D3.4 EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead

Author(s)	ICT Legal Consulting
Status	Final
Version	Final
Date	31/07/2019

Dissemination Level

X	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)

Abstract:

This deliverable ("Deliverable") offers recommendations to policy-makers with regards to the interaction between the General Data Protection Regulation and the Directive on security of network and information systems and the challenges brought about by the deployment of new technologies like Artificial Intelligence, Internet of Things and Blockchain. Moreover, it collects proposals from EU projects on areas of research and policy solutions within the scope the two main strategic elements which will shape the EU landscape in cybersecurity and privacy: Horizon Europe and Digital Europe Programme. Finally, the Deliverable provides also, legal recommendations on privacy and cybersecurity to the two stakeholders of cyberwatching.eu.

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 – D3.4	
Deliverable lead	ICT Legal Consulting
Related work package	WP3
Author(s)	Paolo Balboni, Anastasia Botsi, Laura Senatore, ICT Legal Consulting
Contributor(s)	Nicholas Ferguson, Trust-IT; Mark Miller and Victoria Menezes Miller CPT, Silvia Garbin, AON; Justina Bieliauskaite, DSME. Gabrijela Dreo, Ivana Bunti-Ogor, Volker Eiseler, CONCORDIA project
Due date	30/06/2019
Actual submission date	31/07/2019
Reviewed by	Nicholas Ferguson, Trust-IT Services & Mark Miller and Victoria Menezes Miller, Conceptivity
Start date of Project	01/05/2017
Duration	48 months

Revision history

Version	Date	Authors	Notes
v0.1	07.07.2019	Paolo Balboni, Laura Senatore, and Anastasia Botsi (ICTLC)	Drafting of Deliverable
v0.2	16.07.2019	Silvia Garbin (AON)	Contribution of insurability of the GDPR
v0.3	16.07.2019	Mark R. Miller and Victoria Menezes Miller (Conceptivity)	Revision of Deliverable and addition of relevant sections from Concertation Meeting
v0.4	16.07.2019	Nicholas Ferguson (Trust-IT)	Revision of Deliverable and addition of relevant sections from Concertation Meeting
v0.5	18.07.2019	Silvia Garbin (AON)	Contribution in the introduction and conclusions
v0.6	26.07.2019	Paolo Balboni, Laura Senatore, and Anastasia Botsi (ICTLC)	Consolidation of all partners' feedback and adjustments of Annexes
v0.7	29.07.2019	Gabrijela Dreo, Ivana Bunti-Ogor, Volker Eiseler, CONCORDIA project	Edits to Concordia-related content
v0.8	30.07.2019	Nicholas Ferguson (Trust-IT)	Final version and PMB approval

Executive Summary

The work in this deliverable is related to Objective 3 of cyberwatching.eu, which is to "play a supporting role in the policy, regulatory standards & legal discussions that contribute to shaping up the global cybersecurity & privacy landscape."

This document is the first, and preliminary version (M26) of the subsequent final version of the White paper around legal compliance & policy statements including recommendations (M48). It combines the legislation, the best practices available, the guidelines or opinions of the European Data Protection Supervisor, the European Data Protection Board (former Article 29 Working Party) as well as of competent Supervisory Authorities of EU Member States, and the practical considerations of European Projects ("EU Projects") participating to the second Concertation meeting organised by cyberwatching.eu– all for the purpose of offering a robust package of recommendations that fit stakeholders' needs. Clear explanations of the fundamental obligations included in the EU Regulation 2016/679, known as "General Data Protection Regulation" or "GDPR", can best be provided by the experts that practice and apply the GDPR on a day to day basis, making the cyberwatching.eu partners the most appropriate means of creating this impact. The ultimate aim of this merging of legal knowledge and practical observation of reality was to develop tools that are meant to complement one another, with the final goal resulting in self-assessment tools with handy self-explanatory legal practical recommendations for all stakeholders, including SMEs.

At the same time, cyberwatching.eu offers a platform where the extensive community can be engaged, for example through the yearly Concertation meetings that are organised for R&Is, or via the SMEs joining policy discussions. Cyberwatching.eu also helps the dissemination of other EU Projects and R&Is in general, by means of promoting among the cyberwatching.eu stakeholders (i.e., the SMEs) the solutions of R&Is.

Even though the main focus is the legal recommendations that stem from the interplay of the GDPR and the NIS Directive, as a result of the Concertation Meeting, other issues are touched upon as well. The interactions occurring during the Concertation Meeting allowed to consortium to propose many recommendations for future European initiatives: the Digital Europe Programme and Horizon Europe.

The main recommendations from the report refer to actions in particular for the European Commission to include in future. Horizon Europe and Digital Europe Programmes. They are listed below and are discussed throughout the document and summarised fully in section six.

Recommendations on GDPR & NIS compliance:

a) Publication of a systematic Methodology for GDPR risk assessments
b) Creation of one or many European self-assessment tools as practical instruments to increase compliance to GDPR
c) Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches by updating of the existing methodology from ENISA.
d) European tool for Data Protection Impact Assessment which could compile the several applicable national black lists.
e) Encouraging the creation of codes of conduct to demonstrate compliance through the DEP
f) Research initiative on European certifications, seals and marks on data protection.
g) Education and training to raise industry awareness in the field of emerging technologies.
h) Guidance on implementation of data protection by design and by default in emerging technologies.
i) Practical guidelines on compliance of automated processing in the context of emerging technologies
j) Structured cooperation between policy makers, the research and the market/industry
k) Guidelines on anonymisation tools and pseudonymisation mechanisms to address the challenges of emerging technologies.
l) Guidelines on methodology for risk assessment especially focused on each sector of the OES (NIS Directive) – which are essentially the critical infrastructure of countries.

m) Clarifications on the intricacies between GDPR and NIS including guidance on sanctions for violations and time efficient compliant procedures in industry.
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*.
Recommendation on Blockchain:
a) Practical clarifications on the application of the GDPR to blockchain are very much needed for this technology and the law to coexist, specifically, of fairness by design, to ensure that individuals' privacy and real control over their data is afforded to them

Table 1 Main recommendations listed

Table of Contents

TABLE OF TABLES

TABLE OF FIGURES

1 Introduction

This document demonstrates the specific activities that have been conducted throughout the past months and delivers practical insights from the cluster effort around EU R&I teams, particularly by going over the policy and the efforts of implementing cybersecurity and privacy into the society.

The goal is to offer a supporting role between the regulatory framework that has been implemented within the EU and the market that needs to apply it to the activities it carries out. Additionally, through the analysis, clarifications and recommendations that this Deliverable (and also the final version D3.7 that will consist of a White Paper) will bring forward, the Consortium aims to help save costs and encourage innovative organisations to transform privacy and cybersecurity challenges in opportunities to increase their competitiveness.

Furthermore, two major legislative tools have been implemented by the EU in the past year, both of which have a high impact on the EU privacy and cybersecurity landscape: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR") and Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter "NIS Directive"). The former became effective on 28 May 2018, whereas the latter is expected to be transposed by Member States by the 9th of May 2018. The two legislative instruments are strictly intertwined, in that the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU as a necessary complementary set of rules to the GDPR.

In the first chapter, the interplay of the two legal frameworks will be explained, in order to state their requirements, and to help the policy-makers understand their intricacies solve potential conflicts of interpretation and compliance, but also to demonstrate recommendations that can stem from each individual legislation and from their combination. Following the explanation of these GDPR requirements, a brief discussion of the data protection challenges that are posed by the Internet of Things ("IoT") and Artificial Intelligence ("AI") and Blockchain is provided. The aim of this section is to raise the awareness of legislators on the possible issues that may be inherent to the processing of personal data by means of these technologies. This section is in a preliminary stage, and will be used as basis to be expanded with respect to the relevant legal and policy recommendations which will be made in the final White Paper of work package 3. Moreover, an in-depth look into the insurability of GDPR fines across Europe will be covered. We provide an overview of the insurability of GDPR-related risks and resulting costs across Europe (information current at date of publishing) as a resource for all those organisations affected by GDPR.

The third and fourth chapters (section 3 and 4) are created for the stakeholders of cyberwatching.eu. On the one side, the content for the GDPR temperature tool for SMEs which will be published and converted into an online tool on the cyberwatching.eu web platform and promoted to SMEs. This has been generated as a preliminary step for SMEs to facilitate their understanding of where they stand with respect to the GDPR in terms of "risks to sanctions". This is not an attempt nor is it supposed to be replaced by the risk assessment that should be conducted by SMEs (i.e., risks of varying likelihood and severity for rights and freedoms of natural persons posed by the relevant processing activities), but merely an indication of their risk to sanctions, according to their responses which provide a basis of their processing activities. Therefore, this tool is to be used as recommendations to SMEs on how to have a more GDPR compliant posture. In addition, an R&I survey has been drafted in order to allow cyberwatching.eu to understand the misunderstandings and misconceptions that exist among

the EU projects. The survey responses have been analysed and presented in a summary form in order for policy-makers to be aware of the needs for improvement and further guidance. In summary, both activities have been carried out so as **to effectively enable all stakeholders focused on privacy and cybersecurity to participate in the policy-making debate, both at national and EU levels, on these matters**.

Chapter 5 of this Deliverable includes outputs from various outreach activities, in particular the second Concertation meeting of cyberwatching.eu, which took place in Brussels on June 4th, 2019. The Consortium considers this event as an exemplar event on the matter of contribution to policy dialogue. The Concertation meeting consisted of several interactive sessions that were focused on discussing and collecting recommendations from EU projects on the two main strategic elements which will shape the EU landscape in cybersecurity and privacy: Horizon Europe[1] and Digital Europe Programme[2] ("DEP").

A summary of the recommendations is offered in chapter 6.

[1] EU Budget for the Future: Horizon Europe; Funding for Research and Innovation 2021-2017. Available at: https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-research-innovation_en.pdf.

[2] EU Budget for the Future; Investing in the Future Digital Transformation 2021-2017. Available at: https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-digital-transformation_en.pdf.

2 Interplay between the GDPR and the NIS Directive

This chapter aims to support cyberwatching.eu end-users in understanding the interplay between the GDPR and NIS Directive, in order to clarify their intricacies, to solve potential conflicts of interpretation and to enable R&I projects focused on privacy and cybersecurity to effectively participate in the policy-making debate of the next years, both at the national and EU level, on these matters. At the end, there will also be some recommendations that will be facing the policy makers – in order to point out matters which are still unclear or can appear problematic in the compliance of stakeholders. This section will be a more critical component in the interplay of the two legislations, that will serve as suggestions or clarifications to policy makers.

Out of the various legislations that are implemented, the focus of this section will be two, relatively, new European legislations, the General Data Protection Regulation (GDPR)[3] and the Directive on the Security of Network and Information Systems (NIS Directive)[4], which have been implemented since May 2018. As a result of these laws, the partners of cyberwatching.eu noticed the emergence of a necessity to clearly understand the expected changes, as well as the available mechanisms or tools that could be used to adapt to the priorities of these new laws.

Seeing as the two legislations have been briefly introduced in previous deliverables (in particular, D3.2 EU cybersecurity and privacy R&I ecosystem and D3.3 White paper on cybersecurity standard gap analysis), we will focus on a quick overview of the rights and obligations that will give rise to the intricacies of the two laws; drafted having also the policy makers in mind to propose areas that require clarification, or possibly further guidance, in order for the laws to be implemented correctly.

As a preliminary remark, the GDPR is analysed more in depth due to its widespread applicability; meanwhile, the NIS Directive will be discussed in a short section, since it is more strictly focused on the essential services of each Member State – therefore its scope is inevitably more limited.

It is worth noting that apart from the two legislations that will be discussed in this deliverable, the European Commission has already proposed a text for a new Regulation on Privacy and Electronic Communications [5] (which will update the previous Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector). This goes to show that the near future will bring further transformations of the legal system to ensure consistency, less legal uncertainty and an evolvement of the law which can regulate the market more comprehensively and effectively. These developments will make the current and future work of cyberwatching.eu very important, as it can both take the role in helping the legislation be communicated in a straightforward manner throughout the different fields that it applies to, and as a result point to policy-makers areas that may need further clarification and/or guidance from the EU level.

2.1 The General Data Protection Regulation ("GDPR") requirements

On the one side, the GDPR's obligations are represented by the overarching principle of accountability, which is established in Art. 5(2) GDPR. The principle of **accountability** states

[3] ≈, OJ L 119, 4.5.2016, pp. 1-88.

[4] The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016, p. 1–30.*

[5] You can find the proposal of the new Regulation on Privacy and Electronic Communications here: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

that controllers are responsible for complying with the GDPR requirements (mainly spelled out in terms of principles in Art. 5(1)):

- **lawfulness, fairness and transparency**;
- **purpose limitation**;
- **data minimisation**;
- **accuracy**;
- **storage limitation**; and
- **integrity and confidentiality**,

as well as for being able to demonstrate their compliance, in a manner which can be understood.

An integral part of the principle of accountability is the, so-called "**risk-based approach**", which is reflected in many Articles of the GDPR, e.g., Art. 24 "[t]aking into account the nature, scope, context and purposes of processing as well as **the risks of varying likelihood and severity for the rights and freedoms of natural persons**, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation".

Furthermore, the GDPR indicates that in order to adhere to the principle of accountability, the controller must consider the combination of data protection by design and data protection by default.[6] The first component is that the controller considers data protection issues at the design phase of all services or products, as well as through their entire lifecycle. Meanwhile, the second component reflects that the controller must ensure that, by default, it only processes personal data which is strictly necessary for the purpose of that processing. This means that privacy must be considered in all subsequent 'default' settings of services and products. This could be achieved by ensuring that the minimum amount of that data is collected and stored, by allowing the data subject to control the extent of the processing of their personal data, and by automatically choosing the least intrusive means of processing. The GDPR requires controllers to consider the combination of data protection by design and data protection by default.

However, it is important to mention that in order for data protection by design and by default to be achieved, the performance of assessments of the risks to the rights and freedom of data subjects must occur (i.e., the risk-based approach). This is a rather complex assessment to carry out as an SME or as an EU project, therefore it will be further discussed in the second section of this chapter. At any rate, the GDPR is clear on the fact that where the data protection risk is high, then a data protection impact assessment ("DPIA")[7] must be carried out. In addition to this, controllers and processors must define and implement the appropriate technical and organisational security measures, in order to ensure that the level of security is appropriate to those risks – as stipulated under Article 32 GDPR. The GDPR only lists some examples which can be considered, if they are evaluated to be the appropriate measures by the controller or processor; such as:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner, in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The risk-based approach also creates uncertainty for controllers on whether the implementation of particular measures can lead to a level of security which is appropriate to the risk. Therefore, it goes hand in hand with the challenge of carrying out a proper risk assessment – **controllers and processors that do not have the necessary financial means and expertise (e.g., SMEs) may find it extremely difficult to determine the necessary security measures, both organisational and technical, in order to minimise the risks on individuals of their processing activities. This assumption is confirmed through the**

[6] Article 25 General Data Protection Regulation.
[7] Article 35 General Data Protection Regulation.

multiple interactions that cyberwatching.eu had with its stakeholders, such as events, webinars and Concertation meetings.

