global and European bodies, it is recommended to move away from the traditional training methods to those of the more tailored and practical ones.

In particular, ENISA called for greater use in cyber-ranges[167], such as the one embedded in the CYBERWISER.eu platform. Also, the ECSO report on 'Gaps in European Cyber Education and Professional Training'[168] states that training needs to move to more innovative forms such as a flipped classroom style and the greater usage of online tools.

[166] https://www.cyberwiser.eu/open-pilot-stream

[167] https://www.enisa.europa.eu/news/enisa-news/stocktaking-of-information-security-training-needs-in-critical-sectors

[168] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

6.1.8 ReACT: Reactively defending against advanced cybersecurity threats

Evangelos Markatos, REACT & FORTH-ICS
https://react-h2020.eu

Cybersecurity is not a new problem, but since the Internet/ARPANET was accessible only to a small community (at least during its first couple of decades) cybersecurity was not a major problem. On the contrary, when the wider public started accessing the Internet in the mid/late '90s, then cybersecurity became a major problem and a significant concern. Unfortunately, by that time, it was too late to change some of the design decisions which were already embedded deep into the implementation of the network.

In recent years computers have transformed and are now embedded in all sorts of devices: smart appliances, smart cars, medical equipment, etc. Attacking these new kinds of computers/devices may have a devastating impact on human lives: medical equipment not working, faulty home appliances, dangerous cars, etc.

The ReACT project proposes to deal with the cybersecurity problems: the approach of ReACT to cybersecurity involves a completely new mindset. ReACT argues that instead of rushing to protect computers (without really knowing what is their weakest spot), first try to make computers fail (crash), and then try to protect them by fixing the failures which were just found. ReACT argues that by trying to make computers fail, their weakest points can effectively be uncovered, which can then be protected from future cyberattacks. Using semi-automated fuzzing combined with manual inspection, ReACT partners have already discovered several vulnerabilities in popular software and hardware systems and have catalysed the distribution of security patches and updates for them.

6.1.8.1 Recommendations

- Look at the security infrastructure with the eyes of a cyber attacker to find the weakness to break into the infrastructure. Only then will it be possible to discover the weakest points and only then will it be possible to secure them.
- Try to make computers crash before taking steps to protect them: if the result is to successfully crash the computer, then at least one weak point has been found.
- Before solving a problem ask “why has this problem not been solved yet?” This can reveal all the areas where previous attempts have failed and where new attempts may have an opportunity to succeed.

6.1.9 Conclusions

This webinar focused on how better cybersecurity is essential in order to have effective protection of critical infrastructures against cyber threats and making them more resilient. The main recommendations from this webinar are summarized below:

- **Cybersecurity needs to consider 360° aspects**. It is a continuous process to ensure the security of the new technologies that are being integrated into critical infrastructure, which bring new vulnerabilities and changing attacks.
- Do not forget that not only are systems designed and maintained, but also the skills, which are an important factor, play an important role also for the critical infrastructure when they are operating in the field.
- Further efforts need to be applied to the development of more advanced systems that will rely on advanced technologies such as Artificial Intelligence

(AI) and machine learning techniques to provide more advanced functionalities, which can be shared with the operators in order to deal with such threats.
- Human aspects are extremely important and training is fundamental. Cybersecurity is not a destination, it is a journey, so it is key to keep up to date to cope with the fast-evolving threat landscape.
- Break things first and try to fix them later, and try to make the system fail in order to try to protect it.

6.2 EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks

- Date:12 November 2020
- Presentations and recording[169]
- Final report[170]

6.2.1 Summary

The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity. With the growing use of digital devices and advanced communications and interconnected systems, the EPES is increasingly exposed to external cyber-threats, and therefore requires an attentive evaluation of the cybersecurity risk in order to ensure that proper countermeasures are taken.

On the other hand, despite Smart Grids (SG) supporting a dynamic two-way exchange of information between utility companies and their customers, contributing towards smart and sustainable energy management in Europe and the establishment of a wiser energy consumption mentality, the power grid is also exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the Smart Grids infrastructure, are emerging.

Attacks to EPES and SG may lead to cascading failures, ranging from destruction of other interconnected critical infrastructures to loss of human lives.

The European Commission adopted in April 2019 a sector-specific guidance that identifies the main actions required to preserve cybersecurity and be prepared for possible cyberattacks in the energy sector, taking into account the characteristics of the sector such as the real-time requirements, the risk of cascading effects and the combination of legacy systems with new technologies.

This webinar also met the goal of cyberwatching.eu to cluster active projects with similar goals for their mutual benefit, by identifying possible opportunities for lightweight synergies and supporting them with targeted support activities. The following four research and innovation projects presented their work during the webinar: DEFeND[171], EnergySHIELD[172], SDN-Microsense[173] and SealedGRID. The R&I projects presented their solutions to protect EPES and Smart Grids against cyber-

[169] https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks

[170] https://cyberwatching.eu/publications/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks

[171] https://www.cyberwatching.eu/projects/1039/defend

[172] https://www.cyberwatching.eu/projects/2013/energyshield

[173] https://www.cyberwatching.eu/projects/2325/sdn-microsense

threats, and preserve consumers' privacy. The webinar attracted over 120 registered participants.

6.2.2 Programme

The programme took the following outline with experts from the different projects and Marina Ramirez acting as the Moderator:

- Cyberwatching.eu Introduction and welcome note - Marina Ramirez, Cyberwatching Project Partner & AEI Ciberseguridad
- The DEFeND project to help GDPR compliance in the Energy Sector - Jean-Baptiste Bernard, GRIDPOCKET, Annarita Iodice & Andrea Praitano, MATICMIND, DEFeND
- From Honeypot-oriented Risk Analysis to Islanding Solutions in Energy Systems - Panagiotis Sarigiannidis, University of Western Macedonia, SDN-Microsense
- Distributed Key Management for MicroGrids - Prof. Christos Xenakis - School of Information and Communication Technologies, University of Piraeus, SealedGRID
- Assessing, Enhancing and Cultivating a Cyber-Security Culture in the EPES Sector - Anna Georgiadou - DSS Lab, NTUA, EnergySHIELD

6.2.3 The DEFeND project to help GDPR compliance in the energy sector

Jean-Baptiste Bernard, GRIDPOCKET & DEFEND
Annarita Iodice and Andrea Praitano, MATICMIND & DEFEND
www.defendproject.eu

The DEFeND Platform aims to raise the awareness of data controllers to the real status of an organization, through enhanced visualization elements, and information that can be exploited for each department, third party and/or processing. An important point for the Board of an organization is a synthetic dashboard with the status of the organization compliance to Data Protection. The DEFeND Platform include a Dashboard service to provide this kind of information to the Board and stakeholders.

The DEFeND architecture is composed of the five (5) DEFeND services, the DSM service, Data Process Management (DPM) service, Data Breach Management (DBM) service, General Data Protection Regulation (GDPR) Planning Service, GDPR Reporting Service and all the components included in the DEFeND service. The Defend Platform aims to support the Data Controller to define an improvement program to increase the maturity of the organization in data protection based on the law and related best practices.

6.2.3.1 DEFeND – Recommendations on EPES and Smart GRIDS

- Be in control of the status of the organization compliance to Data Protection, a compliance status for each of the GDPR Principles for the whole organization, for each department and each third party and compliance status information for the data subject.
- Define the list of processing activities, the connections with Departments and Third Parties involved in the activities' linked assets, systems and threats.
- Perform Threats Analysis, Data Minimization Analysis, Privacy by Design/by Default based on the result of the analysis and design modelling techniques, and continuous Risk Assessment.

6.2.4 From honeypot-oriented risk analysis to islanding solutions in energy systems

Panagiotis Sarigiannidis, University of Western Macedonia & SD-microSENSE
www.sdnmicrosense.eu

SDN-μSense

The Smart Grid (SG) is considered as the next-generation electrical grid, transforming the conventional energy model into a new era with a variety of benefits, such as two-way communications, increased reliability, pervasive control and self-healing. However, this evolution raises severe cybersecurity concerns due to both the insecure nature of the legacy systems (e.g., Supervisory Control and Data Acquisition (SCADA)) and the new vulnerabilities originating from smart technologies. Moreover, it is noteworthy that the vast amount of SG sensitive data attracts even more cyber attackers. Characteristic Advanced Persistent Threats (APTs) against energy-related infrastructures are, for example, Stuxnet, Dragonfly, Dragonfly 2.0, BlackEnergy3, TRITON and Crashoverride.

The SD-microSENSE project aims to address the cybersecurity risks in Electrical Power and Energy System (EPES), by introducing an integrated platform of four pillars, namely (a) risk assessment, (b) intrusion detection and prevention, (c) self-healing and energy management and (d) privacy-preserving.

The **first pillar** introduces a collaborative risk assessment methodology and tool, which cooperates with the other components of the SDN-microSENSE architecture to assess the risk level of the various security alerts dynamically.

A large-scale Security Information and Event Management (SIEM) system orchestrate the **second pillar**, including several Artificial Intelligence (AI) detectors related to industrial protocols, such as Modbus, IEC 60870-5-104, IEC 61850, MQTT and DNP3. Furthermore, it adopts advanced visual analytics to identify possible threats and electricity-related disturbances.

Next, the **third pillar** takes full advantage of the Software-Defined Networking (SDN) technology to mitigate possible cyberattacks in real-time. In addition, it comprises islanding and grid restoration mechanisms that can be adopted in emergencies. Furthermore, it is worth noting that through the blockchain technology, it also provides an energy management and transaction platform among various energy-related stakeholders.

Finally, the **fourth pillar** focuses on privacy, introducing an overlay privacy framework, which is responsible for ensuring the confidentiality, integrity and authenticity of the various energy-related data, by using homomorphic encryption and anonymisation techniques.

A honeypot is an asset with no production value that imitates the behaviour of real assets, aiming to protect them and collect valuable information about the cyberattackers. It can play a significant role in the risk assessment procedure since it is an effective detection countermeasure by hiding the real assets, and in parallel, it can act as a threat intelligence mechanism. In the context of the SDN-microSENSE project, three main EPES honeypots were developed, namely (a) Modbus Honeypot, (b) IEC 60870-5-104 Honeypot and (c) IEC 61850 Honeypot. These honeypots are deployed dynamically by a Honeypot Manager, which also can communicate with the SDN controller to re-direct malicious network traffic to an EPES honeypot, thus (a) protecting the real assets and (b) receiving insights about the cyberattacker activities. The security events originating from the EPES honeypots can raise the application of an islanding mechanism, thus mitigating the devastating consequences of a critical cyber-attack. Through a clustering approach, the project introduces an Isolating and Islanding Mechanism (IIM), which solves the problem of the intentional islanding, thereby guiding the system operator to apply the most optimum islanding scheme, taking into account the various constraints and the available Distributed Energy Resources (DERs).

6.2.4.1 Recommendations

Based on the current progress of the SDN-microSENSE project, the following recommendations for the Critical Infrastructures (CIs) are identified.

- **Adoption of the IEC 62351 security controls**. IEC 62351 establishes a set of security and privacy controls, specially designed for industrial environments. In particular, it consists of 14 parts that cover multiple cybersecurity and privacy aspects, such as authentication, access control, privacy, security profiles, key management and security architecture.
- **Timely intrusion detection**. The critical infrastructures include ingredients and communications that were designed without having cybersecurity in mind. However, they are necessary for their core operation. Therefore, appropriate intrusion detection mechanisms should be adopted, considering the unique properties of each individual infrastructure.
- **Timely mitigation.** Smart mitigation mechanisms should act as fast as possible, thus mitigating or even preventing the potential cyberattacks. Smart authentication and access control systems compose characteristic examples. Moreover, the intentional islanding and the grid restoration compose efficient mitigation measures for the energy-related CIs. Finally, the proper usage of SDN technology can contribute significantly to the mitigation of the possible intrusions coming from malicious insiders.
- **Privacy-preserving**. The critical infrastructures comprise a plethora of sensitive data. This data should be protected by many privacy risks. Blockchain, holomorphic encryption and differential privacy are sufficient mechanisms that can guarantee the confidentiality and authenticity of the various data transactions.
- **Threat-Intelligence.** The cyberattacks are evolving rapidly. Therefore, it is crucial to adopt and design adequate systems and methods that can mine information and knowledge about these cyberattacks and malware. Honeypots and anonymous repositories of incidents are characteristic examples that can contribute to this aspect. However, the presence of proactive relevant countermeasures is necessary.

6.2.5 Distributed key management for MicroGrids

Christos Xenakis, University of Piraeus & SealedGrid
www.sgrid.eu

Security for smart industrial systems is prominent due to the proliferation of cyber threats threatening national critical infrastructures. Smart grid comes with intelligent applications that can utilize the bidirectional communication network among its entities. Microgrids are small-scale smart grids that enable Machine-to-Machine (M2M) communications as they can operate with some degree of independence from the main grid. In addition to protecting critical microgrid applications, an underlying key management scheme is needed to enable secure M2M message transmission and authentication. Existing key management schemes are not adequate due to microgrid special features and requirements. SealedGRID proposes the Micro sElf-orgaNiSed mAnagement (MENSA), which is the first hybrid key management and authentication scheme that combines Public Key Infrastructure (PKI) and Web-of-Trust concepts in micro-grids. Our experimental results demonstrate the efficiency of MENSA in terms of scalability and swiftness.

The major challenges, which specifically concern key management in microgrid networks, are the following:

- A microgrid is a network with high churn meaning that nodes frequently join and leave, affecting the efficiency of centralized solutions due to the overhead created by multiple and constant node connection requests to a single entity;
- When the Certification Authority (CA) is compromised, the traditional approach is to revoke all certificates issued and this is an administratively intensive task that would temporarily obstruct the smooth operation and impair information exchange;
- A microgrid can operate either in parallel with an existing power grid or in an “islanded” mode using the M2M communication paradigm; if smart meters lose connectivity to the CA, e.g. due to network outages, it is not currently feasible to validate their certificates affecting the security level of the entire microgrid and the seamless execution of the processes performed inside the network; and
- The storage of certificates to a central server creates a single point of failure which may result in the discontinuation of all network operations.

6.2.6 Assessing, enhancing and cultivating a cybersecurity culture in the EPES sector

Presentation by Anna Georgiadou – NTUA & EnergyShield
https://energy-shield.eu

The EnergyShield toolkit includes five cyber-security tools namely, the Security Behaviour Analysis (SBA) tool, implemented by the Management & Decision Support Systems Laboratory (DSS Lab) of the National Technical University of Athens. In a 15-minute session, participants were presented with the tool specifics including the cybersecurity needs which addressed its main features and challenges. This presentation was concluded with a short demo exhibiting a common use case scenario from the EPES sector reality showcasing the currently available version of the tool.

6.2.6.1 EnergyShield – Recommendations on EPES and Smart GRIDS

- Invest in promoting the personnel of an organisation from a profile of potential cyber-threat to a profile of valuable cyber-security asset.
- Get to know the vulnerabilities of the organization in order to be in a position to defend it.
- Auditing and monitoring are key mitigation policies for a robust cyber-reality.
- Being able to detect anomalies and ongoing attacks is the first step towards protecting assets.
- Information is valuable. Treat it as such. Encrypt it!

6.2.7 Conclusions

The Cyberwatching.eu webinar on "EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks"[174] provided very useful insights and tangible solutions in protecting the electrical power, energy systems and smart grids against cyber attacks and how to preserve the privacy of the data.

During the webinar, the key solutions demos coming from the four (4) research and innovations (R&I) projects were presented providing different offerings:

- EnergyShield is developing the integrated cybersecurity solution/tool for vulnerability assessment, monitoring and protection of critical energy infrastructures.
- The DEFeND platform should help GridPocket to follow GDPR rules at different processing levels to respect the privacy and security rights of its customers and data controller.
- Inside SND-microSENSE project, novel international islanding solutions are proposed, exploiting powerful fitting and generalization capabilities offered by deep learning architectures, offering a real-time solution with increased time efficiency.
- SealedGRID project proposed the Micro **sElf-orgaNised mAnagement (MENSA)**, the first distributed key management and authentication system for microgrids, paves the way toward developing microgrids further and it will help to realise their full potential in terms of scalability and performance efficiency.

[174] https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks

6.3 Cybersecurity Risk Management

- Date: 23 November 2020
- Presentations and recording[175]
- Final report[176]

6.3.1 Summary

Cybersecurity risk management has become a priority for companies and organisations. Staying ahead of threats and regulatory compliance is no joke, let alone how to identify risks, prioritise and take action. So, what steps can you take to ensure resilience and build trust in your services?

Cyber risk management can be challenging in multiple ways given that many organisations do not perceive the risk until something bad happens and many smaller organisations do not have the means or even the awareness of the risks that exist. All too often, an SME (or even a large company or organisation) only sees their risk exposure when an actual breach occurs, a denial-of-service attack or when they are “locked out” of their own data by a ransomware attack.

This 17th webinar entitled “Cybersecurity risk management: How to strengthen resilience and adapt in 2021”[177], gathering over 132 registered participants from 29 countries around the globe.

The webinar focussed on standardisation and certification, in particular in relation to the large European SME community with presentations from ECSO[178], which provided a policy setting to the webinar and key players such as SGS[179], and Cyberwatching.eu partners Digital SME Alliance[180] and AON[181].

The webinar also shone the light on R&I research into the topic. Six R&I projects CyberSure[182], CUREX[183], GEIGER[184], PANACEA[185], RESISTO[186] and SECONDO[187], presented their research in the field highlighting the risk management challenge they address, the key results and the main impacts of these results on European organisations (in particular SMEs).

A key aspect of the webinar was to highlight the importance of online resources and tools which target SMEs. These are essential in helping SMEs prepare for cyberattacks and become more resilient. The Cyberwatching.eu Risk Management tool and the forthcoming cybersecurity certification seal, are tools that can help organisations to expose and employ prevention mechanisms in areas where there

[175] https://cyberwatching.eu/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[176] https://cyberwatching.eu/publications/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[177] https://cyberwatching.eu/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[178] https://ecs-org.eu/
[179] https://www.sgsgroup.it/
[180] https://cyberwatching.eu/european-digital-sme-alliance
[181] https://cyberwatching.eu/aon
[182] https://cyberwatching.eu/projects/1789/cybersure
[183] https://cyberwatching.eu/projects/1814/curex
[184] https://cyberwatching.eu/projects/2126/geiger
[185] https://cyberwatching.eu/projects/1270/panacea
[186] https://cyberwatching.eu/projects/1974/resisto
[187] https://cyberwatching.eu/projects/1972/secondo

could be significant cybersecurity risks, which were not identified and addressed previously.

6.3.2 Programme of the Webinar

This half-day webinar was targeted towards small and medium enterprises to assist them by providing practical guidance for risk management and to share tools and solutions which could help increase their cyber risk readiness covering, among others, the following topics:

Managing risk in 2021

- “Managing risk in 2021" - Mark Miller, Vice Chairman, ECSO & EOS; Conceptivity & Cyberwatching.eu
- Cybersecurity certification, standardisation and supply chains" - Roberto Cascella, European Cyber Security Organisation (ECSO)
- "Why a Light Cybersecurity label is the way forward for SMEs" - Lucio Gonzalez Jimenez, Digital Trust Services, SGS
- "The SME Guide for the Implementation of ISO/IEC 27001" - Fabio Guasconi, DIGITAL SME Alliance and Bl4ckSwan
- "Understanding your organisation's risks" - Paolo Modica, AON

New directions addressing risk management challenges

- SECONDO - "Optimising cybersecurity investments and cyberinsurance" - Christos Xenakis, and Aristeidis Farao, University of Pireaus
- CYBERSURE - "A framework for liability-based trust" - Panos Chatziadam, ICS Forth
- RESISTO - "Controlling risk for communication infrastructure operators" - Mirjam Fehling-Kaschek and Natalie Miller, Fraunhofer
- GEIGER - "The risk management geiger counter" - Max Van Haastrecht, University of Utrecht
- CUREX - "Blockchain-based risk-assessement management for healthcare" - Christos Xenakis and Eleni Veroni, University of Pireaus
- PANACEA - "People-centric risk management for heatlthcare" - Fabrizio De Vecchis, RHEA Group
- Ending the webinar was a 10 minute Q&A

6.3.3 Why a light cybersecurity label is the way forward for SMEs

Lucio Gonzalez Jimenez, Digital Trust Services, SGS
www.sgs.com

Implementing processes, procedures and policies to protect information and data is essential for all companies. And these challenges are faced in every single sector, **no matter specialization or company size.** Certification is very important because it helps you to protect your **business** (market differentiation, supply chain, etc.) and **customers** (security by design, etc.). In addition, the EC launched the **Security Industry Policy** in 2012 that underlined the importance of meeting standards and certifications to overcome market fragmentation.

Currently, the certification ecosystem (certification, accreditation, audits, etc.) is a very **complex environment from the SME point of view**. There is a strong need to offer SMEs a clear approach to help them understand what they have to do to avoid getting lost during the process. The **EU Cybersecurity Act** and the different certification schemes that are to be implemented will help, but this is still a long road and a lot of information to read and process.

Taking into account the amount of information regarding schemes, standards and methodologies that an SME needs to understand to properly choose the testing, inspection and certification services to improve its position in the market, it's highly recommended, as a first step, to trust in a **consulting firm** to help SMEs to implement the standards and/or technical certifications. The second recommended step is an internal exercise of **self-assessment** to identify the critical assets you want to protect. The third and final step is the **certification** itself, accredited by a Third Independent Party. These three steps are as important as **different** to be competitive in the Digital Single Market (for instance, in some countries you need to be certified in order to sell your products to public administrations).

In spring 2021 the **SME Cybersecurity Label** will be launched. Created by SGS and the Cyberwatching.eu project the label is designed to ease the entrance of SMEs into the certification ecosystem. The label provides a **self-assessment based on a robust approach and a solid background to the certification path**.

6.3.3.1 Recommendations on cybersecurity risk management for SMEs

More online resources should be made available to the SME community. The Cybersecurity Label will provide SMEs with an accessible first step to understanding the areas in which they have gaps in security and the types of actions that they should take towards an eventual certification. Covering topics such as software, protocols, hardware and infrastructure, the label provides a first check for SMEs in helping them to understand, evaluate and assess security gaps. This lowers the barrier to entry into the certification process and gets companies into the habit of carrying out checks of systems which can lead to greater resilience and ultimately trust for their customers.

6.3.4 Towards a trustworthy and resilient digital Europe

Roberto Cascella, ECSO
https://ecs-org.eu

ECSO Working Group (WG) 1 focusses on "standardization, certification, and supply chain management". Key areas that are addressed include:

- **Connected components**
  Work on the inter-relationship ("composition") of EU scheme certified components based on standards for trusted supply chain and product certification in line with the EU Cyber Act.
- **Digital services and systems**
  Understand the systems' and services' dependencies: needs and current approaches for risk management and operational aspects.

ECSO has contributed to the recommendation for certification scheme of the industrial, automated control system report done with the pilot projects.

The ECSO product certification composition, known by the common criteria community and they already using it, was presented, and explain how to move it from common criteria and bring this concept in any certification scheme by:

- Enabling efficient re-use of certificate and evaluation evidence.

- Decreasing certification cost and improve overall process speed.
- Providing benefit to horizontal components specialised in application domains.
- Contributing to the time to market of certified products.

6.3.4.1 ECSO – Recommendations on Cybersecurity Risk Management

It is important to look at the European cybersecurity certification and understand what could be the main challenges that could hinder the usage of future European cybersecurity schemes across industries, consideration such as:

- Cybersecurity framework consistency.
- Composition of evidence and considerations for system integrators.
- Analysis of priorities for cybersecurity certification based on market needs.

6.3.5 The SME guide for the implementation of ISO/IEC 27001

Fabio Guasconi, Bl4ckSwan S.r.l. & Digital SME Alliance
www.digitalsme.eu

Digital SME Alliance is the largest network of small and medium-sized ICT enterprises in Europe, representing about 20,000 digital SMEs, which is a joint effort of 30 national and regional SME associations from EU member states and neighbouring countries. Digital SME Alliance is also a founding member of the Small Business Standards (SBS). SBS is one of the Annex III organisations of Regulation (EU) 1025/2012, which represents and defends SMEs' interests in the standardisation process at European and international levels.

As part of its SBS activities, Digital SME Alliance leads the SBS sectoral approach on ICT and involved in the creation of the "SME Guide for the Implementation of ISO/IEC 27001" [188], dedicated to SMEs for the implementation of ISO/IEC 27001 on information security management. ISO/IEC 27001 is the international standard for companies that need a robust approach to managing information security and building resilience. With its Guide, DIGITAL SME aims to help SMEs better understand ISO/IEC 27001 and assist them in its concrete implementation.

How can the guide be helpful for Small and medium-sized enterprises?

1. SMEs make up the vast majority of businesses in Europe, outnumbering large corporations and employing more people. They are recognised to be a driver for innovation in Europe.
2. Most SMEs underestimate their risk level for cyber-attacks, in the belief that they do not handle any information worth stealing.
3. However, small businesses have a lot of digital assets compared to individual user and they often have fewer security measures in place than larger organisations.

The SME Guide for the implementation of ISO/IEC 27001 was developed by information security experts appointed by recognised SME and cyber-security trade associations of various European countries. The guide is written for and applicable for

[188] http://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

SMEs that rely on technological assets. Its guidelines can be easily implemented by any organisation, whatever their size or complexity.

6.3.5.1 DSME – Recommendations on Cybersecurity Risk Management

The SME Guide describes a series of practical activities that can significantly help with establishing or raising information security levels within an SME. This will strengthen their business and facilitate partnership opportunities within local and EU markets.

The main advantages for SMEs using the guide are:

- Disseminating high-level information concerning information security management in small businesses.
- Increasing uptake of information security management concepts based on ISO/IEC 27001 by European SMEs.
- Having a reference document that will represent the port of call for SMEs willing sort out the wild ecosystem of information security management.

6.3.6 Understanding your organisation's risks

Paolo Modica, AON & cyberwatching.eu
www.cyberwatching.eu

The new Cyber risk temperature tool[189] produced by the cyberwatching.eu project provides a preliminary assessment of the exposure to cyber risk for SMEs. By completing this online questionnaire, any SME, business or even public administration can receive an initial evaluation of their current risk to a cyber-attack and recommendations on how to reduce risk.

The questionnaire is divided into two main parts. Firstly, the interviewee is asked to give a personal assessment of his company's IT security. Then the interviewee is asked more technical questions. By assigning a score to each answer and analysing this score, a profile is assigned to the interviewee.

6.3.6.1 AON and Cyberwatching.eu – Recommendations on Cybersecurity Risk Management

It is important to get a vulnerability assessment as most thorough as possible, since dangers and gaps may come from multiple sources such as i) methodologies ii) knowledge iii) distribution of administrative rights iv) information segmentation policy v) authentication policies vi) etc.

The risk management tool serves as a first entry-level to inform the user of initial steps to take. A more in-depth and complete analysis is highly recommended in order to receive a precise and tailored vulnerability assessment for one's company, though the Cyber risk Temperature tool represents a smart and rather quick starting point for both the user and the organisation.

[189] https://cyberwatching.eu/cyberwatching-cyber-risk-temperature-tool

6.3.7 Cyber Security Insurance – A Framework for Liability Based Trust

Panos Chatziadam, ICS Forth & CyberSure
www.cybersure.eu

CyberSure is a programme of collaboration and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance for cyber systems. The purpose of creating such policies will be to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches. The framework will be supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems.

CyberSure will develop its cyber insurance platform at TRL-7 by building upon and integrating state of the art tools, methods and techniques. These will include: (1) the state-of-the-art continuous certification infrastructure (tools) for cloud services developed by the EU project CUMULUS; (2) the risk management tool of NIS enhanced by the NESSOS risk management methodology; and (3) insurance management tools of HELLAS.

The impact of the project firstly improves the process of cyber insurance such

- Baseline risk analysis: Risk assessment methodologies and tools will support the early analysis and specification of risk models.
- Certification: Generation of executable cyber system certification models and use them to carry out assessments of the soundness and the effectiveness of the countermeasures used for mitigating risks.
- Comprehensive risk assessment: The certificates and/or the operational evidence generated by certification should provide inputs to a subsequent comprehensive assessment of risk that may be required for formulating and pricing cyber insurance policies.
- Cyber insurance policy management: This phase covers the activities of managing cyber insurance policies, i.e., policy creation, pricing and updating and claim handling.