Moreover, controllers and processors, therefore, need to implement internal policies or procedures to ensure that the correct security measures are defined to prevent **data breaches** and that, in case the data breaches occur, that they are appropriately managed this in a timely manner. In short, the controllers must be able to detect, identify, assess, and then notify the relevant Supervisory Authority, or even communicate to the data subjects, that the data breach has occurred. These requirements get even more intensified by the fact that unless the assessment of the severity of a personal data breach indicates that it is unlikely to result in a risk to the rights and freedom of the data subjects, then the controller must notify to the competent Supervisory Authority the personal data breach – within 72 hours of becoming aware of the breach.[8] However, the obligation to identify and notify a breach in such a short time is a requirement that may not be realistic, especially for organisation with limited resources – both in terms of technical tools and expertise deployed If the controller's assessment reflects a high risk to the data subjects, then a communication must further be sent to the data subjects who were affected by the personal data breach – in accordance with the principle of transparency.[9]

Controllers also have to provide concrete and comprehensive **information** to data subjects regarding processing operations taking place. The principle of transparency is another way for the controllers to show accountability. In this case, the GDPR enlists the specific information requirements that should be included in these privacy policies, which slightly change depending on whether the personal data is collected directly from data subjects or not. [10] However, apart from the specific information which must be provided – the GDPR also raises the bar in terms of the methods and language that the communication itself must adhere to. For example, the data protection matters must be clearly explained so as to be understood by the intended audience, avoiding unnecessary ambiguities and describing the information in a simple manner. [11] In short, controllers must ensure that the information provided is concise, transparent, intelligible and easily accessible, meaning that a short evaluation must also be conducted so as to decide which information should be included, to what extent of detail and which are the best ways to deliver this information to data subjects.[12]

An integral part of compliance is then the correct choice of a **legal bases** for the purposes of the personal data processing activities involved, as established in Art. 6 GDPR. In order for a controller to determine the legal basis of a processing, there must be a clear understanding of the scope and additional requirements that need to be met in order for them to rely on a specific legal basis under the GDPR. The controller may choose one of the six different legal bases, namely:

- consent,
- the necessity to perform a contract with the data subject or take steps prior to entering into a contract at the request of the data subject,
- the necessity to comply with a legal obligation,
- the necessity to protect the vital interests of the data subject or another individual,
- the necessity to perform a task in the public interest,
- the necessity for the purposes of a legitimate interest pursued by the controller.

The core of this obligation is that the controller must carefully choose a legal basis that is most appropriate for the processing activity carried out and justify this choice in the information

[8] Article 33 (1) General Data Protection Regulation.
[9] Article 34 General Data Protection Regulation.
[10] Article 13 of General Data Protection Regulation enlists the information to give in case the personal data are collected from the data subject, while Article 14 General Data Protection Regulation describes the information to give in case the personal data were not obtained from the data subject.
[11] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (11 April 2018), pp. 6-13. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[12] Article 29 Working Party, *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01 (11 April 2018), p. 18. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

notices and the records of processing activities created. **Even though this may be a straight forward requirement, it is also a heavy burden for stakeholders that may not have the legal expertise, or reasoning, to accurately choose**.

Last but not least, the GDPR offers data subjects a wide variety of rights which they can exercise towards controllers. Controllers are required to not only provide data subjects with relevant information as to the existence of those rights, and how they can be exercised, (Arts. 13(2)(b) and 14(2)(c) GDPR, tied in to the principle of transparency), but also to develop a consistent and effective approach to receiving, tracking and addressing in full any requests received from data subjects to exercise any of the rights granted by the GDPR:

- right of access
- right to rectification
- right to erasure
- right to restriction of processing
- right to data portability
- right to object to processing
- rights concerning automated individual decision-making

Addressing data subjects' rights under the GDPR present significant challenges for controllers in terms of data mapping (especially relevant, e.g., for access, erasure, portability), data management (especially relevant, e.g., for rectification, erasure, portability, restriction of processing, object to processing, rights concerning automated individual decision making), and communications with data subjects (especially relevant, e.g., for access, portability, rights concerning automated individual decision making). Again, **stakeholders do not really have enough expertise, budget and tools to fully comply with one of the core obligations under privacy law: grant data subjects the effective exercise of their rights**.

All of the above requirements that were discussed is an overview and not conclusive. However, a clear understanding of these requirements will help identify the challenges of achieving compliance and shall serve as a basis for the proposal of the legal recommendations to policy-makers.

2.2 Challenges of AI, IoT and Blockchain

In the events organised, in whole or in part, by the Consortium, in relevant events which we joined, and based on the practical Consortium experience we had the opportunity to identify challenges when it comes to emerging technologies. Three of the most recurring topics that came up are AI, IoT and Blockchain. Therefore, in the sections below an overview is given of the most significant barriers to having GDPR compliant solutions and services with respect to these three technology/technological applications. This Deliverable is utilised to lay down the main challenges that are posed by these technologies, and in the final White Paper concrete recommendations on these matters will be proposed.

2.2.1 Artificial Intelligence Challenges

Artificial intelligence ("AI") is an undeniable component of the future of technology and cyberspace, which can be implemented in the systems, software and devices of different sectors.[13] From a data protection perspective, AI is typically utilized as a tool for automated

[13] Guidelines on Artificial Intelligence and Data Protection, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 25 January 2019.

decision-making and profiling, by leveraging algorithms to process a large volume of data.[14] The challenges arise where the processing done by the AI is of such nature that it creates significant effects for the data subjects.

Firstly, the principle of transparency is at stake. When controllers use AI as a tool to process personal data because the data subjects may not be sufficiently informed about the way in which their personal data is being collected and processed. The reason for this is that, when it comes to AI, effectively proper/full information about processing data cannot always be given. As a matter of fact, if a controller uses AI it may be quite challenging to strictly define how the personal data will be processed and for which purposes exactly, given that a machine learning algorithm has, per definition, a behaviour that changes (learn) over time in terms of actions on the data, correlations drawn, and outputs (that can effect an individual). Therefore, it becomes hard to give prior information notice to data subjects when the content of that notice may be dependent on the result of the AI decision making. As can be seen, **there is a circular process that would allow for those utilizing AI an additional requirement – in which the data subjects whose personal data is being processed must receive additional information as the AI comes to conclusions. However, as per the current legislative framework of the GDPR – this has not been envisaged**. The information notice, as per Article 13 and 14 GDPR, must include all information regarding the processing, and where the processing includes automated decision making, it must also include the logic of the algorithm and the impact that it may have on the data subject. Therefore, **a solution must be given for the AI models that process personal data by means of machine learning algorithms that may change the logic and the impact on individuals over time**.

Related to the previous challenge is the fact that **the machine learning algorithm may in fact autonomously (and in an unexpected/unpredictable way) process personal data of individuals for purposes different or incompatible with the ones for which the data were collected**. Essentially, this would mean that the AI has already processed personal data of that person, for a purpose which was not originally disclosed or that it is incompatible (see Art. 6(4) GDPR). Therefore, the controller and, therefore, the data subject are not in control anymore of how the data are processed. This is a challenge that seriously undermines the entire rationale behind the protection of personal data.

Furthermore, **the risk assessment of the automated processing conducted through AI may be in several cases unrealistic**. For the reasons outlined above, the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller (in contrast with what required by Art.s 24 and 24 GDPR). Therefore, the risk-based approach would be severely undermined in processing activities relating to AI. This may also lead to a case where the security measures that may have been implemented originally, are no longer adequate (see Art. 32 GDPR), considering the evolving circumstances of the processing activities.

2.2.2 IoT Challenges

The Internet of Things (“IoT”) is another emerging technology that poses challenges to the European framework for data protection. The opportunity for the economy and society to have an ecosystem of interconnected services and devices is undoubted. However, the amount of personal data that is collected through the sensors of these IoT devices or services is both large and inherently intrusive.

The first concern in the realm of IoT devices and services is the principles of data protection by design and by default and data minimisation. In complex IoT environments,

[14] Big Data, Artificial Intelligence, Machine Learning, and Data Protection https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

designing data flows aimed at minimising the use of data and preserving individual privacy to the maximum extent without diminishing the functionalities of the systems is a great challenge. Moreover, assuring end-to-end security during the entire data-lifecycle is a clear issue given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data. **There is a need for further guidelines on the application of the principles of data protection by design/default and data minimisation for IoT deployments**.

Additionally, **in IoT environment users may struggle to receive meaningful and complete information regarding the relevant data processing activities (see Art.s 12-13-14 GDPR)**. Usually, IoT-related data processing happens without an effective user knowledge and/or understanding of it. There is no clear and comprehensive information point where users can understand how data are processed in the IoT environment and by whom. In such a situation, furthermore, the IoT devices may inadvertently collect personal data of data subjects who may not have consented to that processing of their data; such as visitors of smart homes/offices. **In this case, the principle of transparency becomes significantly challenged and the solution does not seem to have been taken into account within the GDPR.**

This last point also brings up the **issue of lawfulness** of the processing of personal data of visitors or data subjects that may not be the primary IoT user. A detrimental component of processing personal data is that it may give rise to the risks of sanctions for IoT services that do not have a legitimate legal basis to process personal data of third parties, or other persons that may neither be informed of the processing nor be given the change to consent or object to it. **This challenge is closely related to the data subject's rights**, which it can hardly be argued, are able to be exercised. In fact, if a data subject is not adequately informed of the IoT processing their personal data, then it follows that they will also not be offered an appropriate method to exercise their rights as data subjects.

Lastly, **IoT poses strong challenges to the allocation of privacy roles**. For example, IoT data processing is often carried out by machines managed by different organisations, each of them using computational capacity provided by cloud service providers and that can also involve analytic software programmes supplied by the related vendors. This exponentially increases the number of parties involved in the data processing activities and to clearly allocate the privacy roles in terms of controller, processor or joint- controller. Failing to correctly identify the roles will result in a possible misallocation of respective duties and obligations towards the data subjects and towards the competent Supervisory Authorities. Additionally, when the parties to a processing activity of IoT deployments are so numerous, it is not realistic to expect that all controllers will legally bind their processors. However, the GDPR clearly requires, through Article 28(3), that a contract or other instrument must be signed between the controller and the processor. **Practical guidelines should be given in the allocation of privacy roles in IoT environments in the light of the GDPR**.

2.2.3 Blockchain Challenges

It is also very important to address the matters raised by the GDPR when considering the use of blockchain-based systems, as not only do they offer the possibility for personal data to be directly recorded 'on-chain', but also require the use of personal data (in the form of public keys/identifiers) for their very functioning. Given the high standard for anonymisation set by the Article 29 Working Party, even encryption or irreversible hashing of personal data stored on blockchain will not suffice to circumvent the discussion (at least, for now).

The interaction between blockchain and internationally recognised data processing principles is not always smooth. **While some principles remain largely unaffected by the technology, such as the principle of lawfulness and purpose limitation, and others may even find themselves enhanced by the additional functionalities brought about by blockchain, such as the principle of fairness, others still appear to frontally collide with**

its 'set-in-stone' nature, namely the principles of data minimisation and storage limitation which, in turn, may affect the ability to effectively exercise some data subject rights regarding personal data stored 'on-chain' (such as the right to rectification or erasure). It is also not a simple matter to identify and agree on the **data processing roles** played by the participants in a blockchain-based system. **An even more complicated matter is to ensure that the formal requirements tied into these roles are met, such as the need for a contract or other legal act containing a set of minimum obligations to be entered into with each processor engaged by a controller, in light of Art. 28 GDPR – this problem currently appears not to have a practically viable solution when considering public blockchains**. The matter of **international transfers** and the implementation of the requirements for their lawfulness raises similar difficulties in light of the decentralised nature of blockchain-based systems.

In general, many of these issues can be solved by storing personal data in an 'off-chain' solution, and merely referencing those data (e.g., via a commitment or hash pointer) within the blockchain-based system itself. However, in any case, it must be understood that, while blockchain has the potential to allow individuals to retain control of their data and even to understand, in a transparent manner, who has access to their information and to what extent, this by no means results automatically from the use of blockchain-based systems to process personal data. Rather, those systems must be specifically crafted, in careful consideration of the rules set by the principles of data protection by design and, specifically, of fairness by design, to ensure that individuals' privacy and real control over their data is afforded to them.

The use of blockchain technology as a means to process personal data has been called into question ever since the GDPR was first announced, with doubts solidified by the European Parliament's stance on the matter. For now, it seems that there are manners in which to handle the potential objections raised, at least where private or permissioned blockchains are concerned.

Practical clarifications on the application of the GDPR to blockchain are very much needed for this technology and the law to coexist.

2.3 Insurability of GDPR-related risks

It is worth mentioning and going over an additional challenge for stakeholders, which is the practical component of how insurance matters work with the costs or infractions that may arise from the GDPR. Even though it is common in administrative law that insurance does not cover imposed fines, there are instances where other GDPR costs may be covered by insurances. Below is an outline of these cases and subsequent recommendations for the policy-makers to understand and managing the impact of GDPR on European organisations[15].

The GDPR has brought new legal rights for data subjects, while extending the scope of the responsibilities of controllers and processors. It also enhanced enforcement rights for regulators, to include fines of up to €20 million or, if higher, 4% of an organisation's annual global turnover.

Two recent examples are: the UK Information Commissioner's Office (ICO) issued a notice of intent to impose a fine of €204 million on an airline company, representing about 1.5% of the company's global turnover. The ICO issued another notice of intent to impose a fine of €110 million on an international hotel chain, representing about 3% of the company's global turnover. The scale of these fines has understandably generated concern in boardrooms. GDPR has replaced a regime under which fines for a data breach were limited and enforcement

[15] This section strongly builds on a previous research on the subject matter that Aon has carried out with DLA Piper, as outlined in the following document: Aon Risk Solution. The price of data security – A guide to the insurability of GDPR fines across Europe 2nd Edition, July 2019.

actions infrequent. The regulatory environment across European Member States is undoubtedly shifting and regulators now have greater powers of enforcement, and significant GDPR fines are expected to be imposed where organisations are subject to investigations. Moreover, the consequences of GDPR non- compliance are not limited to monetary fines. There are also the costs associated with non-compliance. These costs, potentially resulting from a data breach, could include, for example, legal fees and litigation, regulatory investigation, remediation, public relations, and other costs associated with compensation and notification to impacted data subjects. Furthermore, the potential damage to an organisation's reputation and market position can be significant. **The magnitude of GDPR fines means organisations are keen to know whether these fines can be insured. Typical cyber insurance policies only insure fines when "insurable by law", and stipulate that the insurability of fines or penalties shall be determined by the "laws of any applicable jurisdiction that most favours coverage for such monetary fines or penalties." Organisations also need to consider other costs and liabilities that could result from GDPR non-compliance**.