It also improves risk assessment for (1) cyber insurance by providing practical risk assessment targeted at organisations, who are providing cyber insurance, which leads to the enrichment of the cyber insurance sector via the application of risk assessment methodologies and innovative techniques applied for cyber services, (2) dynamic and automated risk assessment evidence collection as opposed to manual testimony-based risk assessment (remove the human factor), improving the insurance setup process and policy identification through objectives and measurable assessment of the degree of reliability, and (3) dynamic semi-automated adaptation of the insurance policy based on the evidence collected.

6.3.7.1 CyberSure – Recommendations on Cybersecurity Risk Management

The CyberSure project considered the different business impact that cyber insurers and cyber system providers in terms of delivering security services to their customer.

Cyber insurers:

- Provision of a comprehensive approach and platform for creating, monitoring and adapting cyber insurance policies, providing cyber insurance policies customised to the needs of individual customers and their organisational risk assessment.
- Dynamic and continuous risk management will lead to a more thorough and accurate basis for monitoring cyber insurance policies, reducing the risk and cyber insurance management costs and consequently policy premiums.

Cyber system providers:

- Improving security through the provision of automated risk management and S&P assessment and certification services,
- Incentivising service providers to improve their security according to reference security standards and benchmarks, to reduce their insurance premiums, and
- Establishing liability through the undertaking of cyber insurance policies.

6.3.8 Optimising cybersecurity investments and cyberinsurance

Aristeidis Farao, University of Pireaus & SECONDO
https://secondo-h2020.eu

First and foremost, most of the organizations working with the internet and network services get experienced an increase in cybercrime. We need to protect our systems against the increased cyberattacks. Regarding cyber threat intelligence (CTI), we separate the CTI operations into four different phases. First, we need to Acquire Data. The data come from internal sources and external sources. Data from internal sources are related to how the organization works, the internal procedures that get used as well as the services that get used. While, the data from external sources come from social media, open-source intelligence, human intelligence, and the dark web.

Secondly, we have to Analyse the data we acquired from the first phase. For that purpose, we have many tools, like artificial intelligence, to make predictions, to extract insights and patterns. We also use data analytics to analyse raw data to make conclusions. Also, since we miss some data, we use machine learning to predict these missing values. Thirdly, we have to take action (Intelligence). Based on the previous analysis, we have to detect the threats of our organizations and evaluate the status of our organization. Also, we have to respond and prepare the organization’s future actions aiming to mitigate the risks, and since we cannot mitigate them at all, we can also transfer the risk. The last phase is related to Continuous Risk Monitoring. During that phase, we continuously assess the risk level and the performance of the implemented security controls. However, we can observe that the CTI comes with many challenges, e.g., proper team, budget allocation, access to all intrusion points, understanding and integrating CTI).

The SECONDO Project proposes an Economics-of-Security-as-a-Service platform that encompasses a comprehensive cost-driven methodology for a) estimating cyber risks based on a quantitative approach; b) recommending optimal investments in cybersecurity for efficient risk management and c) determining the residual risks and estimating the cyber insurance premiums.

The SECONDO platform consists of four modules. The Quantitative Risk Analysis Module is responsible to quantitatively estimate the cyber risk exposure, utilizing data that not only come from the internal sources that are related to the valuation of the assets and the assessment of the user's behaviour, but also from external sources, using crawlers to find data in social media but also in the dark web. The second module is the Cyber Security Investment Module. This module consists of two parts, the Econometrics Module and the Game-Theoretic Module (GTM). The ECM will provide estimates of all kinds of costs of potential attacks as well as the costs of each possible security control. On the other hand, the GTM will model all possible attacking scenarios and defensive strategies and then uses game-theoretic techniques to derive optimal defending strategies in the form of Nash Equilibria. The third module is called Cyber Insurance Coverage and Premium Module (CICPM), which is responsible not only to generate the premium but also to store it in a smart contract. The last module is the Continuous Risk Monitoring Module (CRMM) that is responsible to continuously assess the risk level and the performance of the implemented security controls. We can observe that the main modules follow the four phases of the CTI.

The impact of organizations can get reflected in four stages. The first one is related to Mitigate Cyber Risk. It can get achieved since we collect data from phishing campaigns on the organization assessing the user behaviour, we analyse data from SIEM, we collect data from social media and dark web but also, we have our asset valuation function. Secondly, the organizations can get consulted on cybersecurity strategies and investments due to the ECM and GTM. Also, we can ensure fair premiums due to the CICPM.

6.3.8.1 SECONDO – Recommendations on Cybersecurity Risk Management

- Improve the Continuous Risk Monitoring: More specific, a successful continuous risk monitoring will be responsible to assess continuously the risk levels, including the performance of the implemented cybersecurity controls.
- Risk Transfer: If the organization installed tools and methods to mitigate the risk but not in an acceptable level the risk transfer is a solution.
- Comply with Guidelines and Regulations: The compliance of an organization with guidelines and regulations related to cybersecurity can reinforce the organization against potential cybersecurity incidents.

6.3.9 The risk management Geiger counter

GEIGER

Max Van Haastrecht, University of Utrecht & Geiger
www.project.cyber-geiger.eu

The Horizon 2020 project GEIGER aims to help micro-and small-sized enterprises (MSEs) in becoming more aware of the cybersecurity risks they face. The GEIGER application will also help users and their companies to become more resilient to cyber threats.

Using a well-known formula for risk:

Risk = Threat x Vulnerability x Consequence, we argue that there is a discrepancy between the cybersecurity risk people feel, and the cybersecurity risk experts estimate exist. Generally, people underestimate risk, meaning they are less likely to feel the need to use cybersecurity risk management solutions than cybersecurity experts may think.

Part of this discrepancy comes from an inaccurate definition of ‘threat’ that is often used in research and other projects. To define the threat level, proxies such as the prevalence of vulnerabilities in an MSE are often used. In GEIGER, we aim to take threats at their face value. To get an accurate understanding of the frequency with which MSEs face digital security threats (e.g., phishing), we work together with Computer Emergency Response Teams (CERTs) and National Cyber Security Centres (NCSCs) throughout Europe.

The GEIGER indicator, together with the education ecosystem that the project will also develop, contributes to creating an attractive cybersecurity solution for small businesses and entrepreneurs. One of our ambitious goals is that by the end of the project, 50,000 MSEs have tried the GEIGER solution.

6.3.9.1 GEIGER – Recommendations on Cybersecurity Risk Management

Cybersecurity risk management can be handled better by MSEs:

- Researchers must commit to more accurately reflecting the concept of ‘threat’ in their risk management solutions. This is an important step in limiting the discrepancy in understanding of risk between theory and practice.
- Working together with CERTs, NCSCs, and other governmental organisations in cybersecurity projects is essential. Not only do they have information that accurately reflects the state of the world, but including them in projects helps to harbour trust among potential users of the cybersecurity risk management solutions we offer.
- Cybersecurity risk management is a process, not a ‘quick check’. Cybersecurity risk management solutions should always aim to help users over an extended period of time, for example by incorporating an education framework.

6.3.10 Controlling risk for communication infrastructure operators

Mirjam Fehling-Kaschek, Fraunhofer & RESISTO
www.resistoproject.eu

RESISTO is an EU H2020 project with the aim of improving the risk and resilience of telecommunication infrastructures and improves their ability to handle cyber, cyber and combined cyber-physical threats. RESISTO comprises two main control loops: the long term and short term. The long-term control loop includes offline analysis and a risk and resilience management process. This management process extended the risk management ISO-31000 standard to include resilience assessment. Alternatively, the short-term control loop is an online process that works to detect anomalies in the system and evaluate the impact of those anomalies or adverse events. The short-term loop also provides decision support. The two control loops are connected via the Knowledge Base where indicators from both loops are compared and feedback can be given to the long-term control loop for adjustments in the simulations.

6.3.10.1 RESISTO – Recommendations on Cybersecurity Risk Management

- Resilience should be incorporated with risk management. Including resilience will allow for the systems to able to handle more adverse events, including ones that are unknown or have too low of an occurrence probability to be considered in traditional risk management.
- One of the outputs of the risk and resilience management process should be the quantitative measurement of many specific resilience indicators, each one related to a specific threat. For reasons of convenience and to reduce complexity, it is necessary to prioritize threats in terms of probability and level of impact, and then focus on the most relevant.
- When investigating threats and adverse events to improve cybersecurity, cyber-attacks should be considered, but also physical-cyber-attacks. This is to say that physical events, whether intentional, accidental or natural, may lead to problems in the cybersphere and therefore should be investigated and included in any risk analysis related to cybersecurity.
- Furthermore, in the event of physical and cyber threats that can occur at the "same" time and/or in the "same" place, even in a completely independent way, the aggregate impact should be assessed and the countermeasures to be implemented should be unified.

6.3.11 Blockchain-based risk-assessment management for healthcare

Presentation by Eleni Veroni, University of Pireaus & CUREX
www.curex-project.eu

The greatest challenge for the e-health ecosystem is to find the balance among security requirements, new regulations and human welfare. Every day, more and more paper-based health records are being replaced with electronic ones, raising new risks, vulnerabilities and threats. At the same time, modern healthcare services, to function properly, require constant data sharing between stakeholders and service providers. These interconnections form a complex ecosystem with many interrelated entities, creating a very large attack surface. To secure such an evolving and complex environment from unknown vulnerabilities and new cyber threats, secure-by-design devices and services are required, as well as a risk-based approach to help the higher management to stay ahead of a potential cyber crisis.

It has been identified that the newly introduced threats against the healthcare domain are mainly targeting standard procedures applied to Electronic Health Records. One such standard procedure is the health data exchange. Health data exchange takes place intending to advance the services provided to patients today. Health data may be exchanged within the same organisation where, for example, different clinics need to share data to effectively treat a patient. Another common scenario is the one that foresees the cross-organisation transaction of medical records, where the data need to be sent to a different institution or even a different country, for further assessment.

The future of healthcare services will be highly dependent on the massive exchange of data, which, to be realized, increased connectivity is required between platforms, devices & organizations. The interconnectivity, however, creates several security issues that need to be addressed beforehand, such as zero-day vulnerabilities and advanced threats. Every attempt against healthcare infrastructures puts at risk both patients' privacy and health and may cause severe operational disruptions and major economic losses to the healthcare organizations. On top of that, the responsible authorities, through the legislation and directives enforced in European Union member countries, have created additional obligations for organizations that operate on clinical & medical data (e.g., GDPR).

CUREX, a three-year R&I Action funded under the 2018 call for “Trusted digital solutions and Cybersecurity in Health and Care”, addresses comprehensively the protection of the confidentiality and integrity of health data by producing a novel, flexible and scalable situational awareness-oriented platform. CUREX allows a healthcare provider to assess the realistic cybersecurity and privacy risks they are exposed to and which are propagated to the data that is exchanged between hospitals and care centres. For this purpose, CUREX proposes a cybersecurity and privacy risk assessment toolkit tailored for different types of healthcare organisations. The toolkit is comprised of the Cybersecurity Assessment Tool (CAT) and the Privacy Assessment Tool (PAT).

CAT assesses risks related to cybersecurity threats and vulnerabilities as modelled by the CUREX vulnerability discovery process and the threat intelligence functionality. Analysing data coming from multiple sources, it estimates the risk level of an organization in real-time, performing both quantitative and qualitative risk analysis and producing cybersecurity risk scores per organisation and asset, which are stored on the CUREX Private Blockchain. CAT has the ability to propose countermeasures to address the identified risks on the fly, which are later leveraged by the CUREX decision support tool.

PAT measures the privacy level of an organisation aiming to support compliance with the GDPR for protecting patients’ privacy. Based on every business process that concerns the processing and exchange of data, PAT assesses the degree of compliance of the healthcare organisation with the GDPR by providing an indicative privacy score by looking at all assets used to process sensitive data. Finally, PAT, using its Privacy Quantification Engine, merges the cybersecurity and privacy impact to quantify an overall privacy risk level, that will also be stored on the CUREX Private Blockchain.

A significant challenge that the healthcare domain needs to overcome is its closed nature due to its criticality, complexity and strict regulation, which disallows the threat of intelligence sharing between organizations and the community in general. Repositories containing information specifically for software and hardware used in the domain are not currently available, and care centres, especially public ones, are rarely in a position to afford proprietary cybersecurity solutions.

6.3.11.1 CUREX – Recommendations on Cybersecurity Risk Management

During the first few months of the COVID-19 crisis, the attacks against the healthcare sector reached unprecedented levels. The current healthcare infrastructures, under the extreme pressure of the pandemic, are unable to handle the digital crisis happening at the same time. CUREX’s aim to enhance the security level of the domain is more relevant than ever, and for this to happen the involved stakeholders should invest in tools and procedures that will:

- Ensure the organisation’s compliance with the current European legal framework. More specifically, healthcare organisations should take action to address the requirements posed by EU legislation and directives, such as the General Data Protection Regulation (EU) 2016/679 (GDPR), the Directive 2011/24 (EU) on patients’ rights in cross-border healthcare (Patients’ Rights

Directive), the Regulation (EU) 2017/745 on medical devices (MDR), the Regulation (EU) 910/2014 on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation) which introduces the mutually recognised electronic identification of patients and healthcare providers facilitating the proper cross-border provision of healthcare services, as well as the Directive (EU) 2016/1148 on network and information security (NIS Directive), and the Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), both of which are expected to become mandatory in the near future.

- Improve the cyber hygiene culture among personnel. The definition of strategies for raising cybersecurity and data privacy awareness focusing on the specific needs of different employee groups in a healthcare organization (i.e., Admin, Medical, IT, Mgmt. /Security), can help identify and close group-specific gaps through the recommendation of tailored human-centric actions/controls.
- Minimize the impact of possible violations of the organisation’s infrastructure and data. Medical facilities should invest in cybersecurity risk management solutions, to complement and extend their existing cybersecurity infrastructures. A risk-based approach that takes into account risks not only coming from direct cyber-attacks but also knowledge gaps and legal breaches should be adopted by the higher management to address future cyber threats holistically.