Given the size of the potential financial impact of GDPR non-compliance, it is important for organisations to understand how the insurability of fines, legal and other costs and liabilities following a data breach is approached in different jurisdictions. There are only a few jurisdictions where it is clear that civil fines can be covered by insurance - even then there must be no deliberate wrongdoing or gross negligence on the part of the insured. Criminal penalties are almost never insurable. GDPR administrative fines are civil in nature, but the GDPR also permits European Member States to impose their own penalties for personal data violations. If those penalties are criminal, they almost certainly would not be covered by insurance.

While the insurability of fines may be limited, insurance forms a key component of an organisation's GDPR risk management strategy to manage costs associated with GDPR noncompliance and resulting business disruption losses. In addition to insurance, there is significant business advantage to taking privacy and data protection seriously. Properly securing the data you hold is critical, but a robust data retention strategy is essential. Organisations frequently retain too much data for too long, without discernible commercial benefit; thereby increasing their risk exposure. High profile breaches and revelations regarding the misuse of data shared via social media have made consumers more aware of how their data might be collected, stored, analysed and used.

Figure 1 - Biggest cases per country in Europe (as of July 2019). Source: DLA Piper.

GDPR not only applies to organisations located within the European Union, but also to organisations that offer goods or services to, or monitor the behaviour of, European data subjects, even where those organisations are located outside of the EU.

GDPR applies to the processing of "personal data", meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier. This can include any information that can be used to identify an individual; a name, an email address or a phone number, but it could also include IP addresses, job roles, employee IDs or depersonalised claims data, survey information or pension details. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about individuals.

Some of the GDPR requirements for organisations are:

- Governance and accountability - GDPR is concerned with the principle of accountability, which requires organisations to be able to demonstrate compliance with GDPR. The effect of this is that all organisations need to implement a formal data protection programme to demonstrate that data protection is seriously taken and their processing activities are performed in accordance with GDPR.
- More rights for data subjects - Data subjects (identified or identifiable natural person) are entitled to a range of rights, including a right to erasure, a right to data portability, a right to challenge certain forms of non-essential processing, and a right not to be subject to an automated decision in certain circumstances. Data subjects have more control over the processing of their personal data.

- Privacy by design and by default - Organisations must take privacy risks into account throughout the process of designing a new product or service, and adopt mechanisms to ensure that, by default, minimal personal data is collected, used and retained.
- Privacy risk impact assessment - Privacy risk impact assessments are required before processing personal data for operations which are likely to present higher privacy risks to data subjects due to the nature or scope of the processing operation.
- Appointment of a data protection officer - Appointment of a data protection officer with expert knowledge is mandatory for public authorities and for organisations whose core activities involve the regular and systematic monitoring of data subjects on a large scale (for example, data-driven marketing activities or location tracking), or which process large amounts of special categories of personal data, such as insurers, banks and healthcare companies.
- Personal data breach - Requirement to notify personal data breaches causing risk to individuals to the supervisory authorities within 72 hours. In the event the incident is likely to pose a high risk to the affected individuals' rights and freedom, there is also a duty to notify those individuals of the breach.
- Processors - The processing of personal data by a processor (the entity which processes personal data on behalf of the controller) must be governed by a contract between the processor and the controller (the entity which determines the purposes and means of processing of personal data). Furthermore, unlike its predecessor, GDPR imposes direct statutory obligations on processors, which means they are subject to direct enforcement by supervisory authorities, fines, and compensation claims by data subjects. In practice processors may, therefore, strongly resist the imposition of any contractual indemnity on the basis that they are subject to their own direct liability under GDPR, and argue that a more balanced apportionment of risk is appropriate (for example, a cross-indemnity), or else the replacement of an indemnity with capped liability. Alternatively, the parties may agree to allocate liability in such a way as to completely exclude GDPR indemnities and accept sole responsibility, with respect to GDPR fines, penalties and assessments, while allocating responsibility for all other non-GDPR fines related liability.

The scope of GDPR is broader than most insurance policies which are often triggered by privacy or security incidents, whereas GDPR violations can also be triggered by non-compliance separate and apart from a privacy or security incident. A policy which was entered into before the GDPR came into force may have been intended to cover fines imposed for wrongful collection and use of personal data and / or regulatory fines for cyber-related incidents. That policy would treat GDPR fines in the same way. Similarly, a policy which excludes fines imposed for wrongful collection and use of personal data and / or regulatory fines for cyber-related incidents would also exclude such fines imposed under GDPR. Where a policy is intended to cover such fines, a key issue is the extent to which those fines are insurable.

DLA Piper has carried out a review of whether regulatory fines, GDPR fines in particular, and legal and other costs and liabilities following a data breach, are insurable in each EU country, Norway and Switzerland. The findings assume that in each country local law is applied. Often it will be possible for the parties to agree that another system of law applies to an insurance contract. However, legal rules governing insurability are often derived from public policy principles which can override the parties' choice of law, meaning it cannot be assumed that such choice will prevail. The findings also set out whether fines and other costs and liabilities are insurable "in principle" - DLA Piper has not considered whether insurance cover is available for particular risks. **The issue of insurability is dynamic and fluid. Where GDPR fines are "not insurable" in a particular jurisdiction, this position may be a matter of debate in the local insurance sector, and some market participants may nevertheless provide cover for GDPR fines.**

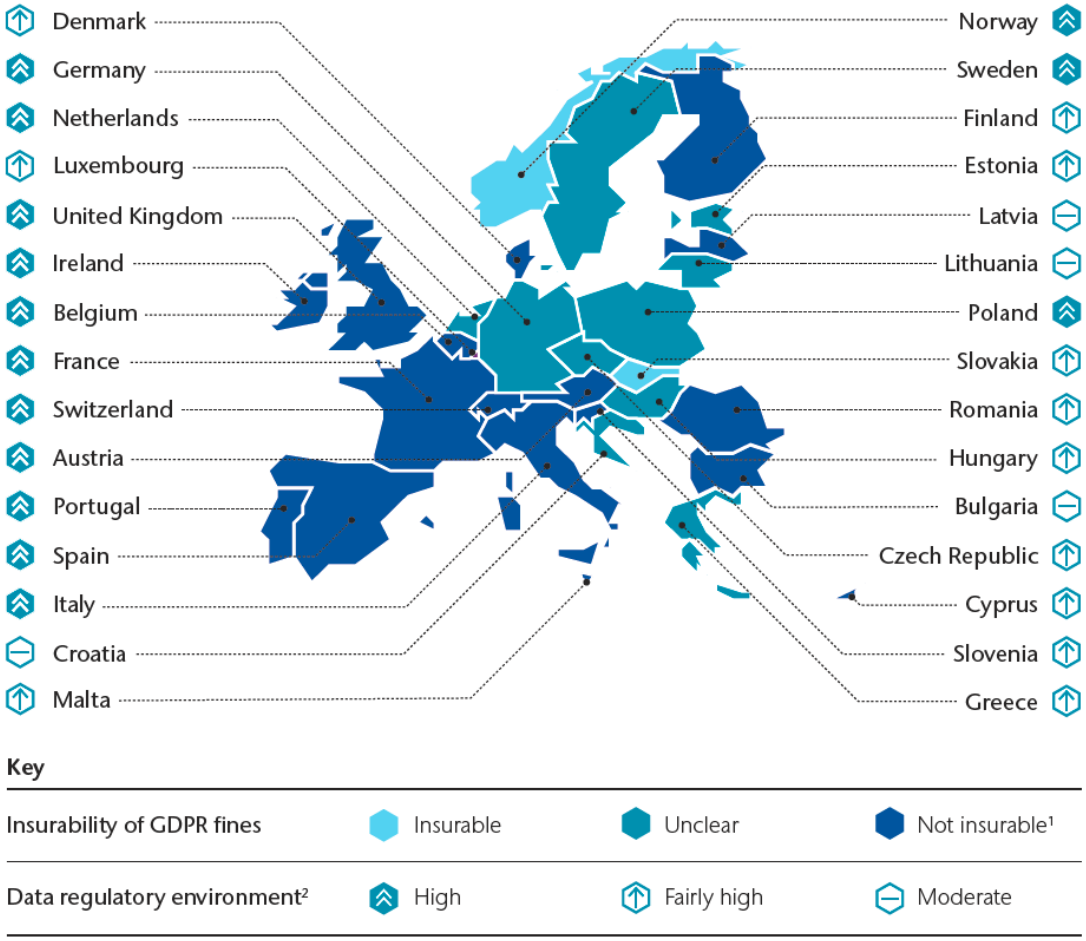


Figure 2 - GDPR heat map. Source: DLA Piper [16,17]

However, **in most of European countries it is possible to insure against:**

I. **costs of investigating an incident;**
II. **defence costs;**
III. **claims by third parties (customers/suppliers/data subjects) for consequences of breach;**
IV. **costs of mitigating a breach including public relations expenses.**

Unless it is otherwise clearly stated, a policy will not cover costs that are due to a willful act or gross negligence.

[16] DLA Piper has included as "not insurable" countries where in certain limited circumstances a fine might possibly be indemnifiable, but under local laws or public policy fines would generally not be regarded as insurable

[17] Data regulatory environment: Presented as a metric to o-er a high-level guide to the approximate likelihood of exposure to regulatory action from data protection authorities, and the possible strength of that action. It is assessed through a variety of factors, including (i) availability of criminal sanctions under local law; (ii) size and historic activity level of the regulator; and (iii) presence (and complexity) of supplementary privacy and information security laws. The heat rating assigned to a jurisdiction should not be interpreted as an indication of the likelihood of that country's data protection authority commencing enforcement action in respect of any specific scenario.

There is no doubt that GDPR is a continuous challenge for organisations, but there are steps that can be taken to help manage the potential impact through risk governance, insurance review and incident response:

- Carry out a security audit to check personal data is secure against unauthorized access or processing
- Put in place a plan for ensuring continuous monitoring and follow up of data compliance efforts
- Ensure contracts with all third-party processors contain at least the minimum terms stipulated by GDPR
- Adopt a privacy-by-design methodology when initiating new projects or developing new tools
- Ensure adequate cyber insurance coverage is in place
- Review your existing cyber insurance policy with assistance from qualified coverage counsel and your broker regarding coverage for GDPR non-compliance, especially fines, penalties and lawsuits
- Ensure you have an incident response plan in place, including data security breach notification procedures
- Review your existing enterprise-wide incident response plan to ensure that it incorporates escalation plans and nominated advisors covering all required stakeholders. This includes business operations, legal, PR, and key third parties such as IT service providers.

Whilst GDPR has a positive impact on the privacy of EU citizens, there are still concerns about the financial impact to organisations. Ongoing effort will be required to manage the implications of GDPR.

2.4 The Directive on the Security of Network and Information Systems ("NIS Directive")

The NIS Directive is a legislation with a different scope compared to the GDPR which covers all matters that concern processing activities of all– controllers, processors – insofar as they may affect data subjects' rights and freedom, regardless of their field or scope of operations. On the other hand, the NIS Directive is focused on cybersecurity. More precisely, the aim of the NIS Directive is to establish a common level of security for network and information systems, since these systems are a vital component to address the risks that may be posed in important sectors of a society. The NIS Directive focuses on two types of service providers, the operators of essential services ("OES") and the relevant digital service providers ("DSPs"). At this point it is important to note that there is an exemption for DSPs who are micro or small enterprises, to whom the requirements that will be mentioned below do not apply.[18] This was done in order to ensure that the European micro and small enterprises will not suffer a disproportionate financial and administrative burden. This means that this Directive applies strictly to the larger organisations or companies of larger groups. For the purpose of this deliverable, the **NIS will be discussed according to the scope of the stakeholder community of cyberwatching.eu – meaning that it will mostly include recommendations towards OESs and DSPs that must comply with the legislation.**

Keeping the above scope in mind, we can dive into the requirements that arise from the NIS Directive for the identified operators of essential services, and the digital service providers. Firstly, the operators of essential services are different in every Member State, since each Member State has the obligation to specifically identify their OES for each sector, energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure. The

[18] Recital 53 of the Directive concerning measures for a high common level of security of network and information systems across the Union.

OES can therefore be both public and private entities, as long as they are enlisted by the Member States. As for DSPs, they can be any legal person(s) that provide(s) a digital service in the online marketplace, online search engines, or cloud computing services.

The NIS Directive establishes several requirements for OES, which focus around risk management and incident reporting – topics which at first glance seem also closely related to those covered by the GDPR. Firstly, OES must take appropriate and proportionate technical and organisational measures to manage risks posed to the security of network and information systems which they use in their operations, pursuant to Article 14 NIS Directive. In the same article, it is emphasized, that the level of security must be appropriate to the risk posed. The European Union Agency for Cybersecurity has produced **Guidelines on assessing the compliance of OES with the NIS Directive, whereby it has enlisted a set of questions which correspond to security measures and appropriate evidence that can be used to support the implementation of such security measures**.[19] Regardless of the Guidelines being mostly drafted in order to support national competent authorities to conduct audits, it remains a useful tool that can be used to implement appropriate security measures. However, **what seems to be missing is a risk assessment approach especially focused on each sector of the OES – which are essentially the critical infrastructure of countries.**

Secondly, Article 14(2) NIS Directive ascertains that OES must take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems, in order to ensure the continuity of those services. Essentially, the OES must also be equipped with the appropriate security measures in order to manage specific incidents that may affects their systems. Hand in hand goes the last component of obligations for OES according to Article 14(3) NIS Directive, which obliges OES to notify incidents that have a significant impact on the continuity of the essential services to either the competent authority or the Computer Security Incident Response Teams ("CSIRTs"). Following these notifications, the CSIRT or the competent authority may then inform the public about the incidents.

Concerning the DSP, in theory Article 16 NIS Directive finds separate security requirements and incident notification obligations. However, in reality, the requirements consist of the same risk-based method, which will aid the DSP to take appropriate measures in order to manage the risks posed to the security of network and information systems. In addition to the abovementioned description of the obligations, **ENISA has focused on the role of the risk assessment, through the description of sophistication levels – basic, industry standard and state of the art - that can be used to select the relevant security measures of objectives.**[20] This is a helpful tool that can be used by DSP to define sophistication levels, based on the specific characteristics of the services it provides, and subsequently choose security measures that are comparative to that sophistication level.

2.5 Recommendations on the GDPR and the NIS Directive: Calls to Action and Next Steps

As can be seen in the above sections, there are many intricacies that arise when organisations need to combine the two relatively recent legislations. While the wide applicability of the GDPR and the focus on critical infrastructures of the NIS Directive may assist most entities in applying the accurate legislation depending on their sectors of operation – there are several unresolved issues that can be noticed when applying both legislations. As a result,

[19] Guidelines on assessing DSP and OES compliance to the NISD security requirements, Information Security Audit and Self-Assessment/Management Frameworks, November 2018. Available at: https://www.enisa.europa.eu/news/enisa-news/information-security-audit-and-self-assessment-frameworks-for-oes-and-dsps.

[20] Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. Available at: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

entities seem to apply the legislations incompletely – for example, failing to implement security measures adequate to the risk, and spend their resources, aiming to increase their compliance efforts, without being able to achieve it in reality. Therefore, cyberwatching.eu has identified several priority areas that both EU Projects and policy-makers can consider in their future activities, also connecting each recommendation with one of the two programs: Horizon Europe and the DEP.

An area that requires further research and practical guidelines– which could be enacted by the Horizon Europe projects - is one which focuses on the GDPR requirement to carry out risk assessments in order to ensure an adequate level of protection and data protection by design and by default. The privacy by design and by default are meant to make data subjects be in control of their personal data, meaning that it should be practically achievable for organisations to adhere to. The Opinion on the privacy by design, which was drafted by the European Data Protection Supervisor (EDPS")[21], does help organisations to understand and implement the complex principle of privacy by design. However, there is a lack of a practical reflections on the actual implementation of the two principles. Data protection by design and by default and the risk-based approach are fundamental pillars of the GDPR and there is a need for practical tools that can provide actionable solutions to comply with them, departing from the theoretical guidelines. The need for practical tools, possibly freely available, which could help with these activities is confirmed if we consider – as already mentioned - that not all controllers and processors – such as the SMEs - may have the expertise and resources to be able to figure out methodologies in order to comply with such obligations.

Taking an in-depth look into the risk assessment process, the GDPR raises the bar for organisations in expecting a risk analysis of all processing activities that are carried out. Needless to say, the advantages of following the risk-based approach in order to protect personal data is that it is a diligent system that serves the greater security of personal data around Europe and more protections for individuals rights. **However, the subjectivity of this approach also opens up grey areas for entities which process personal data (such as SMEs). Therefore, the recommendation of cyberwatching.eu for both research projects and policy makers is to create a "framework", which can be utilised by controllers with the aim of guiding them in assessing the risks of their processing operations in a complete manner**. This "framework" can create several objective factors or indicators that may help and guide, in a non-inclusive way, the determination of the risk results. In order for policy-makers to be able to create such a structure, the realistic outlook of industry must be taken into account, giving rise to an open discussion that can stir a structure for risk assessment not only including the theoretical aspects but also presenting them in a practical and manageable manner. In order to achieve this challenging goal, the Supervisory Authorities have an important role as well. As a matter of fact, while fulfilling their tasks, they contact many entities that process personal data, and this gives them the possibility to also get to know the state of art when it comes to sector-specific activities of processing. Furthermore, as far as recommendations to policy makers are concerned, **the tasks of the Supervisory Authorities provided for by Art. 57 GDPR could be broadened, thereby evaluating the opportunity to find an efficient instrument that allows the entities that process personal data to ask for guidelines on the most challenging obligations they face, especially when it comes to emerging technologies.**

It is important to understand that the European market must both have a reasonable risk assessment method and also be able to constantly adapt it to the rapid advancements of technology. This may create a burdensome atmosphere, which expands from Europe to all companies under the scope of the GDPR, deeming a practical structure to assess risks even more crucial. Apart from the point of view of the controllers' abstract carrying out of risk assessments, having structured indicators to conduct risk assessments can also be leveraged

[21] EDPS Opinion 05/2018 on privacy by design is available here: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

by Data Protection Officers, since it will provide a starting point that cannot be easily avoided or ignored by controllers and this would facilitate their task of monitoring the compliance of processing activities. Having this as a first step will generally assist in the compliance posture of organisations. Therefore, **it is recommended that the DEP be utilized as a platform that can bring the policy-makers and the industry closer together through a systematic methodology of risk assessments**.

Parallel to the above recommendation stands the appropriate identification of security measures; which is another demanding obligation that requires high cybersecurity expertise that some controllers may not be privileged to have. It is one concern to assess the risk of a processing, and another to also allocate the necessary security measures to minimise or eliminate these risks. Therefore, **Horizon Europe may consider focusing research initiatives that will work on the creation of risk assessment structures, which will also be coordinated with the DEP, and further enhance these methodologies by corresponding them with appropriate security measures**. Even though ENISA has provided the Technical Guidelines on the implementation of minimum-security measures[22], it is restricted to digital service providers and may not include SMEs or other entities that may process personal data. In conclusion, **the gap between the legislation and the practical considerations that a company must take can be tackled by creating a systematic methodology to analyse the risks of the entity's processing activities and subsequently select appropriate security measures to mitigate those risks**. This recommendation could concretely consist of the **drafting of a self-assessment questionnaire that will yield an approximate result of the risk, and subsequently promote a specific group of security measures that may be expected according to the level of risk, and circumstances of the company at stake, and whose adequacy should then be evaluated by the data controller.**

In addition to the recommendations given with regards to the GDPR, policy-makers must consider that when it comes to OES assessment or the risks and threats that may be applicable to their sector, there is no methodology on how to tackle the risk-based approach. Having a method of assessing risks is especially fundamental for essential services of Europe. This can be handled by the DEP, seeing that the industry must be involved in the establishing of this methodology. **A recommendation would be that ENISA, as the European Agency for Cybersecurity, works together with the DEP stakeholders, with the aim of producing practical guidelines for assessing the risks in the essential services of member states at a centralised European level**. ENISA has already developed guidelines aimed at DSPs, which identify security objectives and list technical and organisational security measures which can be implemented to achieve each one. The challenge with the OES is that their services may cross borders, and the risks may be of a very different kind (for example, risks in the energy sector is different from the risks in the health sector) therefore there is an even higher necessity to create a pan-Europe method of assessing risks of this kind.

Furthermore, **guidelines to help organisations that must comply with both GDPR and the NIS Directive legislations are important**. Given that the occurrence of a data breach is likely to trigger one of the most serious risks which an organisation may face, it is essential to provide further recommendations on this issue. If it is assumed that a cross-border breach occurs, and the risk towards data subjects is high, then an organisation has an obligation to notify the breach to the competent data protection authority, as well as to the competent authority for the NIS Directive or the CSIRTs. The obligations may seem manageable when considered individually, however, they can quickly become hard to achieve under these circumstances. Since the GDPR gives a time limit with regards to the notification, 72 hours, there is an urgency to have recommendations on how to manage breaches that are under the legislative scope of both the GDPR and the NIS Directive. In short, it could be useful for

[22] ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers are available here: https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

organisations to have further guidance on the methodology of managing the appropriate notifications to all competent authorities in due time. This recommendation could be relevant for the priorities of the DEP, which could use industry to shed light on the procedures that take place in real time of such circumstances, and the research component to find the most time-efficient and compliant method of managing notifications that fulfil the requirements of both the NIS Directive and the GDPR.

Additionally, in order to notify data breaches appropriately and in a timely manner, the organisations must be able to assess the risks to the data subjects (for compliance with the GDPR) or to the services provided (for compliance with the NIS Directive) at the same time. This creates a further point of research – whether the two risk assessments can be combined in one risk assessment process. Therefore, **Horizon Europe should prioritise a research initiative in which cross-border data breaches can be notified in a method that would incorporate both obligations of the GDPR and the NIS Directive**.

This last point brings rise to a more minor issue, which is a question of the sanctions that may be implemented as a result of a lack of compliance with security measures or a fine due to a data breach. It remains to be seen whether the intersected legislations can lead to a double sanction; in which, each one would coincide with the breach of the obligations of the GDPR and of the NIS Directive. **Policy-makers could provide guidance for organisations on the extent to which sanctions will be applied for both legislations and how such violations will be regarded by competent authorities and member states**.

3 Description of SME surveys: the "GDPR temperature" tool and the Survey on Information Notices

The "GDPR temperature tool" is a survey that was created for the purpose of providing recommendations to SMEs, especially focusing on their exposure to risk of sanctions due to GDPR violations. In this deliverable, the recommendations will be included for the purpose of being publicly provided and accessible by SMEs. However, it is important to note that the final aim of this survey is to be distributed in the new website of cyberwatching.eu, in the form of an online interactive tool which will be used to give an insight to SMEs of their risk to being sanctioned for failure to comply with the GDPR. It is important to note that the SME GDPR Temperature tool was preliminarily created in order to yield to a result of low, medium, high in order to help assess the risk to **sanctions** – but not the risk of the processing itself. An analysis of each question and recommendation for the SMEs can be found in **Annex A**.

While creating the tool for SMEs, the consortium came to the conclusion that tools like the GDPR Temperature tool are the kind of deliverables that are useful for all stakeholders of cyberwatching.eu. For this reason, an additional survey was created – a shorter and more practical one than the above; with a strict focus on the provision of information notices and the content of these privacy notices. Essentially, this survey is more or less like a check-list of content of the information and the manners of communicating it to the data subjects; thus, the possible answers to the survey are "Yes", "No", and "Not Applicable". **Annex B** includes the questions and their corresponding answers that will be included in the online tool which will be published in Autumn 2019.

3.1 Remarks

No data from these tools have been collected, due to the fact that they will be included in the new website of cyberwatching.eu as interactive instruments that stakeholders can use based on their needs. Therefore, the plan is to utilise the next deliverable (D3.7) to give

feedback on the results received and how this tool has been improved, or enhanced by month 48.

4 Survey for R&I Projects

The cyberwatching.eu project aims to contribute to a safer and more trusted Digital Single Market, by promoting the understanding of cutting-edge cybersecurity and privacy services, which emerge from R&I initiatives. The role of the R&I projects is very important in this effort. On one hand, by submitting to the Cyberwatching.eu Catalogue of Services (the full list of the Services is available at https://cyberwatching.eu/ services/catalogue-of-services), R&I Projects get to communicate their objectives and disseminate their results to a broader audience. **On the other hand, since EU projects are likely process personal data as well, it is paramount that these processing activities carried out are compliant with the GDPR**.

For this reason, in the context of Work Package 3, cyberwatching.eu created a survey (included in **Annex D**), which aimed to collect information on how EU Projects process personal data in the context of their activities. The purpose of this work was to use their contribution as feedback that will help cyberwatching.eu analyse the EU Cybersecurity & Privacy framework, also with reference to the EU Projects themselves. In this respect, the objective was mostly to provide recommendations to EU Projects in order to support them in addressing compliance with the GDPR.

4.1 Dissemination of the survey

The survey was uploaded on the cyberwatching.eu website and disseminated across the mailing list of cyberwatching.eu in June 2018. Additionally, the survey was distributed to the participants of the Second Concertation Meeting in June 2019.

4.2 Analysis of the responses to the survey

The survey attempted to capture most data protection issues that are potentially applicable to EU projects, with the aim to then give personalised recommendations to their answers. Therefore, the questions will not be looked into in depth, however the entire survey can be found attached in Annex D of this deliverable. A total of 7 European projects responded to the questionnaire.

The first consideration helps understand the geographical scope of the operations of the projects which answered the survey, which is that 66% of the projects were EU-based operating across the EU globally (two or more EU countries); meanwhile 33% of them were non-EU organisations operating in the EU. Interestingly 57% of the projects process personal data of individuals, while only 75% of the projects referred to have provided information to the data subjects prior to the data processing. This goes to show that some projects may not be fully aware of their obligation to provide an information notice to their data subjects. This observation is highly concerning, because if the projects are not provided with easy to understand digestible instructions on how to inform their data subjects of processing activities (as will be provided in the next sub-section) the principle of transparency could be at stake.

Furthermore, when taking a closer look at the question on how the projects ensured that data subjects' rights can be exercised, 50% of the projects chose to leave this answer blank. The lack of action or possibly lack of knowledge of this aspect may be interpreted as an indicator of indifference towards data subject rights or simply lack of guidance or knowledge on how this could be done. However, the other 50% of the projects showed that the exercise of data subject rights was respected through policies of the project and even through the development of systems that can be used in tested databases. This is a positive note, which

proves that EU projects do have the ability to further improve the manner in which they allow data subjects to exercise their rights. However, there may need to be a centralised method which is coordinated at an EU level; in order for the projects to be assisted on this matter. This can be achieved, for example, by funding research initiatives that promote the clarification and creation of practical tools for the exercise of data subject rights. Especially when considering emerging technologies (as in chapter 6), the need of instruments to enhance data subject rights and facilitate their exercise – is a compelling solution to the obligation of exercising data subject rights.

Another observation which can be made is the fact that only 57% of the official website of the EU projects include a Privacy and Cookie Policy. When looking in-depth into the websites of the projects which did not have a Privacy and Cookie Policy, it was noticed that cookies were present on their website. This means that projects may be unaware of the need to include information regarding cookies on their website.

Additionally, to the above, 71% of the projects answered that they have a newsletter, meaning that in one way or another the projects process personal data – which is contrasted to the 57% of the projects which answered positively to processing personal data. Even though this is an assumption that by sending a newsletter the projects process personal data, it goes to show that the projects may continue to be unaware of when their activities imply the processing of personal data.

4.3 Remarks

As was expected when the survey was initially distributed, the recommendations towards the EU projects can be found. As can be noticed in Annex D, each recommendation is corresponding to the questions of the survey.

As final remarks, this survey and the recommendations to the survey will be uploaded on the new website of cyberwatching.eu, as another interactive tool that projects can use to receive recommendations on their data protection posture. The survey will continue to be promoted, in order to reach a higher number of EU Projects, and try to provide useful recommendations to them.

5 Feedback and Recommendations for Horizon Europe and DEP – Reporting from the 2nd Concertation meeting

Based on the outcomes of a series of cyberwatching.eu activities, this part of the document will reflect and provide recommendations for the Horizon Europe and Digital Europe Programmes. This includes reflection and validation of recommendations already included in sections 1-4 of this document which focus on privacy issues and also includes other cybersecurity topics such as standards and certifications and SME needs.

The main activities that are taken into consideration are:

- The 2nd Cyber Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy" (Brussels, 4th June 2019)[23]

[23] https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0

- GDPR compliance in the age of emerging technologies – 7th Cyberwatching.eu webinar (18 July 2019)[24]
- H2020 Project clustering workshop organised by the GHOST Project (Athens, 28 March 2019)[25].

5.1 2nd cyberwatching.eu Concertation meeting

The 2nd Cyber Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy"[26] saw over 60 representatives from all projects in the unit[27] in order to discuss a series of topics, including focus on the key topics and collaboration between the newly funded competence centre pilot projects and discussion on future directions for the Horizon Europe and Digital Europe Programmes.

With a series of plenary and break-out sessions, the event also saw collaboration with ECSO secretariat and ECSO WG chairs who led discussion in a number of these sessions.

The rest of the section will cover the other sessions at the event which include:

- Recommendations for the Digital Europe and Digital Europe Programmes
- Key themes and common definitions of the competence centre pilot projects

5.2 Break-out Sessions

The interactive break-out sessions and open panel discussions at the Concertation meeting provided an opportunity for EU projects to contribute to recommendations for the Horizon Europe and DEP programmes. Therefore, below we have outlined the main recommendations on how to move forward on the key strategic elements which can shape Europe's R&I cybersecurity strategy. The sections are structured taking into consideration the topics to which the Concertation meeting's Break-out Sessions were dedicated.