6.3.12 People-centric risk management for healthcare

Fabrizio De Vecchis, RHEA & PANACEA
www.panacearesearch.eu

The greatest challenge for the e-health ecosystem is to find the balance among security requirements, new regulations and human welfare. Every da DRMP protects complex hospital IT infrastructures by enabling the computation of possible attack paths on multiple layers (network, access, humans, e.g., medical staff). An innovative aspect of DRMP is the multi-dimensional attack model, reflecting the role played by human behaviours in the development of a cyber-attack. The model tries to capture how human users access ICT and medical devices, identifying human vulnerabilities that can be exploited to materialise the most common threats in healthcare organisations.

Use case scenarios include:

- Gemelli University Hospital: Laboratory of Systems and connected point of care testing (POCTs).
- Irish Health Service Executive: Hospital monitor control system and wireless connected medical devices.

The presentation highlighted multi-dimensional data acquisition and reachability computation of the monitored environment; acquisition of IT infrastructure knowledge (scans, topology of data flows, asset characteristics); acquisition of vulnerability surface knowledge (scans); acquisition of users and user access information; acquisition of business and governance models. It also showed the threat analysis, risk and response evaluation, including technical, governance, organisational and human mitigation actions, as well as the visual analytics environment, explaining how the DRMP increases cybersecurity resilience of IT infrastructure in healthcare organisations.

6.3.12.1 PANACEA – Recommendations on Cybersecurity Risk Management

- Factor in human aspects and staff security profiles in risk management, analysing behaviour like the sharing of credentials and other weak links or vulnerabilities caused by negligence or carelessness. Ensure mitigation actions include training or secure behaviour nudging.

- Consider a multi-dimensional approach to risk management, across the business, access, network and human layers with attack paths for each layer to reduce organisational risk and impacts on business processes.

- To increase cybersecurity resilience in healthcare IT infrastructures, adopt new models that can rapidly capture and analyse multiple variables in a potential attack and proactively and continuously monitor current risks, supporting operators with increased situational awareness and guided and interactive risk analysis.

- Involve end-users in testing new tools and solutions to ensure usability, effectiveness in reducing threat surface and affordability.

6.3.13 Conclusions

Cybersecurity is a pressing issue not only for large enterprises, as well as for small businesses. The fundamental risks areas are similar no matter how big the scale is, as they still hold potentially lucrative data and information. Frequently, criminals are targeting SMEs and start-ups as they are softer target with less IT security resources, and cannot invest in the same specialist technology or training as larger corporates.

Over the decade, cybersecurity has moved from a technical specialism to a mainstream business issue. Under the general data protection regulation (GDPR), small businesses now have the same responsibility as large corporations when it comes to processing and protecting data.

The Cyberwatching.eu webinar on "Cybersecurity risk management: How to strengthen resilience and adapt in 2021", provided practical aspects, while at the same time shared tools and references that can give organisations, particularly SMEs, MSEs and start-ups, an edge in cybersecurity risk management.

The main recommendations from this document are detailed below:

- It is important to look at the European cybersecurity certification and understand what could be the main challenges that could hinder the usage of future European cybersecurity schemes across industries.

- Certification can be a long, complex and expensive road for SMEs. Providing an accessible first step to understanding the areas in which they have gaps in security and the types of actions that they should take towards an eventual certification.

- Providing practical activities that can significantly help with establishing or raising information security levels within an SME. This will strengthen their business and facilitate partnership opportunities within local and EU markets.

- Dynamic and continuous risk management will lead to a more thorough and accurate basis for monitoring cyber insurance policies, reducing the risk and cyber insurance management costs and consequently policy premiums.

- Cybersecurity risk management is a process, not a 'quick check'. Cybersecurity risk management solutions should always aim to help users over an extended period of time, for example by incorporating an education framework.

- Resilience should be incorporated with risk management. Including resilience will allow for the systems to able to handle more adverse events, including ones that are unknown or have too low of an occurrence probability to be considered in traditional risk management.

- One of the outputs of the risk and resilience management process should be the quantitative measurement of many specific resilience indicators, each one related to a specific threat. For reasons of convenience and to reduce complexity, it is necessary to prioritize threats in terms of probability and level of impact, and then focus on the most relevant.

From a healthcare perspective, the current healthcare infrastructures, under the extreme pressure of the pandemic, are unable to handle the digital crisis happening at the same time.

- Improve the cyber hygiene culture among personnel. Ensure the organisation's compliance with the current European legal framework which include the GDPR.

- Factor in human aspects and staff security profiles in risk management, analysing behaviour like the sharing of credentials and other weak links or vulnerabilities caused by negligence or carelessness. Ensure mitigation actions include training or secure behaviour nudging.

- Consider a multi-dimensional approach to risk management, across the business, access, network and human layers with attack paths for each layer to reduce organisational risk and impacts on business processes.

6.4 Webinar on Security and Privacy by Design for Healthcare

- Date of webinar: 10 December 2020
- Presentations and recording[190]
- Final report[191]

6.4.1 Summary

Delivery of health services (clinical and administrative) through ICT and connected medical devices is a necessity for healthcare organisations and changes the way healthcare services are delivered and data are shared. Therefore, cyberattacks and staff misbehaviour may have significant negative effects on business continuity, patients' safety and data privacy.

[190] https://cyberwatching.eu/security-and-privacy-design-healthcare

[191] https://cyberwatching.eu/publications/security-and-privacy-design-healthcare

Current levels of privacy protection and security are highly dependent on the intrinsic risk embedded in the existing systems, medical devices and procedures: in a long-term perspective, if the investments for physiological renewal/upgrade of these assets were inspired to a "privacy and security by design" approach, the overall risk would decrease.

According to this approach, the European Commission has set-up regulatory measures (e.g., GDPR, MDR, EU Directive 2016/1148), and also, through the Horizon 2020 programme, funded research and innovation projects to develop solutions that are effective and usable in the healthcare context to reduce the overall ex-ante risk. This includes threats specific to Covid-like situations.

This webinar entitled "Security and Privacy by Design for Healthcare" took place on 10 December 2020 at 11 AM CET. On this occasion, the following projects showcased their cybersecurity solutions: DEFEND[192], PANACEA[193] and PAPAYA[194]:

- The ***Data Governance for Supporting GDPR** (**DEFeND**)* project provides an innovative data privacy governance platform which supports Healthcare organizations towards GDPR compliance using advanced modelling languages and methodologies for privacy-by-design and data protection management.
- The **Protection and Privacy of Hospital and Health Infrastructures with Smart Cyber Security and Cyber Threat Toolkit for Data and People** (**PANACEA**) project provides medical device manufacturers, and healthcare organizations with a Security-by-Design Framework (SbDF), a comprehensive workflow including processes, software solutions and links to regulations, covering the entire Medical Device lifecycle, from requirement definition to in-hospital deployment.
- The **PlAtform for PrivAcY preserving data Analytics** (**PAPAYA**) project is developing privacy-by-design solutions and a dedicated platform for data analytics tasks which are outsourced to untrusted data processors. This will allow stakeholders to ensure their clients' privacy and comply with the European GDPR while extracting valuable and meaningful information from the analysed data. PAPAYA targets two digital health use cases, namely arrhythmia detection and stress detection, whereby patients' data are protected through dedicated privacy enhancing technologies.

With representatives from the health, legal and cybersecurity sectors, this webinar presented the main challenges facing the medical sector in ensuring secure integration of services that comply with EU regulations.

6.4.2 Programme of the webinar

The programme took the following outline with the following experts presenting and Marina Ramirez acted as the Moderator:

- Welcome note and purpose of the Webinar - Marina Ramirez, AEI Ciberseguridad, Cyberwatching.eu
- Challenges and an overview of the proposed Solutions - Sabina Magalini, Fondazione Policlinico Universitario Gemelli

[192] https://cyberwatching.eu/projects/1039/defend
[193] https://cyberwatching.eu/projects/1270/panacea
[194] https://cyberwatching.eu/projects/974/papaya

- The Roadmap to GDPR Compliance in e-Healthcare Services - Paolo Balboni/Anastasia Botsi, ICT Legal Consulting, Cyberwatching.eu
- PAPAYA: PlAtform for PrivAcY preserving data Analytics (Healthcare Use Cases) - Orhan Ermis, EURECOM
- Security and privacy by design for healthcare data governance - Andrés Castillo, Pediatric Hospital Niño Jesús and Haris Mouratidis, University of Brighton, DEFeND
- PANACEA framework of Security-by-Design Principles applicable to Health systems and medical devices development - Martina Bossini Baroggi, RINA

6.4.2.1 Registrations

This webinar attracted a large audience, as described below:

- 125 participants registered with a broad distribution from 20 countries
- 98 participants attended.

6.4.3 Challenges and an overview of the proposed solutions

Sabina Magalini, Fondazione Policlinico Universitario Gemelli (FPG), Rome Catholic University School of Medicine & PANACEA

Panacea
People-centric cybersecurity in healthcare

There is an urgent need for security and privacy-by-design solutions in healthcare given the following challenges that are being faced, such as:

- **Hospitals and digital service providers need «protocols» for secure integration**:
  - Systems developers and medical device manufacturers need to apply Security & Privacy by Design approaches.
  - Also, hospitals and digital service providers need to master Security & Privacy by Design, when they procure and deploy the assets.

- **All healthcare actors need to comply with the EU regulatory framework:**

  GDPR (EU) 2016/679:
  - Art.25 Data protection *by design and by default: ... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, … designed to implement data-protection principles.*
  - *Art.30 Records of processing activities: … Each controller … shall maintain a record of processing activities under its responsibility…Each processor ... shall maintain a record of all categories of processing activities carried out*

  Directive (EU) 2016/1148 (NIS) concerning measures for a high common level of security of network and information systems across the Union.

  - *Whereas 50): … manufacturers and software developers … play an important role in enabling operators of essential services and digital service providers to secure their network and information systems.*

  Medical Devise Regulation (EU) 2017/745

- *Requirements regarding design and manufacture. 17.2: For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of the development life cycle, risk management, including information security, verification and validation.*

Cyber Regulation (EU) 2019/881

- *Reinforce by the said regulation, which establishes an EU-wide cybersecurity certification framework for digital products, services and processes.*

In the Covid-like context, specific requirements pointing to the need of Security & Privacy by Design have been raised:

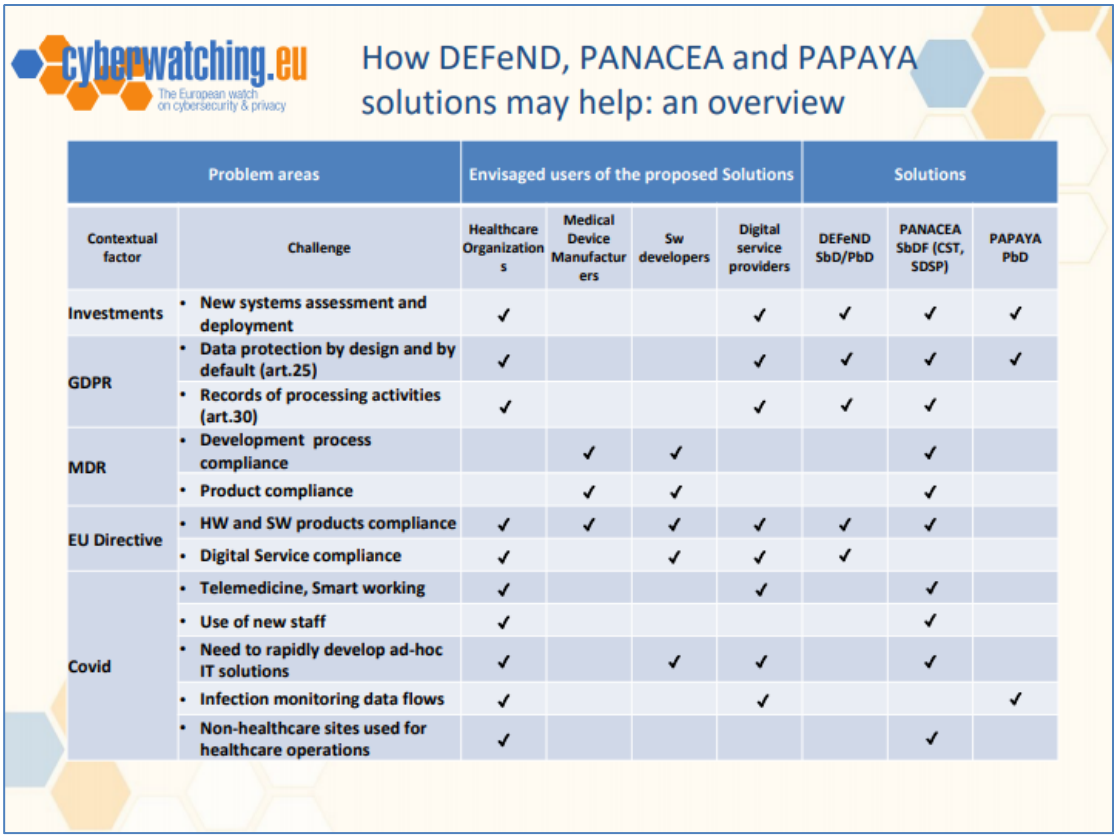
- **Telemedicine**: the policy to keep non-severe COVID patients at home and the need for telemonitoring, expanded use of telemedicine, that has a low level of security.
- **Smart workin**g: Risk may come from technology illiteracy of the staff at home and increased risk of infection due to connections from home devices potentially defenceless; carelessness arising from exchange of credentials with colleagues to VPN or shared folders.
- **Use of new staff**: newly hired healthcare personnel are inexperienced in the company cybersecurity and privacy policies; sudden arrival of massive new staff can weaken the provisioning, de-provisioning and profiling processes, leading to security issues.
- **Need for ad-hoc IT solutions fast design**: The healthcare sector needs to rapidly design and deploy Apps and back-end systems. Fast design leads to the risk of delivering non-secure solutions.
- **Infection monitoring data flow**: there has been a major request of data flux to monitor infections, to do epidemiological reporting, etc. These data fluxes take place between many institutions; information sharing has a low level of security.
- **Non-healthcare sites used for healthcare operations**: Temporary Hospitals, Churches, nearby Hotels, other empty but usable spaces have been upgraded to “hospital-level”. WIFI systems of these structures, in general, are not secure. Hackers can monitor traffic over the air to steal or access credentials.