5.2.1 Cyber security skills and training for SMEs

Chair: Sebastiano Tofaletti, Digital SME Alliance & Chair ECSO WG4 Support to SMEs

In the beginning of the session, the challenges for the future of cybersecurity skills and training for SMEs were identified. These challenges are detailed in Annex E and created the context for the recommendations are mentioned below:

- **Provide support to local networks of SMEs** – trade associations, clusters, environment where SMEs feel familiar and are more likely to reach out for advice. These networks should be equipped with knowledge on how to advise SMEs on cyber security and have tools to organise local trainings, seminars, etc.
- **Fund projects to train service providers, and provide voucher systems, etc:** Provide cybersecurity training and support to service providers of SMEs (e.g. cyber insurance providers, accounting and tax consultants, etc.). They should have a basic knowledge of cybersecurity and privacy so they can at least direct SMEs towards further consulting or giving the basic understanding of where to look for support, raise awareness of cybersecurity and privacy, etc.
- **Fund development of more tools that could support low-level professionals to manage basic cybersecurity**.
- **Supporting them in incorporating cybersecurity to their business plan, business model and HR strategy**: Supporting SMEs in creating cybersecurity strategies and

[24] https://www.cyberwatching.eu/news-events/events/gdpr-compliance-age-emerging-technologies
[25] https://docs.wixstatic.com/ugd/1d2842_ea779c8abd0e45e98cf9d8aa25885592.pdf
[26] https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0
[27] https://www.cyberwatching.eu/brussels-second-cw-concertation-meeting-participants-list

understanding need and economic value of it (potential risk of revenue loss vs. benefits of offering cyber secure and privacy compliant services).

- **Facilitating 'on field' work with SMEs, through bootcamps, hackathons, etc**. Based on such direct interaction with organisers, identification of problems, real solutions can be created.
- **Voucher schemes shall be reinforced more internationally** rather than locally thus fostering cross-border learning and exchange of practices.
- **Exchange programmes** (e.g. something similar to Erasmus+ for entrepreneurs or Erasmus traineeships or Digital Opportunity) shall be encouraged also **for cybersecurity**. E.g., middle-level managers and other professionals shall be sent to train in a bigger company where they could also get basics of cybersecure behavior, see examples of corporate cybersecurity policies, etc.
- More work to be done in standardizing curricular, making eCF more popular and used, aligning it closer to ESCO profiles (because eCF profiles shall also be translated between different countries, education systems, languages). **More attention on common language, certification, etc. in the field of skills.**

Although participants were from different sectors, no concrete sector specific challenges were identified, as cybersecurity skills gap is highly cross-sectoral issue.

5.2.2 Emerging cyber security challenges from emerging technologies

Chair: Roberto Cascella, ECSO WG6 SRIA & Cyber Security Technologies

This session was used in order to come up with the cyber security challenges of emerging technologies. Below the challenges and recommendations that were mentioned during the session. This list of topics should be interpreted taking into consideration the content sections 2.5 (*Recommendations on the GDPR and the NIS Directive: Calls to Action and Next Steps*) and 5.3.2 (*The impact of GDPR on emerging technologies)*.

The challenges that were proposed for the initiatives of Horizon Europe are enlisted below:

- The development of the concept of fairness by design to be complied with by algorithms. Fairness goes beyond what is strictly prescribed by the law, taking into consideration an ethical dimension as discussed above. Like Data Protection by Design, it should be built into the very design of data processing activities, whether they be products, services, or applications and – most importantly – the algorithms that underpin the information/data processing should be designed and developed in a way that is compatible with the concept of "fairness by design".
- More transparency of the algorithms is needed.
- Related to the previous challenges, it is that all emerging technologies must be inclusive of ethical aspects, and the need to spell out practical ethical guidelines on technology.
- Fake news and freedom of speech.
- No legislation on data sharing.
- Sophisticated algorithms to understand whether particular information is collected – seeing as there are different business domains for different information models.
- Process mining, the information process along the supply chain or along the different involved actions whether that is considered GDPR compliance or not,
- Better privacy preserving or privacy conscious cybersecurity measures are needed (seeing as homomorphic encryption is slow),
- It is necessary to enhance performance, because at the moment cybersecurity is still slow,
- More maturity of applications is required: meaning deploying these software applications to the laymen in order to have faster adoption.

As for cybersecurity challenges that can be tackled by the DEP, the recommendations that were discussed are explained below:

- Certification on IoT and the lifecycle of IoT devices is required,
- Forced recovery for devices should be implemented, because if they are compromised, it will necessary to preliminarily detect it and then to force recovery them,
- Trustworthy storage database should be encouraged,
- A method for a secure identification of nodes as sources of information should be investigated,
- More transparency is needed: it is not clear how to effectively inform people about how their data are processed and guarantee their right to object; on this topic the interaction with industry is crucial to investigate realistic solutions to the problem.

5.2.3 Standards and certification for cyber security

Chair: Mark Miller, Conceptivity & ECSO Board of directors and Chair SWG1.3, WG1 Standards, certification

During this breakout session, there were 8 participants. The first half of the session allowed the project participants to present their projects and outcomes. The second half of the session was devoted to an interactive discussion on challenges and recommendations concerning cybersecurity and certification for the future. The projects that presented and their presentations can be found in Annex F. In addition to that, the challenges have been reported in Annex G were brought up as a means of understanding what gaps exist and how the recommendations may help prioritise the future EU initiatives.

The following main topics were recommended as priority recommendations for policy makers:

- **Responsible vulnerabilities disclosure is necessary:** Exchange of threat information needs to be coordinated and standardised. There is a need for standardized vulnerability disclosure. There may be a need for a regulation in this area.
- A GDPR and privacy certification framework should be harmonised across the EU.
- EU National Mutual Recognition in certification is necessary.
- Diversity of Europe is a strength and through the projects interesting tools are created. Build on what has been created in these projects and what remains relevant – in this case, the example of the Atlas tool was given.
- More effort is required to make cybersecurity affordable for SMEs.

This session participants divided priorities according to H2020 and DEP, as follows:

H2020	DEP
Standards, Certification framework	Harmonization
Compliance Free Flow of non-personal data	Enforcing base line security in software
Compliance to GDPR	Standard processes for vulnerabilities
Artificial Intelligence	IoT baseline security
	Accreditation of certification schemes
	Build on ATLAS to develop a dynamic tool
	Responsible vulnerabilities disclosure procedures

Table 2 Standards and certification recommendations

5.3 World-Café Sessions

The sections below are structured based on the five topics covered in the World Café Sessions. Participants circulated around the room discussing the topics with 10 minutes being spent on each topic. The nature of the session means that a high-level view of each topic have been focussed on and this is reflected in the often wide-range of topics that emerge in the summaries. The main exception to this is the impact of GDPR on emerging technologies (5.4.1) which is very much related to the main topic of this deliverable. Therefore, considerable effort has been put into elaborating the discussions that emerged.

5.3.1 The impact of GDPR on emerging technologies

Cyberwatching.eu facilitators: Anastasia Botsi & Laura Senatore, ICT Legal Consulting & cyberwatching.eu

During this World Café session participants were invited to give their ideas and feedback on the topic and were asked to identify which of the instruments chosen for European investments (Horizon Europe or DEP) could be used to address the envisaged challenges. This was also an opportunity for the validation of recommendations already included in sections 2-4 of this document.

5.3.1.1 Recommendations for Horizon Europe

Below the recommendations for Horizon Europe are identified and divided into short, medium and long-term priorities and goals.

A. Short-term

i. ***"European self-assessment toolkit"***

In the interactions, it became clear that a general tool for helping 'translate' the principles, requirements and obligations of the GDPR is missing from the realm of guidance of European legislators. Ideas for this tool could include more practical considerations for the companies that the GDPR applies to, possibly creating divisions of the tool for micro, small and medium enterprises. It was mentioned that, at the moment, elongated opinions and guidelines may at times generate further burden than the one they try to alleviate; therefore, legal complexity intensifies. For this reason, the first short term goal that is worth mentioning is the **necessity for a tool, or several ones, that can serve as more practical instruments to increase the compliance of all organisations (multinationals, medium, small and micro enterprises, research projects) under the scope of the GDPR**. This was placed under the short-term goals because, according to the discussions, it seems that a year after the GDPR has been enforced a lot of controllers and processors struggle with the enforcement of compliance strategies and are in need of practical tools to help them tackle the multiple requirements of the legislation. A practical example of what is recommended at the European level can be seen analysing a "toolkit" that Information Commissioner's Office ("ICO") has created to address the same challenges at national level. In fact, ICO has created a Data Protection self-assessment checklist on topics that they deemed to be crucial to improve the data protection compliance of data controllers and processors, especially for the small and medium-sized organisations.

Cyberwatching.eu recommends that within Horizon Europe, the projects should address this challenge, creating a tool which could work as the ones created by ICO, but taking into consideration the European perception as well as the expertise and decisions coming from the different member states' Supervisory Authorities.

Additionally, and even though it was not explicitly mentioned, for the purpose of this deliverable it is deemed necessary to underline that the same can be said for the companies to which the NIS Directive applies. Especially when considering that emerging technologies will be integrated also in crucial sectors of the society, it is clear that **it would be useful to have practical tools to self-assess the compliance with the NIS Directive – such as a tool that helps organisations to evaluate their security measures taking into proper consideration the level of risk.**

In conclusion, it is important **to develop tools that will:**

a. **practically support organisations to comply both with GDPR and NIS Directive;**

b. **map the overlaps between the two legislative sources and provide methodologies to rationalise compliance efforts for organisations that are subject to both laws;**
c. **measure organisation level of compliance with both sources of law.**

ii. Methodology for GDPR risk assessments

Furthermore, a short-term priority is one which focuses on the **need of clear guidelines for organisations in the field of emerging technologies on methodology to carry out risk assessments.** In fact, this need was confirmed not only during the Concertation meeting but also during the several events attended by the Consortium, where discussions on emerging technologies often arose. Chapter 1 explains that the risk- assessment is a necessary component a risk-based approach required by the GDPR.[28] However, participants to the world café sessions mentioned that the risk-based approach is usually loosely applied by companies. Therefore, it recommended that Horizon Europe concentrates its efforts in structuring a clearly applicable methodology which could be used by organisations to carry out risk assessments. From the legal perspective, the need for a risk assessment comes from the interpretation of articles 24 and 32 GDPR. In fact, in order to adhere to Article 24 GDPR, the controller shall take appropriate technical and organisational measures to ensure and demonstrate compliance according to the risks of varying likelihood and severity for the rights and freedoms of data subjects. Additionally, the risk assessment is necessary under Article 32 in order for both controllers and processors to implement appropriate measures to ensure a level of security appropriate to the risk.

iii. Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches

As an addition to the recommendation of the stakeholders, it is also important to provide **further guidelines on the assessment of the severity of breaches – by using the risk-based approach – and a methodology on how to manage and react to the breaches.** This could include guidelines on the implementation of appropriate measures to prevent the breaches, as well as the provision of a structured approach on assessing and mitigating risks. This is a short-term recommendation as the risk-based approach is one of the most core principles that the GDPR is based on. If organisations are not able to assess the data protection risks of the sector in which they operate, then the implementation of appropriate security measures will be hardly possible and data breaches will be easier to occur and harder to deal with. Thus, this is a recommendation that must stand out when emerging technologies are considered.

More concretely, we believe that a very good practical starting point for this recommendation could be the update and dissemination of the existing Recommendations for a methodology of the assessment of severity of personal data breaches that ENISA created in 2013, prior to GDPR. In the ENISA official website it is mentioned that ENISA, in co-operation with the DPAs of Greece and Germany, has already developed a tool for the notification of personal data breaches (using the existing methodology mentioned before). In particular, the purpose of this tool is to provide for the online completion and submission of a personal data breach notification by the data controller to the competent authority, as well as to provide the competent authority with an assessment of the severity of the breach. **As a result of this recommendation and in the context of the activities related to Task 3.4 (*Legal compliance in cybersecurity and privacy*), cyberwatching.eu is willing to take an**

28

active role in the eventual updating of the existing methodology as well as in testing this tool, with the help of ICT Legal Consulting which would support these activities in the context of the Deliverable 3.7 (*White Paper around Legal Compliance and policy statements including recommendations*).

B. Medium-term

iv. Education and training to raise industry awareness

As for the medium-term goals, one general recommendation arose: education and the raising of awareness on the legislation should be immediately directed to industry players, taking into consideration the size of the entities involved (multinationals, large, medium & small and micro enterprises) as well their sector-specific activities. This becomes even more crucial when one considers the requirements of emerging technologies and crosses them with the challenges that were discussed above in Chapter 2. The data protection challenges discussed above help understand this recommendation further, since they prove that the legislation leaves a gap for uncertainty when it comes to emerging technologies. This recommendation can be considered as referred to both Horizon Europe and DEP. As far as Horizon Europe is concerned, **it is recommended for research initiatives to find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance**. However, DEP seems to also be able to offer support to address this recommendation, since it plans[29] to fund advanced digital skills in the context of designing and delivering short-term training and courses for entrepreneurs, small business leaders and the workforce.

Specifically focusing on the market of **artificial intelligence and internet of things**, three recommendations arose.

v. User-friendly instruments to disseminate Ethics guidelines for AI

Firstly, stakeholders mentioned that the *Ethics guidelines for trustworthy AI* presented in April 2019 by the European Commission's High-Level Expert Group on AI cannot be considered easily comprehensible and concretely usable by all the organisations deploying AI. Cyberwatching.eu interpreted this concern as a **need for more user-friendly instruments to disseminate the content of these guidelines, such as Frequently Asked Questions, official disseminating videos, checklists etc**. It is believed that the European AI Alliance could play a significant role in this topic.

vi. Define common level requirements for cross-border operations

Secondly, organisations in the field of emerging technologies can easily carry out cross-border activities of processing and according to the GDPR, when it comes to certain processing activities, such as those referring to special categories of personal data, the member states are left free to establish a higher level of guarantee to demand.[30] The concrete consequence of that is that the organisations carrying out cross-border operations may have to also take into consideration the content of national legislations. It is clear that such an obligation is demanding and requires resources which some organisations (especially smaller ones, like start-ups) may lack. These circumstances have both a practical and a theoretical impact. Practically, the

[29] For more details see: https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-digital-transformation_en.pdf.
[30] Art. 9(4) GDPR.

need to take into consideration all national localised legislations inevitably places the competitiveness of European enterprises at a disadvantage in the international digital market. Secondly, and on a more theoretical level, it conflicts with the original harmonisation purpose of the GDPR. In order to address this challenge, we believe that **coordinated initiatives between member states (involving legislators, national Supervisory Authorities, European Data Protection Board and European Data Protection Supervisor) must be stimulated, in order for industry players to be able to assess a 'common level of guarantees' needed to comply with the applicable data protection laws.**

vii. Guidelines on AI/machine learning and data minimisation

Thirdly, stakeholders participating to discussion observed that when it comes to AI and machine learning models, it is inevitable to process a large quantity of data to achieve the desired purpose. Therefore, this presumed need to process big data should be balanced with the obligation to respect the principle of data minimisation. Stakeholders observed that there is a lack of solid and technical guidance on this topic and even mentioned that AI and machine learning are by default incoherent with the principle of data minimisation. Therefore, it is recommended that policy makers strive for research initiatives that look into how to concretely deploy AI and machine learning models, respect the principle of data minimization, storage limitation and data accuracy (Article 5 (1) (b), (c), (d) GDPR).

C. Long-term

The long-term goals consisted of many optimistic and visionary recommendations, from which it was chosen to describe the most realistic and concretely applicable ones.

viii. European tool for Data Protection Impact Assessment

As described above, when it comes to the processing with the use of emerging technologies, organisations are often demanded to take into consideration several requirements also coming from national laws or competent national Supervisory Authority's decisions. This is particularly true if we consider what is provided for by art. 35(4) GDPR, which establishes that each national Supervisory Authority had to create and make public a list of processing operations (also known as "black lists") which require a previous data protection impact assessment. As a consequence of that, once again the organisations operating cross-borders might have to take into consideration several applicable black lists when assessing the necessity of a DPIA.

For this reason, a good way to address this challenge could be the **creation of a tool for data protection impact assessments which could compile the several applicable national black lists.** In order to get as concrete as possible, a tool that could help initiate such a pan-european instrument is the tool already created by the French Supervisory Authority carrying out data protection impact assessment. This existing tool could be used by policy makers and EU Projects as starting point to get an updated and pan-european version.

ix. Open source tools for compliance of emerging technologies that are periodically updated according to the state of art

On a more general note, stakeholders recommended that **for emerging technologies there must be practical tools (possibly open source) that are specifically focused on compliance of emerging technologies and that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies**. While, this is undoubtedly a challenging recommendation,

cyberwatching.eu believes it could be concretely achievable by **combining the precious expertise of ENISA with the core projects that have been launched and that will be launched in the context of Horizon Europe**. The alliance of those players could allow for practical tools that are updated on a semester or yearly basis, according to the industry changes and state of art. For this final objective to be achieved it is believed that the **interaction with the industry sector will be crucial**; for this reason, this recommendation can be considered as also referred to DEP.

x. Complexity of processing in the context of AI and principle of transparency

Lastly, during several sessions of the Concertation meeting several participants referred to the topic of the contraposition between the complexity of processing activities carried out in the context of AI and the obligation to give clear and transparent information to data subjects on how their personal data are processed. When it comes to AI and machine learning methods, it is highly **recommended to invest in researching initiatives that aim to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them**. More precisely, a transparent and clear information notice should explain in a user-friendly way the logic of the algorithms applied to the automated processing and the practical consequences on the rights and freedom of the natural persons. According to our experience, companies find it very hard to explain the logic of algorithms, and the possible consequences of automated processing to the data subjects – a task which is hard both for legal personnel and for cybersecurity experts. Furthermore, according to art. 22 GDPR, in case the processing activities carried out in the context of the emerging technologies also implies a decision which can be considered as "based solely on automated processing which produces legal effects concerning the data subjects or similarly significantly affects them", then the organisation shall make sure that the data subjects are able to easily exercise their right not to be subject to such a decision. This concretely means that the organisation is required to implement suitable measures to safeguard the data subjects' rights to ask not to be subject to such a decision and to ask to obtain human intervention on the part of the controller. Addressing this challenge requires intense interdisciplinary work that combines a high legal expertise (i.e. in order to assess when a decision severely impacts on people and in order apply the principles provided for in WP 29 Guidelines on transparency as well as Guidelines on automated processing) with elevated skills in the field of cybersecurity, which allow to master the technical details of decisions based solely on automated processing. [31]

Therefore, **research initiatives should strictly focus on how to safeguard and ensure transparency when the complexity of emerging technologies escalates constantly, as well as on giving guidelines and recommendations on how to concretely identify when a processing activity falls into the provision of Art. 22 GDPR** (because it implies a decision "based solely on automated processing which produces legal effects concerning the data subjects or similarly significantly affects them") **and how to concretely ensure the right not to be subject to the decision and to obtain a human intervention.**

Finally, taking into consideration the key role of the industry players in defining solutions which could fit real market's needs, it was observed as DEP could be concerned as well by this recommendation.

[31] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (11 April 2018), pp. 6-13. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

5.3.1.2 Recommendations for the Digital Europe Programme

A. Short-term

i. Encouraging the creation of codes of conduct to demonstrate compliance

The first recommendation that arose for the DEP is one that regards the **support of the DEP in the creation of codes of conduct, both sector specific and generic, according to the requirements of the GDPR set forth in Art. 40 GDPR.** This would require the combination of legal knowledge and experience but also information from the industries in which these codes of conducts would focus on. **It is recommended that in the context the DEP's objectives the European Commission encourages the creation of codes of conduct that take into account the specific features of the processing sectors as well as the specific needs of micro, small and medium-sized enterprises**. More specifically, DEP projects, national associations, and other bodies representing categories of organisations operating in the field of emerging technologies, such as AI and IoT, may prepare codes of conduct, for the purpose of specifying the application of this Regulation to this specific sector. These codes of conduct could then be used as a means to demonstrate compliance to GDPR, as provided for by Art. 24(3) GDPR. However, at this stage, further research is much needed in order for codes of conducts to be drafted – mostly on how to apply the requirements of legislations, and possibly customise them, to emerging technologies. It is needless to say that if codes of conducts are a mature instrument that can be used to ensure the compliance of emerging technologies to the GDPR – then this recommendation should be prioritised as much as possible.

ii. *Guidelines on anonymisation tools and pseudonymisation mechanisms*

On a more specific note, it was **recommended to create guidelines on anonymisation and pseudonymisation mechanisms which are acceptable as being able to address the challenges of emerging technologies, from a security standpoint**. These guidelines would require research that is funded from an EU level – in order to have a wholistic and pan-European approach to these mechanisms. Even though past guidelines on this topic already exist, specifically published by the Article 29 Working Party in its Opinion 05/2014 on anonymization technique[32], nevertheless its update after the application of the GDPR is undoubtedly necessary. A very good starting point on this topic could easily be the recent "Code of practice on anonymization" published by ICO.

B. Medium-term

i. Structured cooperation between policy makers, the research and the market/industry

Generally, it was frequently mentioned that there must be a continuous "loop of mutual feedbacks" between the policy makers, the research and the market or industry. This recommendation suggests that in the medium-term, the **DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies**. This recommendation ties perfectly with the aforementioned suggestion for Horizon Europe (*Open source tools for compliance of*

[32] WP 29 Opinion 05/2014 on anonymization techniques is available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

emerging technologies that are periodically updated according to the state of art) and give the DEP the mandate of coordinating the industry in order to find an appropriate method for an advantageous and continuous sharing of information. Once this method is decided, then all stakeholders can be part of a larger conversation that would include:

- the industry players, who innovate their products and services and enhance emerging technologies,
- researchers, who help find the gaps of those technologies and recommend methods to close those gaps,
- trainers, who combine the information in order to give back to the community,
- and policy-makers, who can use that feedback constructively in their next legislative initiatives or soft-law guidance.

ii. European certifications, seals and marks on data protection

During the Concertation meeting the stakeholders shared their interest in certifications and seals that could be obtained for data protection, just as it would be for other industry safety standards. This recommendation can be considered as directed to both Horizon Europe and the DEP. As far as Horizon Europe is concerned, cyberwatching.eu strongly believes that **the Member States, the Supervisory Authorities, the European Data Protection Board and, more in general, the European Commission shall encourage, in particular at the European level, the establishment of data protection certification mechanisms and data protection seals and marks described in articles 42 GDPR**. In order to enable the establishment of these seals and marks, there is a **need for a strategic research initiative which will propose a structured approach to certify tools and other instruments created by private entities as compliant at European level**.

Furthermore, as far as the DEP is concerned, it was recommended that **national authorities - but it may be suggestable to elevate this to a pan-European level, e.g., by way of a EU technology certification body - should certify software applications and systems (that would include algorithms or models of artificial intelligence) that are compliant with the GDPR or Ethical Guidelines**. The stakeholders underlined how this could help industry players to demonstrate their compliance to GDPR. On top of this was the **recommendation to support the creation of national certification bodies - but also in this case it may be suggestable to elevate this to a pan-European level, e.g., by way of a EU technology certification body - that are dedicated to emerging technologies, as well as EU-wide certification mechanisms (such as EU data protection seals and marks) that SMEs can also adhere to**. The EU level was particularly emphasised, since most emerging technologies are inherently cross-borders – therefore either the supervisory authorities or national certification bodies must cooperate, or a solution must be proposed at the EU level. Within these discussions, we emphasised that the two last recommendations may be considered as more long-term suggestions, however, industry players that were involved in the car industry, informed cyberwatching.eu that this is an extremely key component of ensuring compliance of emerging technologies. For this reason, it was intentionally chosen to include their recommendations in the medium-term goals – so as to reflect their urgency and prioritisation.

iii. Guidance on implementation of data protection by design and by default in emerging technologies

Lastly, **further research and guidance on how privacy by design and by default can be involved in industry standards for emerging technologies was recommended**. This goes hand in hand with cyberwatching.eu's recommendation described in more depth in Chapter 1. The two principles remain applicable to emerging technologies but there is ambiguity as to how to concretely ensure them; for example, how can a smart home be compliant with privacy by default when a visitor enters that home? This recommendation begs the question on whether further research may yield a fresh outlook on the two traditional principles, and on if a new level or definition of privacy by design and by default could or should be found for emerging technologies.

C. Long-term:

i. ***Practical guidelines on compliance of automated processing in the context of emerging technologies***

The DEP can prioritise to give **guidance on how to demonstrate compliance where the automated processing activities may not be possible or easy to disclose in information notices.** This is a very extensive recommendation that needs a wholistic understanding of all emerging technologies that may apply automated processing, as stipulated in Article 22 GDPR. However, in the span of time, it is likely that GDPR compliance will take a new face for industry players of emerging technologies – in which, most likely would include some sort of automated processing.

5.3.2 Risk management and threat intelligence for SMEs and public administrations

cyberwatching.eu Facilitators: Mark Miller, Conceptivity & Silvia Garbin, AON

Risk management is the basis for assessing and addressing the issues of cybersecurity risks. To this end, there are a number of different standards under the ISO 27000 series which can be used in this way. The challenges are diverse as they vary significantly from industrial sector to industrial sector while the challenges for the citizen involve a number of issues many of which are linked to human factors. It is within this context, that the world café session on Risk Management and Threat Intelligence was facilitated.

The below table is a comprehensive approach to try and identify the gaps and the opportunities that the future European research can fill in. It represents all the discussions that took place in the Concertation meeting. The intention of this session was to represent all the discussions that took place and shows the widest footprint with the of what could be covered by Horizon Europe and the DEP in this sector.

Risk Management / Threat Intelligence	
HorizonEurope	Digital Europe Programme
Information Sharing and Analysis Centres (ISACS)	ISACS
Focus on Vertical sectors, Horizontal topics	Focus on Vertical sectors, Horizontal topics
Mechanisms to incentivise sharing of threat data	Development of automated sensors and automated reactions.
Creation of tools for Academic CERTS and National CERTS	Industrial CERTS (Sectorial CERTS) National CERTS
Reduction of fragmentation of software libraries which include lots of projects	Data driven risk management.
Global depository tracking	Fake solutions for fake news

Assessment of ISO 27000 series: Are they fit for purpose?	Vulnerability management
Automatic detector for risk management/Risk management in unmanaged networks	Create "success" stories around threat intelligence
Data protection Technology	Comparisons of Europe vs what exists abroad
Risk management and assessment management	Promoting crowdsourcing security
Data repository Verticals, post, autoresolve etc	Services and support for end users
Issues of cultural diversity and discrimination in privacy	Improved control of main infrastructure
Services and support for end users (no therapies)	Certification for SMEs and citizens including families
Identification of categories of threat intelligence	Need more "down to earth" info on vulnerability including more actual attacks information
Social networks Creation of caution/warning label and Cyber hygiene promoted body to create Certs and guidelines	Testing of social network outputs from Horizon Europe

Table 3 Risk management/threat intelligence recommendations

5.3.3 International cooperation priorities

Facilitators: Yolanda Ursi, Inmark & AEGIS; Evangelos Markatos, FORTH & PROTASIS

The recommendations emerging from this session are divided into short, medium and long-term ones.

International cooperation and priorities	
HorizonEurope	Digital Europe Programme
Short-term: Focus "**Marie Skłodowska-Curie" programs on cybersecurity**.	Short-term: Create a **Task Force to propose recommendations for the international collaboration in cybersecurity**.
Medium-term: Create an "**ERASMUS" (student/researcher/professor exchange) program for cybersecurit**y.	Medium-term: Provide a **legal framework to make the exchange of cyber-security research data** with selected third countries (such as USA and Japan)
Long-term: work towards making the **GDPR an "international instrument**" – not just a European one. Much like the "Budapest Convention" is a binding international instrument for cybercrime.	Long term priorities were not identified in the session.

Table 4 International cooperation recommendations

5.3.4 Cybersecurity priorities for vertical sectors

Cyberwatching.eu facilitators: Justina Bieliauskaite, Digital SME Alliance (TBC) & Eduardo Gimeno, AEI

Participants agreed that all sectors are different, thus there are specific technical challenges, also often more strict requirements for cybersecurity (e.g. in any strategic infrastructures) or privacy (e.g. health sector). However, general cybersecurity is rather horizontal, and needs and challenges, especially for the SMEs, are similar.

The different groups of participants could not though agree whether there are real sector-specific challenges.

Recommendations for the EC for both Horizon Europe and DEP funding schemes):

- **projects should concentrate more on users' needs analysis**: more attention has to be given to work with small companies and understand what their needs are and how can new tools answer them;
- **more support should be provided to end-users in various sectors** (e.g. in using various tools, understanding cybersecurity and privacy aspects of developed tools, providing usage guidelines for non-tech SMEs, etc.);
- **interoperability** must be encouraged, especially once it comes to **data sharing**. Data sharing should be made easy between different vertical sectors (e.g., data collected in logistics can be also very important for environmental sector, etc.);
- data sharing platforms should be created and used;
- possibilities to 'translate' and 'convert' data, find a common language between sectors is very important and necessary – much more research is needed for this;
- mapping of the main threats across the different verticals could be implemented – this would help to create more flexible and trans-sectoral tools.