Over the last few years, ICT and connected medical devices have become mission-critical for healthcare operations, but still, poorly protected and vulnerable. Therefore, cyberattacks and incorrect staff behaviour are growing risks for business continuity, patients’ safety and data privacy.

The **current level of privacy protection and security must be improved**, also because most of the existing assets were designed when data privacy and cybersecurity were not an issue.

- This COVID era offers the opportunity to renew the systems. A way to radically improve is to invest, to substitute/upgrade “obsolete” assets, adopting a “security and privacy by design” approach. A positive side-effect of COVID-19 in Europe is that it has brought to the surface the weaknesses of the national health services and the needs to invest in e-health and telehealth, with the European recovery funds. The new investment will somehow upgrade the system as e-health and telehealth are the future.

- The European Commission (EC) response to the need for security and privacy by design includes not only the revamping and strengthening of ENISA[195] (the EU Agency for cybersecurity, through Cyber Act 2019/881) and regulatory measures (GDPR, MDR, EU Directive 2016/1148, Cyber Act 2019/881) but also the funding, through the Horizon 2020 programme, of research and innovation projects to develop solutions that are effective and usable in the healthcare context. DEFeND, PANACEA and PAPAYA are three of them.
- The three projects collaborated to design a table as shown in figure 1 that can be very useful to understand how these projects have developed solutions that can help to tackle problem areas and specific challenges relative to the healthcare sector.



How DEFeND, PANACEA and PAPAYA solutions may help: an overview

Problem areas		Envisaged users of the proposed Solutions				Solutions		
Contextual factor	Challenge	Healthcare Organizations	Medical Device Manufacturers	Sw developers	Digital service providers	DEFeND SbD/PbD	PANACEA SbDF (CST, SDSP)	PAPAYA PbD
Investments	• New systems assessment and deployment	✓			✓	✓	✓	✓
GDPR	• Data protection by design and by default (art.25)	✓			✓	✓	✓	✓
	• Records of processing activities (art.30)	✓			✓	✓	✓	
MDR	• Development process compliance		✓	✓			✓	
	• Product compliance		✓	✓			✓	
EU Directive	• HW and SW products compliance	✓	✓	✓	✓	✓	✓	
	• Digital Service compliance	✓		✓	✓	✓		
Covid	• Telemedicine, Smart working	✓			✓		✓	
	• Use of new staff	✓					✓	
	• Need to rapidly develop ad-hoc IT solutions	✓		✓	✓		✓	
	• Infection monitoring data flows	✓			✓			✓
	• Non-healthcare sites used for healthcare operations	✓					✓	

Table 6: An overview of how DEFeND, PANACEA and PAPAYA solutions

[195] https://www.enisa.europa.eu/

6.4.4 The Roadmap to GDPR Compliance in e-Healthcare Services

Anastasia Botsi, ICT Legal Consulting and cyberwatching.eu
www.cyberwatching.eu

The COVID-19 situation is a wake-up call to all the actors involved in the sector. Especially from a GDPR perspective, organisations need to start taking this issue more seriously and seeing this regulation not just as a requirement that is there to make their life difficult but a useful tool that can help and assist in ensuring a safer environment and is more privacy-friendly for the patients, doctors and all that are involved.

There are three main legal frameworks and regulations applicable in the context of the health sector.

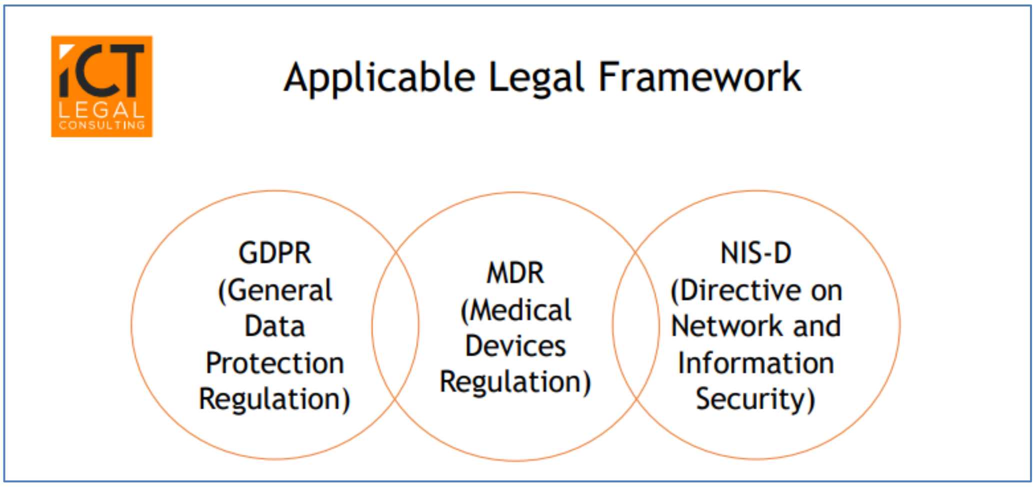

ICT LEGAL CONSULTING
Applicable Legal Framework
GDPR (General Data Protection Regulation)
MDR (Medical Devices Regulation)
NIS-D (Directive on Network and Information Security)

Figure 6: Applicable Legal Framework for the Health sector

GDPR – General Data Protection Regulation:

Indicates principles and obligations relating to the protection of rights and freedoms of data subjects, e.g., data protection by design and by default, and principles of lawfulness, fairness and transparency, and data protection impact assessments, and security measures.

- **Special categories of personal data:** data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.

- **Data concerning health** means personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

MDR – Medical Devices Regulation:

Ensures a consistently high level of health and safety protection for EU citizens for using medical devices:

- Defining devices in the healthcare sector and classifying them
- Designing and manufacturing medical devices
- Making available or putting into service medical devices for human use and placing them on the market.

NIS-D – Directive on Network and Information Security:

Establishes a common level of security for network and information systems focusing on Essential Service Providers and Digital Service Providers, e.g., security requirements, and incident notifications and coordination of computer incident response teams.

The ICT Legal presentation has introduced the Information Notice Tool[196], which was developed as part of the Cyberwatching.eu initiative for informative and awareness purposes, mainly focussed on assisting H2020 Projects and SMEs in evaluating their privacy policies and amending them based on the obligatory components of Articles 13 and 14.

This tool consists of questions about the data processing activities, also providing corresponding recommendations coming directly from ICT Legal Consulting, a law firm with plenty of expertise in the area.

Any organisation that processes personal data must ensure that data subjects are informed about their rights and how to freely exercise them:

- Right of access (Art. 15 GDPR): by what means the persons concerned can obtain the information relating to them.

- Right to rectification (Art. 16 GDPR): how to complete incomplete/inaccurate data.

- Right to erasure (Art. 17 GDPR): allowing the deletion of any data relating to the data subject.

- Right to restrict processing (Art. 18 GDPR): under certain conditions, the data subject may request for the organisation to restrict its processing.

6.4.4.1 Council of Europe Recommendation on the protection of health-related data

Here are a set of principles to protect health-related data, including:

- "Personal data protection principles should be taken into account by default (privacy by default) and incorporated right from the design of information systems, which process health-related data (privacy by design). Compliance with these principles should be regularly reviewed throughout the life cycle of the processing. The controller should carry out, before commencing the

[196] https://cyberwatching.eu/cyberwatching-information-notice-tool

processing and at regular intervals, an assessment of the potential impact of the foreseen processing of data in terms of data protection and respect for privacy, including of the measures aimed at mitigating the risk." [Recommendation 4.2].

- Protecting health-related data flows "Transborder data flows may only take place where an appropriate level of data protection is secured in accordance with the safeguards provided for in Convention 108" [Recommendation 17].

6.4.5 Security and privacy by design for healthcare data governance for Supporting GDPR (DEFeND)

Andrés Castillo, Pediatric Hospital Niño Jesús & DEFEND
Haris Mouratidis, University of Brighton & DEFEND
www.defendproject.eu

DEFeND presented its innovative data privacy governance platform reporting the main project objectives:

- Design and development of a successful market-oriented, platform to support organizations towards GDPR compliance
- Develop a modular solution that covers different aspects of the GDPR
- Automated methods and techniques to elicit, map and analyse data that organizations hold for individuals
- Advanced modelling languages and methodologies for privacy-by-design and data protection management
- Specification, management and enforcement of personal data consent
- Integrated encryption and anonymisation solutions for GDPR
- Deployment and validation of the DEFeND platform in real operations.

Among the main Healthcare and Technical challenges, DEFeND is tackling:

- Redesign hospital data paths according to privacy by design principles;
- Tracking of changes and cancellation of consents;
- Management of health data for research;
- Sharing of health data with other hospitals inside and outside the EU (travellers, tourists, derivations);
- Getting health data from sensors and wearables from patients at home into the hospital (telemedicine contexts);
- Transferring of health data to and from third parties to the hospital (e.g., labs, Insurance);
- Connecting in-hospital emergency department with Emergency Medical Services (e.g., ambulances carrying COVID-19 patients and Multiple Casualties Incidents victims);
- Transforming privacy (social and legal concept, deliberately vague, contextual and subjective) into a technical requirement;
- Deriving technical requirements from GDPR;
- Dealing with conflicts between privacy and security areas;
- Building systems that can support continuous GDPR compliance.

6.4.5.1 DEFeND – Recommendations on Security and Privacy by Design for Healthcare

- **Ensure continuous GDPR compliance**. GDPR compliance mustn't be seen as a one-off but as a continuous effort. In supporting such an approach, privacy-by-design conceptual languages must be developed that consider the context of an organisation and focus on the relationship between privacy requirements, threats/vulnerabilities and privacy-enhancing technologies. DEFeND has developed the SecTro language to support the foundations of such an approach.

- **Embed a culture of privacy governance.** Privacy mustn't be just considered a burden or a regulatory "have-to" but as an aspect that can benefit the whole organisation. Tools, methods and techniques must be developed to embed privacy governance as part of the organisational culture.

- **GO beyond just technical and legal treatment of privacy**. Solutions should follow a holistic socio-technical approach to the management of privacy, supported by common languages across different sectors (e.g., legal, technical, social, ethical) and different domains (e.g., health, public admin, energy). Such treatment of privacy will improve the efficiency and efficacy of organisational and privacy operations, supports financial impact analysis while operating within an ethical framework.

- **Improve decision-making capabilities**. It is important to improve intelligence and predictive capabilities concerning privacy through technological advancements in areas such as artificial intelligence to enable faster response and resolution of privacy concerns.

6.4.6 The PANACEA framework of security-by-design principles applicable to health systems and medical development

Presented by Martina Bossini Baroggi, RINA & PANACEA
www.panacearesearch.eu

Panacea
People-centric cybersecurity in healthcare

Security issues in the healthcare sector start with fragmentation and lack of privacy and cyber awareness. A programmatic approach to the identification, mitigation, and remediation of risk should be developed and implemented at the initial design phase of medical devices, as it is fundamental to introduce right away security aspects, which takes into account cyber risks.

In order to overcome the design limitations of medical devices or systems that include security engineering aspects regarding cyber risks poorly, PANACEA proposes the Security by Design Framework. The main concept is to make systems as free of vulnerabilities and impervious to attacks as possible through different cybersecurity measures that should be integrated into the design process so that the devices will be designed securely from the foundations.

The approach that has been followed was defined taking into consideration ENISA analysis on potential candidates of cybersecurity certification schemes and could be summarized in five steps:

- Context definition
- Relevant standards/certification schemes identification
- Standards mapping, gap analysis and extraction

- Conformity assessment
- Risk assessment

The domain targeted is the healthcare domain and in particular, the focus is on medical devices and systems design. The device lifecycle has been studied and analysed in order to understand the conformity-related activities for each phase starting from the requirements definition to the deployment and use phase.

After that, an analysis of the key applicable standards was carried out to understand what should be considered during the Medical Device and System Lifecycle. Resulting regulations and standards were: GDPR, MDR/IVDR, ISO 27001, ISO 27799:2008, IEC 80000-1:2010, ISO 13485:2016, ISO14971, IEC 62304:2006.

Some of these standards (ISO 27799, ISO 13485 and ISO 80001-1:2010) are specifically considered in the analysis performed by ENISA (Mapping of EOS Security Requirements to Specific Sectors).

All these standards were analysed and links between them were investigated. For each one of the selected standards, the most relevant articles in terms of cybersecurity were extracted in order to define checklists useful to guide the user to assess conformities. Moreover, from the majority of them, taxonomies such as assets/vulnerabilities/threats/security controls were extracted.

The last two steps are conformity and risk assessment. In PANACEA, the conformity assessment, for which continuous evidence collection and audit are essential, is supported by the Compliance Support Tool (CST) and the risk assessment is covered by the Secure Design Support Platform (SDSP).

These two technological solutions compose the PANACEA Security by Design Framework (SbDF). The SbDF was conceived to support medical devices and systems manufacturers for the whole development process to continuously monitor the compliance to standards and at the same time to perform the risk assessment.

CST is designed for internal auditing to support self-awareness on the regulatory side during the development phase, but also for certification auditing as a support to the audit activities. The checklists developed by RINA, extracted by the analysis of several European regulations and in alignment with the ENISA approach, are implemented in CST, which is configured in the Healthcare sector.

SDSP is intended to support the security of a medical device/information system in development, by providing a software platform for risk assessment analysis. Each risk assessment analysis may produce security controls that will lead to new requirements to be embedded in the system in order to improve its resulting security.

The output of the risk assessment is collected in the CST to cover security controls related to risk management and allows to complete the conformity assessment.

In conclusion, the innovation points and the benefits of these solutions could be highlighted as follows:

- Development of tools to support conformity and risk assessment that is fit for the Health Care sector;
- Extraction of taxonomies (vulnerabilities/threats/security controls) from health care most relevant standards in order to take into consideration during risk assessments scenarios that are specific for this sector;

- Use of the Security-by-design principles to lead the manufacturers in the decision-making of possible security controls to be implemented during software/system engineering early phases
- Liaison with ENISA approach and guidelines for the analysis of potential candidates of certification schemes.

6.4.6.1 PANACEA – Recommendations on Security and Privacy by Design for Healthcare

Considering the impact that their widespread adoption may have on cybersecurity**, it is recommended to insert a more explicit reference to Security by Design tools in the next version of the "PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS"** released by ENISA in February 2020, specifying that they can be used in the Plan (analyse and collect requirements) and in the Source (prepare a request for proposal tenders, evaluate received proposals) phases of the Procurement Process. ENISA Guidelines have been used by the Security by design framework (SbDF) and SDSP specifically as a reference for the configuration of Assets and Health Care domain-specific scenarios. As a consequence, during the PANACEA project, a taxonomy of assets and related scenarios has been introduced into SDSP platform so that the procurement types described into ENISA document and these assets are an exact match: from this perspective, the Secure Design Support platform could be evaluated as a practical implementation of ENISA guidelines applied to the risk assessment by design;

As dealt within PANACEA SbDF and CST specifically, **it is recommended to medical device and application providers but also hospitals and policymakers to sustain continuous monitoring of compliance to information security standards of medical devices/information system along the whole development life-cycle process** in order to trigger faster resolution with security health checks, facilitate auditability, reduce complexity and human errors during the operations and maintenance, therefore decreasing the overburden on organizational processes. By the joint focus on this aspect both from producers and consumers of software/medical devices, it is possible to reduce the gap of regulatory information asymmetry between these actors that cause assurance unclarity and vulnerability;

Considering that the EC funds many projects (such as PANACEA) that deliver solutions aimed at improving cybersecurity, and considering the need to digitize the Healthcare Sector (after COVID-19) in the context of the Next Generation EU, it is **recommended that the EC set-ups a funding channel to promote the adoption of those solutions (such as tools for Security by Design)**. This channel could be a co-financing fund that can be used by Healthcare Organization if they use solutions developed through EU Programmes (such as H2020).

6.4.7 PAPAYA - PlAtform for PrivAcY preserving data Analytics Project

Orhan Ermis, EURECOM & PAPAYA
www.papaya-project.eu

The PlAtform for PrivAcY preserving data Analytics (PAPAYA) project is developing privacy-by-design solutions and a dedicated platform for data analytics tasks that are outsourced to untrusted data processors. This will allow stakeholders to ensure their clients' privacy and comply with the European GDPR while extracting valuable and meaningful information from the analysed data.

PAPAYA targets two digital health use cases, namely arrhythmia detection and stress detection, whereby patients' data are protected through dedicated privacy-enhancing technologies.

6.4.7.1 PAPAYA – Recommendations on Security and Privacy by Design for Healthcare

- The PAPAYA consortium recommends that privacy enhancement technologies (PETs) for making the best possible privacy-utility trade-off in privacy-preserving analytics transparent to data subjects. Beyond design considerations of analytics PETs, the selection of analytics PETs, their configuration, and parameter selection are central to this trade-off.
- The PAPAYA consortium recommends that the assessment of privacy enhancement technologies (PETs) against a wide range of attacks, considering both passive adversaries (information leakage) and active adversaries.
- As part of continuous risk management, the PAPAYA consortium recommends that the data collectors should document threats, their associated determined risk and mitigations.

6.4.8 Conclusions

The Cyberwatching.eu webinar on "**Security and Privacy by Design for Healthcare**"[197] provided very useful insights on the main challenges facing the medical sector in ensuring secure integration of services that comply with EU regulations. In order to tackle these challenges, three cutting-edge security and privacy-by-design solutions from Horizon 2020 projects PANACEA, DEFeND and PAPAYA were presented.

The main recommendations from this document are detailed below:

- The current level of privacy protection and security must be improved, also because most of the existing assets were designed when data privacy and cybersecurity were not an issue.
- When processing personal data and especially the special categories of personal data, you need to carefully evaluate the legal basis that the processing activities involved.
- GDPR compliance mustn't be seen as a one-off but as a continuous effort.
- There's a need to improve the privacy enhancement technologies (PETs) to make the best possible privacy-utility trade-off in privacy-preserving analytics transparent to data subjects.
- Next Generation EU and the related recovery plans and investments will be an opportunity to reduce cyber risk if and only if security and privacy by design approaches are adopted by all involved parties.
- While waiting for definitive directions on how to implement the cyber act, hospitals could set up pre-requirements for contracts with medical device manufacturers and system/service providers. These should state that, in face of similar products, preference is given to those that comply with the security and privacy by design approach.

[197] https://cyberwatching.eu/security-and-privacy-design-healthcare

7 Conclusions & Recommendations

This deliverable has addressed the complex landscape of cybersecurity services and how the regulations, emerging technologies, ethics, risk assessment, user needs, developers' requirements, national requirements all play an intrinsic part of the cybersecurity services landscape. The survey launched during the pandemic situation provided a unique and practical insight into where privacy-sensitive areas lie from the perspective of citizens. The webinars were an opportunity to discuss areas of focus and to showcase EU projects' work.

Below, are a set of recommendations, suggestions, further guidance and/or solutions which have been summarized from the research, actual feedback and discussions within this deliverable; some points are of a more practical nature for the attention of cybersecurity services at large (i.e., including developers of services, tools, systems or end users of such services), others are of a more regulatory nature for the attention of policymakers and data controllers.

7.1 Recommendations from Chapter 3 on Emerging Technologies

Artificial Intelligence

AI, GDPR and Purpose Limitation:

- **It is recommended that limitations or further requirements on the use of personal data within AI-based systems be imposed.** The relevant controller should develop algorithms (and, in particular, machine-learning algorithms) ensuring that personal data is not processed for purposes beyond the scope of their collection (carrying out a compatibility test, where necessary) – **any guidance which can be offered by policy-makers and competent authorities in this regard would prove invaluable.**

- **It is recommended that controllers** should carefully analyse the systems that they wish to implement and **ensure that they are able to provide clear and adequate information to data subjects on how those systems will work and, in particular, the purposes for which they will use personal data** – guidelines or templates on how to disclose such information in a digestible way for individuals (consumers), considering, where relevant, the requirements of Art. 13(2)(f) and 14(2)(g) GDPR, could be of great benefit to AI developers and users.

AI, GDPR and Transparency and Lawfulness

- **It is recommended that guidance and/or means be developed for AI developers and users to provide dynamic information notices** (using illustrations, flowcharts, videos, etc.) to data subjects, seeking to inform them about the **key aspects of how their personal data will be used**, walking them through the AI's process step-by-step and, where relevant, asking for their consent to the parts of the processing which are known at the time. This information and consent request could then be updated/renewed in the case of any foreseen substantial changes at a later stage. However, in order for this to function in a manner similar to the possibility foreseen by Recital 33 GDPR, it is important that the renewal of consent is asked prior to the further processing which relies on it being carried out; this would require **developers to design AI so that it does not automatically proceed with incompatible**

further processing of personal data, unless it is confirmed – by the developer or user – that a legal basis for this exists.

- **It is recommended that developers be made aware of the regulations in force** and **design AI-based systems to allow data pertaining to specific individuals to be extracted from a dataset and not further considered by the system in question**. Guidance and further research on how this can be attained in practice – in particular, considering that, where automated individual decision-making is concerned, Art. 22(2)(c) GDPR is, as our practical experience has shown, the most likely exception to be relied on – would be welcomed.

AI, GDPR and Security

- **It is recommended further clear and understandable guidelines be developed for AI developers and users on (1) AI risk management, and (2) examples of security measures**, at varying levels of sophistication (to account for developers and users of different sizes, types and economic capabilities), which may be considered in order to properly address identified risks.

IoT

IoT and Data Minimisation

- It is recommended that IoT developers/providers consider to **more comprehensively design IoT devices and services with the principle of data minimisation in mind**, incorporating the concepts of data protection by design and by default into the development process. In particular, as has been noted by the Article 29 Data Protection Working Party in the past, the principle of data minimisation "*specifically implies that when personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously*".

- One of the ways in which this could be done, which would also address the problem of individuals' lack of control over IoT data flows, would be for developers to consider **creating 'privacy dashboards' or 'privacy interfaces' for individuals** – these dashboards/interfaces, which could be available on specific devices (such as an individual's mobile phone), could act as a control centre for that individual's IoT devices and services, offering information and options concerning data receipt and transmission for each device or service.

- **It is recommended for Controllers to consider if this problem which could be addressed by policy and regulation, where stricter requirements on data collection and transmission could be enforced on IoT developers**. Possible solutions could include an obligation to build in 'do not collect' switches or permissions into IoT devices and services, so that individuals can disable or limit collection and transmission of data before even activating the device or service.

IoT and Purpose of limitation:

- The imposition of limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services, seems to be a reasonable solution. **It is recommended to provide individuals with control over which data may**

be collected and transmitted, through the use of dashboards, privacy centres or other privacy enhancing technologies, - this would already be a large step to achieve this goal.

- **It is recommended that contractual limitations between stakeholders (through Data Management Agreements) be imposed on the further processing of received personal data** as this could be a key step in ensuring that appropriate limitations are in place, particularly in the absence of stricter and clearer policy on IoT data collection, sharing and repurposing.

IoT and Transparency and lawfulness:

- Two suggestions to help comply with the principle of transparency are the use of **just-in-time notifications and periodic notifications,** which may allow developers to deliver specific and relevant information to individuals at times when they are most likely to be able to apprehend such information. Furthermore, as noted above, **the development of privacy dashboards or control centres for individuals may be fundamental in this respect**, as it can allow not only the creation of a central point where information on the processing activities undertaken may be accessed, but also where individuals may set their preferences in regards to data collection/transmission and, potentially, also exercise their rights under the GDPR directly (e.g., accessing, rectifying, deleting or exporting personal data captured by IoT-connected devices).

- It is recommended that **further research continue and guidelines be produced on effective means by which information on processing activities carried out via IoT can be delivered to individuals –** particularly those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by).

IoT Security:

- It is recommended that further research continue and the development **guidelines and procedures be developed to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices.**

- Furthermore, an additional consideration would be the **implementation of end-to-end encryption regarding all data collected and transmitted by and between IoT-connected devices and services.**

- It is recommended that further security measures and best practices which should be considered include those within **ENISA's guidelines on Good Practices for Security of Internet of Things.**

7.2 Recommendations from the Survey on Privacy and Covid-19

Based on the findings extracted from the survey, it was concluded that citizens had a heightened appreciation for their privacy and felt a strong need to control their personal data. Several areas of concern were expressed, in particular, as regards to the contact tracing apps, sharing of health information with government and / or national authorities, with employers and health professionals, and also a fear of a lack of state-of-the-art security measures. These concerns surfaced in various ways, for example:

- In contact tracing, a major concern was the fear of the sharing of information with a third party, the lack of secure storage, the use or abuse of such data for malicious ends, or simply a lack of trust that a government may use personal data.
- In general, there was concern about a lack of security concerning personal health-related data, a lack of awareness of data protection on the side of health professionals and fear that there was a lack of state-of-the-art security measures in the field of health-care.
- Citizens, themselves, were concerned about the amount health information data that could/should be shared with employers.
- A general feeling of distrust was perceived with respect to the implementation of the legal framework or the technical capabilities for such data processing at a government level.
- Citizens also expressed that their concern was not so much with the privacy policies but in the way they were implemented and that data breaches could become more common and under reported.
- An increasing demand for exercising the citizen's data subject rights was frequently mentioned.

Based on the above, the following are a set of recommendations that arise from the feedback of citizens and which cybersecurity services could play an important role to help improve the implementation of the commitments which authorities and/or organisations make to individuals.

Recommendations resulting from the Survey
Ensure a secure framework: • It is recommended that **cybersecurity services focus on providing a more secure collection and storage of personal data, possibly also including anonymity**. This can be especially useful for public and governmental institutions that may, at times, lack proper technical and security state-of-the-art.
Provide citizens with comprehensible information related to their data collection: • When personal data is collected, stored or shared, it is crucial for citizens to be provided with clear explanations of the implemented security measures within privacy policies. It is, therefore, recommended that **cybersecurity services provide guidance and clarity to citizens on the techniques, technical means and tools for exercising data subject rights is integral during the extraordinary times of the pandemic**. • It is recommended to provide **clarity on the steps to exercise data subject rights**, as well as more straightforward ways to track data flows.
Improve compliance posture and consider personal data a priority • It is recommended that **cybersecurity services and developers improve their compliance posture and consider personal data as a main priority, by design and by default.** In this way, cybersecurity services could fill in the

gap between the need to exercise data subject rights (to “control” personal data) and the technical means with which this can be carried out and cybersecurity services could achieve this goal by offering the technical and efficient means to ensure this. A positive outcome, for example, would be that data subjects could exercise their right to interoperability of apps.

Interoperability between EU member states:

- It is recommended that **greater interoperability between tracking applications** (for example, if one is under quarantine in Italy, if they travel to France, they can transfer the relevant data to the application used in France) be established so as to allow data to be transferred where required in a secure way.

Risk assessment in health care systems:

- It is recommended that **cybersecurity services focus on offering privacy by default** to the healthcare systems, software, and applications used.

- It is recommended that **cybersecurity tools and services use privacy by default** as a vehicle to both **carry out a proper risk-assessment of the processing activities in the healthcare sector.**

- It is recommended that stakeholders **ensure that the said privacy-related risks are explicitly communicated to the data subjects**.

Health care systems and data protection:

- It is recommended that **cybersecurity tools and services** should allow for **customization by health institutions in order to guarantee data protection** to special categories of personal data.

- It is recommended that **cybersecurity services focus on appropriate means for data subjects to exercise their rights in the field of healthcare applications, or software,** as well as **embed privacy settings customization**, where possible**.**

- It is recommended **that health care systems use cybersecurity services in order to enhance the data breach management**. Cybersecurity services could offer guarantees, namely, by ensuring that an appropriate management of cybersecurity attacks is available to the healthcare systems.

Training of health professionals with regard to protection of data collected

- It is recommended that **health professionals be trained so as to be aware of the security measures implemented** by the health institution, and to be able to **deliver adequate information to patients when sharing of health-related data.**

7.3 Recommendations from Webinar on Protection of Critical Infrastructures

The recommendations from Cyberwatching.eu webinar on **“Effective protection of Critical Infrastructures against cyber threats”** held on 29 October 2020 are summarized below:

Protection of Critical Infrastructures:

Secure Integration of new technologies:

Cybersecurity needs to consider 360° aspects. It is a continuous process to ensure the security of new technologies that are being integrated into critical infrastructure and which also bring new vulnerabilities and changing attacks.