5.3.5 How R&I can improve the way that they prepare for the market

Cyberwatching.eu facilitators: Marina Ramirez Jiménez, CITIC and Niccolò Zazzeri, Trust-IT Services

The cyberwatching.eu Technology Radar [33] and market readiness level analysis (see cyberwatching D2.3 Methodology for the classification of projects and market readiness) is used to understand and assess how close the R&I projects are to the market (more details on what was presented in the introductory discussion can be found in Annex G). Discussion led to the following recommendations for for the use of the cyberwatching technology radar and market readiness level analysis:

- MTRL questions could be adapted assess other types of project outcomes different from products and services (i.e. methodologies).
- Could be used to check the behaviour of the different kind of projects (FTI, SME instrument, RIA, IA, etc.) to be able to determine the correction factor for each kind of project.
- Specific questions to accurately assess IA and RIA MTRL could be added.
- Consider the real need of assessing the TRL status frequently in IA and RIA, as this kind of projects are not changing its status until the project is almost finishing.
- Consider assessing partial outcomes from the project instead of the entire project.

[33] https://radar.cyberwatching.eu/?sheetId=https://docs.google.com/spreadsheets/d/1Pa1O-_-qdG32tlIwZ-6aXysemr-KpzhHqlryUm3I-cM/edit#gid=0&sheetName=Autumn&sheetName=Spring%202019

5.4 Priorities of R&I Projects from Webinar: GDPR Compliance in the age of Emerging Technologies

In addition to the Concertation meeting, this section gathers further input from the cyberwatching.eu webinar which focused on GDPR compliance in the age of emerging technologies. The projects that were invited to present – together with cyberwatching.eu legal partner, ICT Legal Consulting, were GDPR cluster projects, namely, BPR4GDPR, DEFEND, PAPAYA, PDP4E, POSEIDON, SMOOTH. Towards the end of the webinar, the speakers that presented were asked to shortly come up with the priorities and suggestions for future funding EU initiatives. Below, we report the recommendations of those speakers.

Firstly, an interesting point was brought up in the context of advertising technology. Specifically, **advertising technology that is carried out in real time,** brings up several data protection concerns. In these type of processing activities, there are many stakeholders involved, meaning that it is difficult to deal with privacy issues due to the lack of clarity of the correct privacy roles. Additionally, advertising technology usually involves large amounts of data, possibly also including special categories of personal data. Therefore, this is a topic that should be further researched and dealt with in the future funding initiatives.

Another priority mentioned is **the need to summarise the main GDPR aspects for sectors or for specific sizes of companies.** A more comprehensive method of adopting the GPDR will make this complex legislation and further decisions, opinions and case law easier to deal with it.

Additionally, **the need for an oversight of companies that provide services** was brought up, suggesting that further research must be done on the creation of a system of registration or licensing of companies. The aim of this system would be to build a trustworthy environment that would also take data protection in mind.

Lastly, **raising awareness of the citizens and organisations remains a priority.** The first step to achieving better data protection is to raise awareness to the emerging technologies to citizens. Specifically focusing on how emerging technologies work, what their consequences may be and the alternative options that people have.

5.4.1 Preparing the European Cybersecurity Competence Network

Earlier this year four pilot projects were launched in order to operate a pilot for a European Cybersecurity Competence Network and to develop a common European Cybersecurity Research & Innovation Roadmap. This shall contribute to strengthening the EU's cybersecurity capacity and tackling future cybersecurity challenges.

In addition to already participating at cyberwatching webinar in April[34], CONCORDIA[35], CyberSec4Europe[36], ECHO[37] and SPARTA[38] all participated at the Concertation meeting addressing how each project will address four topics which are central to the objectives of each project:

- Cyber ranges
- Threat intelligence
- Certification and standards

[34] https://www.cyberwatching.eu/pilots-european-cybersecurity-competence-networks
[35] https://www.cyberwatching.eu/projects/1138/concordia
[36] https://www.cyberwatching.eu/projects/962/cybersec4europe
[37] https://www.cyberwatching.eu/projects/1043/echo
[38] https://www.cyberwatching.eu/projects/1136/sparta

- Skills and capacity building

A key objective for the European Commission is that the projects collaborate and agree on shared definitions of these topics. Already with a joint website published, the Concertation meeting and previous webinar are important platforms for the projects to indeed align activities.

Presentations were provided by each project:

- Gabi Dreo, CODE & coordinator, CONCORDIA[39]
- Géraud Canet, CEA & SPARTA[40]
- Wim Mees, Royal Military Academy & coordinator, ECHO[41]
- David Goodman, Trust in Digital Life & CyberSec4Europe[42]

5.4.1.1 Cyber ranges

Cybersecurity exercise is a powerful tool for enhancing an organization's readiness and resilience against modern cyber threats. The complexity of the enterprise's IT environment has created the need to conduct larger scale cybersecurity exercises to train personnel and develop business and IT processes to handle different cyber incidents. Cybersecurity exercises provide opportunities for organisations to demonstrate critical capabilities and exercises reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets

A cyber range as a multipurpose virtualization environment supporting three "security-by-design" needs knowledge and hands-on skills development; improved system assurance in development; and improved system assurance through security test and certification evaluation. Cyber ranges facilitate high-fidelity simulations, improving stability, security and performance of cyberinfrastructures and information technology (IT), operations technology (OT), and industrial control systems (ICS). They are a vital part of the cybersecurity ecsosysem, enhancing training capabilities for professionals, strengthening the Cybersecurity Ecosystem, and representing real-world Cyber threat scenarios in a virtual environment.

There are two main definitions of cyber ranges:

NIST[43] defines cyber ranges as interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing

EDA[44] defines cyber range as: a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination. It consists of three

[39] https://www.cyberwatching.eu/sites/default/files/CONCORDIA.pdf
[40] https://www.cyberwatching.eu/sites/default/files/SPARTA.pdf
[41] https://www.cyberwatching.eu/sites/default/files/ECHO.pdf
[42] https://www.cyberwatching.eu/sites/default/files/CyberSec4Europe.pdf

[43] https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

[44] https://www.eda.europa.eu/docs/default-source/procurement/annex-a---cyber-ranges-cst.pdf

complementary functionality packages[45],: Cyber Research Range (CRR) Cyber Simulation & Test Range (CSTR), Cyber Training & Exercise Range (CTER).

What are the exisiting cyber ranges?

As there is no strict definition of a cyber range, offerings vary globally in terms of scale, complexity and realism varies globally. Existing cyber ranges vary from larger IT vendors (e.g. IBM, Cisco or Palo Alto networks) cyber ranges to national cyber ranges providing commercial training, development, and research services (Finnish JYVSECTEC's RGCE) and other university or state-owned cyber ranges (Czech KYPO or Swedish CRATE)

Typical cyber ranges may be:

- A pre-defined simple and limited environment to provide infrastructure for Capture The Flag (CTF), e.g. a single virtual machine. Network accessible but limited environment to perform CTF exercises.
- Locally accessible infrastructure, participants must utilize their own laptops and actual work emails and systems; no malware can be used.
- Locally accessible complex and large scale infrastructure, where all equipment and devices are provided by the cyber range vendor/operator, which allows real malware running without fear of malware leaking to Internet or exercising parties business network

What technologies do they use?

The cyber range environment is run on a virtualised infrastructure (networks, servers, end user workstations). Depending on the cyber range, the usage of commercial solutions varies, but almost all cyber ranges utilise open source solutions widely to provide training and exercise environments.

- These solutions vary from basic information security controls (IDSs, firewalls, endpoint-protections (AVs) to more advanced machine learning / data analytical solutions.
- In addition, many of the traditional IT infrastructure solutions (Windows domains, proxies, DNS, etc.) are used to create realistic organisational environments for exercises
- For threat actor modelling, many cyber ranges utilise openly available pen-testing tools and red-teaming tools but also different custom-made tools and malware to represent real cyber attacks
- An ideal Cyber Range should also provide means for trainers in order to record the trainings session including screen captures, session events, trainee goals, and trainer comments. Combined with an automated *scoring system* during the training, trainees

[45] **Cyber Research Range (CRR)** A facility where in close cooperation with research centres, private sector, academic institutions knowledge development (research) takes place. Where newly gained knowledge can be utilised in new products, processes and/or services (development). A facility where e.g. ICT, network information & architecture (NII) in a variety of configurations and circumstances can be analysed. Currently used systems can be analysed as well.

Cyber Simulation & Test Range (CSTR) A facility within the cyber range where the current ICT-reality of a specific network configuration can be simulated, in which possible effects of cyber operations can be tested. The CSTR enables experimental testing of cyber capabilities in a realistic manner, but in a safe, isolated setting.

Cyber Training & Exercise Range (CTER) In order to achieve the necessary growth and sustainability in human capital, a state-of-the-art training & exercise functionality is needed. Modeling & simulation is a valuable asset where knowledge and skills concerning cyber capabilities and cyber operations can be trained and tested. A setting where cyber operators under simulated circ'umstances can be trained for utilizing cyber capabilities.

can automatically be evaluated and graded, making it easy to track performance and achievements for a debriefing after the CyberRange Training.

What open problems do cyber ranges face?

The main challenges that cyber ranges face are outlined below.

Technological	Companies and organizations are increasingly utilising cloud services, and providers are usually focused on global actors such as Amazon, Apple, Microsoft, Facebook, Google, Alibaba. Modelling these vendors' services realistically is non-trivial. Increasingly, security control mechanisms are run on cloud environments for performing the analytics and computing required
Research	For example, data analytics/deep-learning on cybersecurity requires suitable data sets not openly available
Economic	Organisations should increase cyber range usage in their annual business continuity plans to test, develop and verify preparedness against modern threats. Many organizations have not identified the need to exercise, often through lack of understanding of the benefits, usually seen as training for technical personnel, whereas they should be seen as tools to develop the whole organization's capabilities on handling cyber attacks and preparing personnel against major incidents.

Table 5 Challenges around cyber ranges

The four competence centre pilot projects will address the topic of cyber ranges in different ways as outlined below.

ECHO will create a marketplace of ranges. Many ranges are broad in scope while others are very specific focusing on one field only. This will be promoted to companies and cyber-specialists and a variety of users will be able to submit and run scenarios and rent capacity

- ECHO Federated Cyber Range (FCR)
  - Interconnect existing and new cyber range capabilities through a convenient portal.
  - Ranges differ in scope from very broad to very specific including focus on one field only.
  - The FCR will enable access to emulations of **sector specific and unique technologies**
  - The Portal will operate as a **broker** among cyber ranges. For example, companies running their own training could through ECHO, rent and very specific technologies into a scenario.
- To be used as virtual environment for:
  - Development and demonstration of **technology roadmaps**
  - Delivery of specific instances of the **cyberskills training** curricula

Cybersec4Europe will provide a lightweight cyber range from existing proven building blocks:

- modern virtual engines and containers
- technologies for software provisioning, configuration, application management and deployment,
- interoperability standards including REST APIs,

- available datasets and testing data generators as well as virtual learning environments

Cybersec4Europe maps existing cyber ranges and open tools in cybersecurity, industry requirements and will provide a specification for implementation, including a sample integration/ federation infrastructure for cyber ranges and testing. It will also examine and provide open tools for certification and validation, closely aligned with education and standardization.

The prototype of the common portable virtual lab will facilitate not only the actual deployment of opensource tools, but also will support hands-on learning with gamification features for engaging and efficient learning, sample training materials, as well as guidelines for developers describing how to prepare their tools and other supplementary materials (documentation, user interface, testing data, APIs) will also be provided.

CONCORDIA will provide specific training based on world cyber threat scenarios and develop appropriate tools for their use. In order to achieve this CONCORIDA will:

- develop a common portfolio platform to present a Federation of Cyber Ranges across Europe in order to provide Cyber training facilities to the consortium and to others according to specific needs,
- implement means in order to *share scenarios* and *scoring methods* between different CyberRanges and
- provide best practice guidelines for implementing and hosting CyberRanges.

For the purpose of education and training, these prepared and deployed scenarios are designed to provide realistic experience for the trainees. For defender (blue team) training, scenarios may be built on known attack vectors, exploiting vulnerabilities that were not patched, or zero days that are utilized for the first time. Whereas red team training may contain penetration testing scenarios. In these situations the specialists under training learn e.g. how to discover the indicators of compromise, what are the right questions to ask, and how to act immediately based on a short investigation.

In order to provide these realistic scenarios in a Cyber Range, main building blocks have to be built and constantly evolved within CONCORDIA as the threat landscape is evolving as well:

- *Network architecture simulation*: An essential research activity will be the investigation how to map real-world network environments into the simulated cyber range environment. This task include to develop automated network discovery/mapping capabilities to simulate topology, components, tools, configurations and services realistically.
- *Real-world traffic composition*: Beyond the network architecture, mimicking a real-world network traffic is crucial to achieve real-world scenarios. This comprises capture of traffic, analysis and processing of traffic as well traffic composition.
- *Automated adversary behavior*: A third research aspect will be the automation of adversary behavior to enable reproducability of training sessions. Especially, the development of an automated attack generator that is able to adapt to a changing network architecture is in scope of this task.
- *Scoring methodology*: Scoring is an integral part of scenario-based training to document the progress of specialists under training. The choice of scoring components is tightly connected to its technical implementation. The weights of scoring components will be developed and continuously improved as the scenario evolves.

CONCORDIA will develop and continuously evolve cyber range training to achieve better automated and custom-tailored training that correspond to the evolving cyber threat landscape.

SPARTA has no cyber range development, but research to provide enablers. SPARTA will create a catalogue of cyber ranges in Europe which is fully labeled with categories:

- handle complexity of cybersecurity threats and deal with early cyber attacks' kill chain phases
- develop methods and solutions for prediction and awareness- and knowledge-based cybersecurity management
- exchange of Threat Intelligence information between sharing partners and the actionability on such data regarding the GDPR

5.4.2 Threat intelligence

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

Cybersec4Europe will provide an elastic intrusion detection system suitable for cloud deployment based on a multi-disciplinary approach that makes use of network traffic analysis, employs online and offline complementary approaches to overcome:

a) online failure diagnosis for arbitrary faults using a white-box approach through the instrumentation of services and the use of domain-knowledge to finger-point the root of the fault, and
b) offline graph-mining for fault-detection by using graph-mining to collect common interaction patterns and then use it to detect faulty patterns through supervisioned learning.

The objective is to define the requirements and mechanisms to share digital evidence between different expert systems, providing solutions to allow interoperability, either through the unification of languages, formats and interfaces, or through trusted intermediate translators systems respecting the privacy, business requirements and the regulations of different countries

The system will enhance the state of the art for reliability, safety and privacy guarantees of security intelligence techniques based on artificial intelligence, machine learning and data analytics. The investigating mechanisms used will be capable of interacting with Threat Intelligence Information Services to capture evidence of malware activity at an early stage.

Research challenges addressed will include on log and event management, threat detection and security analytics with privacy-respecting big data analytics with the goal of enabling security intelligence in defensive systems, by ensuring the underpinning intelligence systems are fortified.