Regularly update skills:

Not only are systems designed and maintained, but also the skills. The human aspect is extremely important and training is fundamental. Cybersecurity is not a destination, it is a journey, so it is key to keep up to date to cope with the fast-evolving threat landscape.

Artificial Intelligence:

Further efforts need to be applied to the development of more advanced systems that will rely on advanced technologies such as Artificial Intelligence (AI) and machine learning techniques to provide more advanced functionalities, which can be shared with the operators in order to deal with such threats.

Critical Information Infrastructures should incorporate:

- Security Monitoring and Analysis capabilities for preventing and detecting any kinds of anomalies, threats, risks.
- Social Information Mining capabilities to extract data from distributed online web sources offering to the security operators’ information on activities and situations that can become a threat to the infrastructures.
- Data Fusion and Event Management capabilities to provide the intelligence needed for an effective and efficient analysis of a security event.
- Risk Evaluation capabilities to thoroughly assess the vulnerabilities of their interconnected cyber assets and to continuously estimate the probability of all possible cyber-attacks.
- Threat Intelligence capabilities to facilitate and promote the secure and privacy-aware sharing of incident-related information.

Training:

- Simulate a complete corporate environment with real-world attacks/threats. The staff of Critical Infrastructure should have the opportunity to play both attacker and defender roles in order to better understand how vulnerabilities can be exploited and how to handle cyber-attacks and defence in real life.
- Train both technical and non-technical staff as people at all levels contribute to the risk and protection of an organization’s cybersecurity practice. Organisations should consider a systematic delivery of awareness training programs as well as further development and practical training for staff in cybersecurity specialist roles.

- Easily access secure online tools for training and upskill their employees. In accordance with most of the global and European bodies, it is recommended to move away from the traditional training methods to those of the more tailored and practical ones.

Find the weaknesses:

- Look at the security infrastructure with the eyes of a cyber attacker to find the weakness to break into the infrastructure. Only then will it be possible to discover the weakest points and only then will it be possible to secure them.
- Try to make computers crash before taking steps to protect them: if the result is to successfully crash the computer, then at least one weak point has been found.
- Before solving a problem ask "why has this problem not been solved yet?" This can reveal all the areas where previous attempts have failed and where new attempts may have an opportunity to succeed.

7.4 Recommendations from Webinar on EPES and Smart GRIDS

The recommendations from the Cyberwatching.eu webinar on "**EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks**" held on 12 November 2020 are, as follows:

EPES and Smart Grids:

Compliance to Data Protection regulations:

- To have under control the status of the organization compliance to Data Protection, a compliance status for each of the GDPR Principles for the whole organization, for each department and each third party and compliance status information for the data subject.
- To define the list of processing activities, the connections with Departments and Third Parties involved in the activities' linked assets, systems and threats.
- To perform Threats Analysis, Data Minimization Analysis, Privacy by Design/by Default based on the result of the analysis and design modelling techniques, and continuous Risk Assessment.

HR:

- Invest in promoting the personnel of an organisation from a profile of potential cyber-threat to a profile of valuable cyber-security asset.

Risk Assessment:

- Get to know the vulnerabilities of the organization in order to be in a position to defend it.
- Auditing and monitoring are key mitigation policies for a robust cyber-reality.
- Being able to detect anomalies and ongoing attacks is the first step towards protecting assets.
- Encrypt information - information is valuable.

Critical Infrastructures:

- **Adoption of the IEC 62351 security controls**. IEC 62351 establishes a set of security and privacy controls, specially designed for industrial environments. In particular, it consists of 14 parts that cover multiple cybersecurity and privacy aspects, such as authentication, access control, privacy, security profiles, key management and security architecture.

- **Timely intrusion detection**. The critical infrastructures include ingredients and communications that were designed without having cybersecurity in mind. However, they are necessary for their core operation. Therefore, appropriate intrusion detection mechanisms should be adopted, considering the unique properties of each individual infrastructure.

- **Timely mitigation.** Smart mitigation mechanisms should act as fast as possible, thus mitigating or even preventing the potential cyberattacks. Smart authentication and access control systems compose characteristic examples. Moreover, the intentional islanding and the grid restoration compose efficient mitigation measures for the energy-related CIs. Finally, the proper usage of SDN technology can contribute significantly to the mitigation of the possible intrusions coming from malicious insiders.

- **Privacy-preserving**. Critical infrastructures comprise a plethora of sensitive data. This data should be protected by many privacy risks. Blockchain, holomorphic encryption and differential privacy are sufficient mechanisms that can guarantee the confidentiality and authenticity of the various data transactions.

- **Threat-Intelligence.** Cyberattacks are evolving rapidly. Therefore, it is crucial to adopt and design adequate systems and methods that can mine information and knowledge about these cyberattacks and malware. Honeypots and anonymous repositories of incidents are characteristic examples that can contribute to this aspect. However, the presence of proactive relevant countermeasures is necessary.

7.5 Recommendations from Webinar on Risk Management

The recommendations from the Cyberwatching.eu webinar on **“Cybersecurity risk management: How to strengthen resilience and adapt in 2021**“ held on 23 November 2020 are, as follows:

Strengthen resilience and adapt in 2021:

Risk Assessment:

- **Improve Continuous Risk Monitoring**: More specifically, a successful continuous risk monitoring system is required to continuously assess risk levels, including the performance of the implemented cyber security controls.

- **Risk Transfer**: If an organization has installed tools and methods to mitigate risk, but not at an acceptance level, risk transfer is a solution.

- **Comply with Guidelines and Regulations**: The compliance of an organization with guidelines and regulations related to cyber security can reinforce the organization against potential cybersecurity incidents.

- It is important to get **a vulnerability assessment as thorough as possible**, since dangers and gaps may come from multiple sources such as i) methodologies ii) knowledge iii) distribution of administrative rights iv) information segmentation policy v) authentication policies vi) etc.

Resilience:

- **Resilience should be incorporated with risk management**. Including resilience allows systems to be able to handle more adverse events, including ones that are unknown or have too low of an occurrence probability to be considered in traditional risk management.

- One of the outputs of the risk and resilience management process should be the **quantitative measurement** of many specific resilience indicators, each one related to a specific threat. For reasons of convenience and to reduce complexity, it is necessary to **prioritize threats in terms of probability and level of impact**, and then focus on the most relevant.

- When investigating threats and adverse events to improve cybersecurity, cyber-attacks should be considered, but also **physical-cyber attacks**. Which is to say that physical events, whether intentional, accidental or natural, may lead to problems in the cybersphere and therefore **should be investigated** and included in any risk analysis related to cybersecurity.

- Furthermore, in the event of physical and cyber threats that can occur at the "same" time and/or in the "same" place, even in a completely independent way, the **aggregate impact should be assessed**, and the countermeasures to be implemented should be unified.

- Factor into risk management human aspects and staff security profiles, and analyse behaviour such as the sharing of credentials and other weak links or vulnerabilities caused by negligence or carelessness. **Ensure mitigation actions include training or secure behaviour nudging**.

Risk Management for MSEs:

- Researchers must commit to more accurately reflecting the concept of 'threat' in their risk management solutions. This is an important step towards limiting the discrepancy in the understanding of risk between theory and practice.

- **Work together with CERTs, NCSCs, and other governmental organisations** in cybersecurity projects is essential. Not only do they have information that accurately reflects the state of the world, but including them in projects helps to harbour trust among potential users of the cybersecurity risk management solutions we offer.

- **Cybersecurity risk management is a process**, not a 'quick check'. Cybersecurity risk management solutions should always aim to help users over an extended period of time, for example by incorporating an education framework.

- **Consider a multi-dimensional approach to risk management**, across the business, access, network and human layers with attack paths for each layer to reduce organisational risk and impacts on business processes.

Risk Management for SMEs:

On the process of addressing risk management:

- Go step by step and apply a mid to long term approach.
- In the event you are facing your first attempt, try an existing and robust lightweight label to acquire a solid background.
- Start with a clear understanding of rules and try to make a decision that will not compromise your business.
- Then try to understand, evaluate and assess the gap of security. Join a consulting firm to help you put measures in place.
- Then you will be more prepared to address a certification process because certification is achievable and a strong value of differentiation.

SME Guide:

- Use the “SME Guide for the Implementation of ISO/IEC 27001”[198], dedicated to SMEs for the implementation of ISO/IEC 27001 on information security management. It is a comprehensive guide a series of practical activities that can significantly help with establishing or raising information security levels within an SME, thereby strengthening business and facilitating partnership opportunities within local and EU markets.

Cyber insurers:

- **Take a comprehensive approach** and provide customers with a platform for creating, monitoring and adapting cyber insurance policies, thereby providing cyber insurance policies customised to the needs of individual customers and their organisational risk assessment.
- **Ensure dynamic and continuous risk management** which is essential as it will lead to a more thorough and accurate basis for monitoring cyber insurance policies, thereby reducing the risk and cyber insurance management costs and consequently policy premiums.

Cyber system providers:

- **Improve security through the provision of automated risk management** and S&P assessment and certification services,
- **Incentivise service providers** to improve their security according to reference security standards and benchmarks, to reduce their insurance premiums, and
- **Establish liability** through the undertaking of cyber insurance policies.
- **Involve end-users in testing new tools and solutions** to ensure usability, effectiveness in reducing threat surface and affordability.

Health care framework:

- **Ensure the organisation’s compliance with the current European legal framework**. More specifically, healthcare organisations should take action to address the requirements posed by EU legislation and directives, such as the General Data Protection Regulation (EU) 2016/679 (GDPR), the Directive 2011/24 (EU) on patients’ rights in cross-border healthcare (Patients’ Rights Directive), the Regulation (EU) 2017/745 on medical devices (MDR), the Regulation (EU) 910/2014 on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation) which introduces the mutually recognised electronic

[198] http://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

identification of patients and healthcare providers facilitating the proper cross-border provision of healthcare services, as well as the Directive (EU) 2016/1148 on network and information security (NIS Directive), and the Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), both of which are expected to become mandatory in the near future.

- **Improve the cyber hygiene culture among personnel.** The definition of strategies for raising cybersecurity and data privacy awareness focusing on the specific needs of different employee groups in a healthcare organization (i.e. Admin, Medical, IT, Mgmt. /Security), can help identify and close group-specific gaps through the recommendation of tailored human-centric actions/controls.

- **Minimize the impact of possible violations of the organisation's infrastructure and data.** Medical facilities should invest in cybersecurity risk management solutions, to complement and extend their existing cybersecurity infrastructures. A risk-based approach that takes into account risks not only coming from direct cyber attacks but also from knowledge gaps and legal breaches should be adopted by the higher management to address the future cyber threats in a holistic way.

- To increase cybersecurity resilience in healthcare IT infrastructures, **adopt new models that can rapidly capture and analyse multiple variables** in a potential attack and proactively and continuously monitor current risks, supporting operators with increased situational awareness and guided and interactive risk analysis.

7.6 Recommendations from Webinar on Security and Privacy by Design for Healthcare

Security and Privacy by Design for Healthcare

Investment:

- The Covid situation has surfaced the necessity for Europe to invest, to substitute or upgrade "obsolete" assets and adopt a "security and privacy by design" approach.
- Considering that the EC funds many projects that deliver solutions aimed at improving cybersecurity, and considering the need to digitize the Healthcare Sector (after COVID-19) in the context of the Next Generation EU, it is **recommended that the EC set-ups a funding channel to promote the adoption of those solutions (such as tools for Security by Design)**. This channel could be a co-financing fund that can be used by Healthcare Organization if they use solutions developed through EU Programmes (such as H2020).

Compliance to Regulatory Framework:

- **Ensure continuous GDPR compliance**. GDPR compliance must not be seen as a one-off but as a continuous effort. In supporting such an approach, privacy-by-design conceptual languages must be developed that consider the context of an organisation and focus on the relationship between privacy requirements, threats/vulnerabilities and privacy-enhancing technologies.

- **Embed a culture of privacy** governance**.** Privacy must be considered as an aspect that can benefit the whole organisation. Tools, methods and techniques must be developed to embed privacy governance as part of the organisational culture.
- **GO beyond just technical and legal treatment of privacy**. Solutions should follow a holistic socio-technical approach to the management of privacy, supported by common languages across different sectors (e.g., legal, technical, social, ethical) and across different domains (e.g., health, public admin, energy). Such treatment of privacy will improve the efficiency and efficacy of organisational and privacy operations, supports financial impact analysis while operating within an ethical framework.
- **Improve decision-making capabilities**. It is important to improve intelligence and predictive capabilities concerning privacy through technological advancements in areas such as Artificial Intelligence to enable faster response and resolution of privacy concerns.

Security by Design:

- Considering the impact that their widespread adoption may have on cybersecurity**, it is recommended to insert a more explicit reference to Security by Design tools in the next version of the "PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS"** released by ENISA in February 2020, specifying that they can be used in the Plan (analyse and collect requirements) and in the Source (prepare a request for proposal tenders, evaluate received proposals) phases of the Procurement Process. ENISA Guidelines have been used by the Security by design framework (SbDF) and SDSP specifically as a reference for the configuration of Assets and Health Care domain-specific scenarios.
- **It is recommended to medical device and application providers but also hospitals and policymakers to sustain continuous monitoring of compliance to information security standards of medical devices/information system along the whole development life-cycle process** in order to trigger faster resolution with security health checks, facilitate auditability, reduce complexity and human errors during the operations and maintenance, therefore decreasing the overburden on organizational processes. By the joint focus on this aspect both from producers and consumers of software/medical devices, it is possible to reduce the gap of regulatory information asymmetry between these actors that cause assurance unclarity and vulnerability;

Risk Management:

- It is recommended that privacy enhancement technologies (PETs) be used for making the best possible privacy-utility trade-off in privacy-preserving analytics transparent to data subjects. Beyond design considerations of analytics PETs, the selection of analytics PETs, their configuration, and parameter selection are central to this trade-off.
- It is recommended that the assessment of privacy enhancement technologies (PETs) be used against a wide range of attacks, considering both passive adversaries (information leakage) and active adversaries.
- As part of continuous risk management, it is recommended that the data collectors should document threats, their associated determined risk and mitigations.

To conclude, this deliverable presents a number of conclusions and a comprehensive set of recommendations, which result from EU projects' work and from direct stakeholder feedback. The Conclusions represent not only recommendations for cybersecurity service providers and users of such services, including SMEs, but also for the attention of high level decision-making authorities, and the healthcare system which needs attention given the many issues arising from Covid-19.

Although the format of the Third Concertation event had to be changed due to the Covid crisis, the output set of key recommendations that can be seen from the above, represent very useful suggestions, which can be implemented, and which will have significant impact well beyond the life of this project. The multiple webinars replacement of the Third Concertation event may be even more important than the original expected results given the different and relevant focus areas, the feedback and wide participation (much more than a physical event would have had).

We will continue to pursue further the feedback from the stakeholder community, especially within the planned roadmap deliverable due at the end of the Cyberwatching.eu project. And we expect that the recommendations found herein will be carefully considered for the future.

8 List of Acronyms

Acronyms	Explanation
AIA	Algorithmic Impact Assessment
AI	Artificial Intelligence
ALTAI	Assessment List for Trustworthy Artificial Intelligence
CA	Certification Authority
CAT	Cybersecurity Assessment Tool
CERTs	Computer Emergency Response Teams
CI	Critical Infrastructures
CICPM	Cyber Insurance Coverage and Premium Module
CII	Critical Information Infrastructures
CoAP	Constrained Application Protocol
cPPP	contractual Public-Private Partnership
CRMM	Continuous Risk Monitoring Module
CSIS	Centre for Strategic & International Studies
CST	Compliance Support Tool
CTI	Cyber Threat Intelligence
DBM	Data Breach Management
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DPIA	Data Protection Impact Assessment
DPM	Data Process Management
DRMP	Dynamic Risk Management Platform
DSP	Digital Service Provider
DSS Lab	Decision Support Systems Laboratory
EDA	European Defence Agency
EDPB	European Data Protection Board
ECSO	European Cyber Security Organisation
EGD	European Green Deal
ENISA	European Union Agency for Cybersecurity
EPES	Electrical Power and Energy System

Acronyms	Explanation
FPG	Fondazione Policlinico Universitario Gemelli
GDPR	General Data Protection Regulation
GTM	Game-Theoretic Module
HLEG	European Commission High-Level Expert Group
HPC	High Performance Computing
IEC	International Electrotechnical Commission
IoT	Internet of Things
M2M	Machine-to-machine
MENSA	Micro sElf-orgaNiSed mAnagement
MEP	Members of the European Parliament
MFF	Multiannual Financial Framework
NGEU	Next Generation EU
NIS	Network and Information Security
NIS-D	Network and Information Security Directive
OES	Operators of Essential Services
PAT	Privacy Assessment Tool
PET	Privacy Enhancement Technologies
R&I	Research and Innovation
SBA	Security Behaviour Analysis
SbDF	Security by Design Framework
SBS	Small Business Standards
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SDSP	Secure Design Support Platform
SG	Smart Grids
SGS	Société Générale de Surveillance SA
SIEM	Security Information and Event Management
SME	Small and Medium Enterprise
SRIA	Strategic Research & Innovation Agenda
UCSC	Rome Catholic University School of Medicine

9 List of Annexes

Annex 1: Survey on Privacy Risks Related to Covid-19

The 2020 pandemic created an unprecedented communications and interactions environment where the dependency on digital information and security was of paramount importance. People were forced to work from home without much prior notice. Work/organisational data was migrated from secure systems to personal devices. Meetings went from face-to-face physical events to virtual interactions via web-based video conferencing and teleconferencing software and applications. Families relied on digital means of communication to maintain social ties. The elderly found themselves needing to adapt to such means of communication to keep in contact with loved ones. Citizens may have been asked to share their location and health data via mobile applications in order to safeguard themselves and their community. The combination of these requirements and behaviours led to paradigm shifts which raised weakness and threats which hitherto had not existed. Data privacy became even more sensitive.

The objective of this survey is to understand the change in social interactions and at the same time to understand society's acceptance of the social good of people giving up some of their privacy (as part of our Cyberwatching.eu project - your personal details will not be asked for and only the information from the survey will be stored). The results will be collected and analysed in the deliverable 3.5 (Risk and recommendations on cybersecurity services) to be submitted on February 2021.

In which country are you based?

(Optional)

Online transactions, work, communication, entertainment

Do you work at home? (multiple choice possible)

□ Yes, before the pandemic
□ Yes, during the pandemic
□ Yes, I have always had the flexibility to work from home
□ No, my work obliges me to be at my place of work

Has it changed during the pandemic?

□ Yes □ No

If “Yes”, briefly explain how:

□

Do you have a cybersecurity environment at home to remotely access your work (e.g. VPN, login and password etc.):

□ Yes □ No

If “Yes”, what kind of security is implemented:

□ VPN
□ Login and password
□ Electronic Key Card Access (which type (small description)?)

□ Hard drive encryption
Other (which?)

Comment:

How many devices do you use to access your work data (email, database, intranet etc.)

□ Work laptop
□ Personal laptop
□ Work Desktop
□ Personal Desktop
□ Work mobile
□ Personal mobile
□ Electronic connected watch
□ Other wearable device(s) (which one(s)?)

□ Other connected devices (not wearable – which one(s)?)

Do you believe that company data is properly protected and secured?
□ Yes □ No

Privacy

Do you feel that you have sacrificed your privacy during Covid-19?
□ Yes □ No

If “Yes”,
Do you think that this sacrifice of your privacy is justified?
□ Yes □ No

If “Yes”, explain why:

If “No”, explain why:

Privacy and Contact tracing/tracking apps

Does your government or public authority have a Covid-19 contact tracing/tracking app?

□ Yes □ No

Do you use it?

□ Yes □ No

Is it mandatory to use it (or, was it mandatory during the peak of Covid-19)?

□ Yes, it was mandatory during the peak of Covid-19 but no longer currently mandatory

□ Yes, it was mandatory during the peak of Covid-19 and it's still mandatory

□ No

If you use it, what are your concerns?

□

If you do not use a contact tracing tracking app, why do you not use it?

□

Do you trust that your government or public authority **protects** the personal data you share or have shared through the contact tracing tracking app?

□ Yes □ No

General Data Protection Regulation (GDPR)

Are you concerned that during this crisis your personal information could be controlled by the government?

□ Yes □ No

What are your concerns, if any, regarding personal data collection?

□

What apps do you use that you feel could be tracking your movements? (Multiple selection is possible)

Google
Google Maps
Facebook
WhatsApp
Instagram
LinkedIn
Wordpress
Email system
News website
Other

Do you feel an increasing need to have control of your personal data during this time? (e.g., by exercising your data subject rights)

□ Yes □ No

Do you feel a greater appreciation of the laws on privacy and data protection after the Covid-19 pandemic? (e.g., GDPR)

□ Yes □ No

Do you have higher expectations from Privacy Policies?

□ Yes □ No

If "Yes", what type of expectations do you have? (e.g., a need for easier to understand information, explanations of safety measures, clear steps on how to exercise your rights)

Do you have other concerns about privacy?

□ Yes □ No

If "Yes", please explain further:

Health Data

Do you have concerns about the privacy of your health records?

□ Yes □ No □ I don't know

Do you have to provide any health information to your employer?

□ Yes □ No □ I don't know

If "Yes", what do you disclose to your employer?

Do you provide your health information to other organizations?

□ Yes □ No □ I don't know

Has your doctor adequately informed you on your data's cybersecurity?

□ Yes □ No □ I don't know □ Not applicable

Do you have any other concerns about your health data?

□ Yes □ No

Annex 2: Cyber Risk Temperature Tool Questionnaire

Self-Assessment Tool

1. How good do you think your company's IT security is? Please choose from 1 to 7, where 1 is “not secured” at all and 7 is “totally secured”.

2. How dependent is your company on IT systems? Please choose from 1 to 7, where 1 is “not dependent” and 7 is “highly dependent”.

3. How do you consider the knowledge of the employees of the company about cyber security terms? Please choose from 1 to 7, where 1 is “there is no knowledge” and 7 is “high level of knowledge”.

Vulnerability assessment

1. Are there any planned specific or refresher courses about cyber security?

- » YES [0]
- » NO [10]
- » NO, but the topic is seen in the general courses [5]

Training courses aimed at increasing staff knowledge and awareness of issues such as the use of IT resources and the risks arising from such use are essential in order to prevent and mitigate IT risk. For example, in Italy, only 43.6% of companies state that they provide courses related to IT security[199], although the need for such courses is widely recognized.

In case the answer to question "1" was "yes":

1.1 To whom are these courses directed?

- » Leadership area [2]
- » All members of the organization [0]
- » Selected employees [2]

2. In your company are there any resources with cyber security competencies?

- » There are no resources with these competencies in the company [10]
- » There are resources that are not fully engaged in these activities [5]
- » There are specialised resources dedicated to cyber security activities [0]

The ICT security manager has the task of defining the security policy of the information system and assessing the risks associated with the use of specific IT tools. The ICT security manager should be distinguished from the IT operator, who carries out operational functions of maintenance and support of information systems.

3. In your company is there one (or more) best practices/cyber security framework?

[199] Source: “Rapporto clusit 2020”

- » The company is certified ISO 27001 [0]
- » We follow particular best practices (e.g. OWASP NIST sp 800-53, COBIT) [5]
- » No, we do not have a certification solution and we do not follow any particular best practices [10]

ISO 27001 is a standard that defines the requirements for setting up and managing an information security management system. The purpose of this certification is to protect data and information by ensuring its integrity, confidentiality and availability. It sets out the requirements for an ISMS aimed at the proper management of sensitive company data.
There are also numerous best practices that, unlike ISO 27001, do not require certification such as the Open Web Application Security Project (OWASP), NIST sp 800-53 and the Control Objectives for Information and related Technology (COBIT).

4. What percentage of staff have administrative rights to company systems?

- » Between 0% and 25% [0]
- » Between 26% and 50% [5]
- » Between 51% and 75% [10]
- » More than 76% / we do not apply a particular policy for administrative rights. [15]

Administrative rights, and in general any kind of user rights, means that the holder can take potentially harmful actions, such as:

- » The voluntary or involuntary application of changes that may reduce the level of network security.
- » The introduction of malware that may adopt potentially harmful changes.
- » The theft of access credentials which, with administrative rights, would allow for full use by the abductor.

To increase security accordingly, it is necessary to limit the assignment of administrative rights to what is strictly necessary, ensuring that the privileges assigned are in line with each user's corporate responsibilities and tasks.

5. What kind of Acceptable Use and Access authorization policies are adopted?

- » Within the company, everyone can see all the information available [10]
- » Access to information is segmented by operational area [5]
- » Access to information is segmented by necessity [0]

An Acceptable Use Policy (AUP) defines the acceptable and unacceptable uses of the company's information resources and IT equipment (computers, wireless devices, telephones, etc.). An appropriate and well-structured policy clarifies the criteria adopted with regard to privacy, user responsibility and personal use of company resources, as well as clarifying the consequences in case of violation. The authorization policies determine the different levels of access to information. An information management system determines whether, when and to which parts of a company's database, the employees are allowed access. These controls define the access to critical information of the company.

6. How does authentication to login into the company's network work?

- » Through a one-factor authentication [5]
- » Through a two-factor authentication [2]
- » Through a three-factor authentication [0]
- » Free access [10]

A user authentication policy can be used to ensure that only certain people can access certain resources in your organisation. User authentication policies are designed to ensure that the person requesting sensitive information and data is authorised to access that information.

7. How often is it required to change of the password for access to the company's network and to the company's resources?

- 6 months or less [0]
- More than 6 months [5]
- Never [10]

A frequent change of password improves security of the company's network and resources.

8.[200]How often do you subject your systems to a **Vulnerability Assessment** and then apply a **Remediation Plan**?

- Monthly frequency [0]
- Quarterly frequency [3]
- Semi-annual frequency [5]
- Annually or more frequently [8]
- Vulnerability Assessment is not carried out [10]

The Vulnerability Assessment (VA) aims to bring out all the critical points and possible vulnerabilities of the IT infrastructure and network from a security point of view. The VA ends with a report containing the detected vulnerabilities with their respective severity. But the VA alone is a useless document if it is not accompanied by appropriate corrective actions (where necessary), therefore the execution of a Remediation Plan that is consistent with the results obtained from the assessment is also very important. This operation should ideally be carried out on a monthly frequency.

9. Is an Intrusion Detection System in place?

- YES [0]
- NO [10]

Intrusion detection systems are used to protect the company's network against suspicious network traffic and attempts to access database files. These systems are equipped with monitoring tools that are placed in the most vulnerable points of the company's network. The system is equipped with scanning software that knows the most common methods of cyber-attack and monitoring software that examines events as they occur for possible ongoing threats.

10. How often is a full backup performed?

- Every day [0]
- Every week [2]
- Every month [5]
- Every year [10]

[200] In case of intermediate frequencies choose the closest response (e.g. if it is performed every 5 months then choose a six-monthly frequency). If it is done bimonthly, then choose quarterly.

- » A full backup is never made [15]

10.1. What type of backup is performed for files that have been modified between full backups?

- » Backup differential [0]
- » Backup incremental [0]
- » Only full backup is performed [double the score of question “11”]

In case the answer to the question “10.1” was “Backup differential” or “Backup incremental”

10.1.1 How often is an incremental or differential backup performed?

- » Several times every day [0]
- » Every day [1]
- » Every week [2]
- » Every month [3]

Backup is an activity of prevention and protection of your data. Having a backup means having a copy of your data and therefore being able to recover it in case of problems in the computer system.
Making intermediate backups (incremental or differential) between full backups allows you to keep your backups up to date at all times.

11. Are there firewalls to protect the devices?

- » YES [0]
- » NO [10]

A firewall is a combination of hardware and software that controls incoming and outgoing network traffic. Usually it stands between the internal private network and unreliable external networks. It can also be used to protect part of a company's internal network from the rest of the infrastructure.
It acts by examining each user's credentials before allowing them access to the network, thus preventing any unauthorised communication entering and leaving the network.