Based on existing information-sharing tools available on the market today, the **ECHO** Early Warning System will provide a sharing capability allowing information between disparate operational units across organizational boundaries:

- **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
- Secure information sharing **between organizations**; across organizational boundaries and national borders
- Coordination of **incident management workflows**
- Retain **independent management and control of cyber-sensitive** information

- Account for **sector specific needs** and protection of **personal information protection** (GDPR compliant)
- Includes sharing of **reference library** information and **incident management** coordination

CONCORDIA is developing a Threat Intelligence platform for Europe which can be used to share threat information across academic, industrial and other organizations, involving especially the European CERT community. While many initiatives have addressed the needs of cybersecurity data sharing by improving the amount ofactionable information shared, other initiatives focused on new types of actionable information, the qualityof information shared or the preconditions of trusted team-to-team relationships that will lead to share more widely, earlier or even more risky information that might be used against the own organization.
With the development of the CONCORDIA's Threat Intelligence platform these critical issues will be addressed:

- Build a central threat intelligence platform for the exchange of actionable information related to security attacks or incidents to be used within the CONCORDIA consortium supporting the maintenance of trust circles for sharing available information within sub-groups depending on the need of companies and governmental bodies.
- Develop access models for the sharing: (i) open, available to all, (ii) sensitive, available to dedicated organizations, and (iii) restricted, available to selected organizations.
- Based on the CONCORDIA's Threat Intelligence platform, develop applications which support (i) the tagging of likely attributions of attacks, and (ii) the assessment of proactive countermeasures in case of a new emerging attacks, identified vulnerabilities, or campaigns of actors.
- The CONCORDIA's Threat Intelligence platform will support the collection, sharing and discussion of cross-sector threat intelligence by adding specific modules for specific sectors, building on the support of trust circles to ensure the sharing based on sector or governmental sharing policies.
- Develop federated machine learning approaches to share models instead of data.

In addition, CONCORDIA is developing sector-specific threat intelligence platforms for the telco and finance sector.

Next to sharing of threat information, CONCORDIA is planning to host a platform which enables to inform stakeholders about incidents in their constituency. Further researchers are able to provide information such as vulnerabilities in certain networks to the platform and share it with the vetted CSIRTs responsible for the network.

Another aspect, CONCORDIA will work on, is the topic of Course of Actions. Today, within Threat Intelligence mostly the part of sharing and detection is covered but not the part of automated incident response. In CONCORDIA we contribute to the standardization efforts in that area and will develop prototype implementation of such standards.

SPARTA deals with early phases of attacks by predicting where and when an attack may take place. Exchange of information is vital for this.

5.4.3 Certification and standards

Cybersecurity certification and standards are an essential part of a successful Digital Single Market ensuring trust and security in products and services.

The Cybersecurity Act, which came into force in June 2019, can be divided into two parts: in the first part, the role and mandate of ENISA are specified, whilst, in the second part, a European system of certification of the cybersecurity of devices connected to the Internet and other digital products and services is introduced. The Competence Centre pilot Projects focus

on this field and contribute to the activities of ENISA with the broader aim of effective enforcement of cybersecurity as a result of harmonized standards and a corresponding certification system to ensure compliance.

A key ingredient of a successful standard is contribution from a variety of expert sources. **CONCORDIA** will focus on exploitation and contribution to existing international best Cybersecurity measures, techniques, methods etc. and Cybersecurity skills.

At the end of the applicable process, independent assessments will be carried out against these standards with the aim of providing the appropriate validation (this includes people as well as process assessments)

As an R&I project **SPARTA** will carry out research into providing enablers for certification and standards. Assessment is a key aspect of certification, yet it is not scaling up to handle modern digital systems. Main activities include

- Development of more agile assessment and certification frameworks, similar to agile development
- Automation, supporting developers in writing requirements and executing tests
- Assessing systems of systems, beyond individual components, and modularizing assessment to enable assessment of complex systems and services
- Lifetime dynamicity of environments who may have long lifespans, but where individual components might be replaced or upgraded
- Execution elasticity, particularly for services

ECHO is delivering a cybersecurity certification scheme to support ENISA. The ECHO Cybersecurity Certification Scheme:

- Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
- Provide **product oriented** cybersecurity certification schemes
  - Support sector specific and inter-sector security requirements
- Support **delivery and acceptance of technologies** resulting from technology roadmaps
  - **Improve security assurance** through use of **certified products**
- Support development of **Digital Single Market**
  - Limit duplication and fragmentation of the cybersecurity market
  - **Common** cybersecurity **evaluation methods, acceptance** throughout Europe
  - Applicability across **Information Technologies** (IT/ICT) and **Operations Technologies** (OT/SCADA)

CyberSec4Europe defines governance and supporting services for security certification, with research, support, guidance and training for validation and certification of security properties of devices and systems for EU industry.

- Investigating certification for critical infrastructure components
- Aligning efforts with ENISA and ECSO framework policy work
- Cooperating with tools / services, standardization, conformity and validation
- Reducing time to certification of critical sector cyber physical systems by designing a unified certified-by design IoT-enabled CPS framework where overall assurance is guaranteed for the complete system.
- Assessing the Cybersecurity Act, ISO27001 and GDPR following approval of EU Cybersecurity Act.

- Aligning with ECSO, on future certification and harmonisation including governance structures and aspects of the further global penetration of the cybersecurity certification scheme.

CONCORDIA is supporting ENISA in setting up and maintaining the European cybersecurity certification framework by providing the technical background for specific certification schemes. Support the certification authorities with testing and validation capabilities within the European Cybersecurity Certification Frameworks for ICT products and services as proposed by the EC. Certification is known to be an important trust-building measure for services and solutions on the market, but also expensive and often slow task leading to time-to-market delays. By granting access to CONCORDIA's virtual labs to certification authorities and providing them with testing and validation capabilities, solutions and services developed by CONCORDIA members will be better tested, quicker certified, and sooner on the market. Furthermore, CONCORDIA will contribute to the certification process and policies via TUV.

CONCORDIA also focuses especially on IoT software verification to develop new continuous assessment methods to not just certify an IoT device prior to deployment but perform fully automated certification after each update. With for example TUV and RISE CONCORDIA has also approved certification bodies in the consortium.

5.4.4 Skills and capacity building

As reported in D3.2 and discussed at Concertation meeting in 2018, there will be a global shortfall of 3.5 million cybersecurity experts by 2021 There is therefore, a strong need to create technical capabilities in the area of cybersecurity and to change the societal view. The situation is further compounded by a current lack of trainers who also need to be educated themselves. The Competence Centre Pilot projects each address the issue of improving Europe's capacity building in the field.

The **CONCORDIA Cybersecurity Ecosystem** will provide virtual labs, services and training activities. CONCORIDA is also building a sustainable CONCORDIA European Education Ecosystem for Cybersecurity including:

- Open source threat intelligence platform – open source
- Pilot DDoS Clearing house
- Mechanisms for community building, support & incentive models

CONCORDIA will also provide services to promote capacity building in Europe:

- Virtual labs
  - Lab infrastructure to support the development of solutions
  - Hosting infrastructure & personnel for the European Threat Intelligence platform
  - Testing and validation capabilities in support of certification
- Services
  - Portfolio of tools (public and proprietary) & best practices for design, analysis and testing of Cybersecurity systems
- Training for professionals
  - Capture-the-Flag, Red-Blue-teaming events (plan/execute/review)
  - Cyber range training – develop realistic scenarios to address the evolving cyber threat landscape

In view of establishing an European Education Ecosystem for Cybersecurity, the following activities are foreseen:

- Pool, assess and disseminate existing courses for professionals organized by the consortium partners

- Develop a methodology for creation of new courses and/or teaching materials
- Develop new courses for mid-level managers and executives
- Develop a framework for CONCORDIA certificate for courses
- Teach-the Teachers – courses and guidelines
- Networking activities

A key part of this is the newly launched the EU cybersecurity training ***map***. The map includes information on cybersecurity courses from industry and academia within the consortium. To date more than 4,000 cybersecurity professionals were trained via the 20+ courses organized by different Concordia partners. Some of the courses are well established on the market, others are brand new, as to respond to the latest challenges of the Cybersecurity sector.

The map targets mainly IT technical team members and experts, middle managers leading IT or non-IT technical departments, executives, who can all find a course that suits their needs for reskilling, upskilling or simply learn about this challenging domain.

Various filters help match specific need for skills development with the offer. You can choose to sort the courses based on the cybersecurity level addressed (Device-, Network-, Software/System-, Data/Application-, User-Centric), or on the industry sector (e.g. Telecom, Finance, Transport/e-Mobility, e-Health or Defence), but also on the format (face-to-face, online, blended) or the language taught.

Over the course of the CONCORDIA project, the map will be continuously updated with the new courses/trainings developed by the project different university and industry partners. Besides, in our effort for establishing a European Education Ecosystem for Cybersecurity, we opened the map for submission of courses/trainings targeting cybersecurity professionals and organized by other European organizations. The map will thus have the potential to become a marketplace for cybersecurity skills for professionals.

The **ECHO** Cyberskills framework will address the needs and skills gap of cybersecurity professionals based on a mapping of the cybersecurity multi-sector assessment framework. The E-CSF will be made up of learning outcomes, competence model and generic curriculum in order to establish a mechanism to improve the **human capacity** of cybersecurity across Europe

- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome based curricula**
- **Hands-on skills development** opportunities through realistic simulation (ECHO Federated Cyber Range)
- Lessons learned feed **knowledge sharing** (ECHO Early Warning System)

Cybersec4Europe will run its platforms as a capability building instrument open to external sources and third-party material outside the consortium (subject to guidelines and quality standards).

By establishing an education and training framework and related instruments to support continuing education and lifelong learning in cybersecurity, organized to demonstrate the effectiveness of governance models and full transfer of pilot results to the future Centre's operations.

- Learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles.
- Knowledge units and curricula, training and awareness to achieve such objectives and competences, setting activities to apply and test such competencies.

- Implementing the CyberSec4Europe education strategy for citizens, students, and professionals through creating and promoting the project brand and the guidelines / procedures to produce and consume content from platforms developed.

6 SUMMARY OF RECOMMENDATIONS

The main recommendations from this document are detailed below.

- ***Methodology for GDPR risk assessments**:* need for guidelines for organisations, especially in the field of emerging technologies, on methodology to carry out risk assessment. For this purpose, DEP could be utilised as a platform that can bring the policy-makers and the industry closer together through a systematic methodology of risk assessments.
- ***"European self-assessment tool"**:* it is recommended that the EC invests in research initiatives in order to create a tool, or several ones, that can serve as more practical instruments to increase the compliance of all organisations (multinationals, medium, small and micro enterprises, research projects) under the scope of the GDPR.
- ***Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches**:* need for further guidelines on the assessment of the severity of breaches and a methodology on how to manage and react to the breaches. This recommendation could be achieved by updating of the existing methodology from ENISA.
- ***European tool for Data Protection Impact Assessment:*** the creation of a tool for data protection impact assessments, which could compile the several applicable national black lists, is highly recommended.
- ***Encouraging the creation of codes of conduct to demonstrate compliance:*** It is recommended that in the context the DEP's objectives the European Commission encourages the creation of codes of conduct, pursuant to art. 40 GDPR; these codes of conduct should take into account the specific features of the processing sectors as well as the specific needs of micro, small and medium-sized enterprises.
- ***European certifications, seals and marks on data protection:*** the European Commission shall encourage, in particular at the European level, the establishment of data protection certification mechanisms and data protection seals and marks described in articles 42 GDPR. For this purpose, there is a need for a strategic research initiative which will propose a structured approach to certify tools and other instruments created by private entities as compliant at European level.
- ***Education and training to raise industry awareness**:* research initiatives should find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance.
- ***Guidance on implementation of data protection by design and by default in emerging technologies:*** further research and guidance on how privacy by design and by default can be involved in industry standards for emerging technologies is highly recommended.
- ***Practical guidelines on compliance of automated processing in the context of emerging technologies**:* The DEP can prioritise to give guidance on how to demonstrate compliance where the automated processing activities may not be possible or easy to disclose in information notices.
- ***Structured cooperation between policy makers, the research and the market/industry*****:** the DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies.
- ***Guidelines on anonymisation tools and pseudonymisation mechanisms:*** it is recommended that the European Commission stimulates the creation of guidelines on anonymisation and pseudonymisation mechanisms, which are acceptable as being able to address the challenges of emerging technologies.
- ***Guidelines on methodology for risk assessment especially focused on each sector of the OES (NIS Directive) – which are essentially the critical infrastructure of countries:*** ENISA could work together with the DEP stakeholders, with the aim of

producing practical guidelines for assessing the risks in the essential services of member states at a centralised European level.

- ***Clarifications on the intricacies between GDPR and NIS***:
  - DEP could use industry to shed light on the procedures that take place in real time of such circumstances, and the research component (Horizon Europe) should find the most time-efficient and compliant method of managing notifications that fulfill the requirements of both the NIS Directive and the GDPR
  - Policy-makers could provide guidance for organisations on the extent to which sanctions will be applied for both legislations and how such violations will be regarded by competent authorities and member states.

As far as AI is concerned:

- ***Guidelines on AI/machine learning and data minimisation:*** it is recommended that policy makers strive for research initiatives that look into how to concretely deploy AI and machine learning models, respect the principle of data minimization, storage limitation and data accuracy (Article 5 (1) (b), (c), (d) GDPR).
- ***Solutions to address complexity of processing in the context of AI and principle of transparency:***
  - it is recommended to invest in researching initiatives which aim at focusing on how to safeguard and ensure transparency when the complexity of emerging technologies escalates constantly, as well as on giving guidelines and recommendations on how to concretely identify when a processing activity falls into the provision of Art. 22 GDPR and how to concretely ensure the right not to be subject to the decision and to obtain a human intervention***.***
  - research initiatives and policy makers should investigate solutions specifically thought for AI models, that process personal data by means of machine learning algorithms that may change the logic and the impact on individuals over time, processing personal data of individuals for purposes different or incompatible with the ones for which the data were collected; such solutions could imply data subjects, whose personal data is being processed by means of machine learning algorithms, receiving additional information as the AI progresses with it inferences and comes to conclusions.
- ***Guidelines on methodology for risk analysis specifically related to AI***, which should take into consideration the circumstances that the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller, due to the evolving circumstances of the processing activities.
- ***User-friendly instruments to disseminate Ethics guidelines for AI:*** need for more user-friendly instruments to disseminate the content of these guidelines, such as Frequently Asked Questions, official disseminating videos, checklists etc

As far as IoT is concerned:

- ***Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments:*** such guidelines should give advice on how to concretely inform users as per Art.s 12-13-14 GDPR, which legal basis is permitted to process personal data and how data subjects can effectively exercise their rights. Morever, such guidelines should address end-to-end security during the entire data-lifecycle, given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data.
- ***Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR*** are needed, since IoT poses strong challenges to the allocation of privacy roles of the several parties involved in processing. The use of data protection contracts (i.e., Privacy Level Agreements) - other than data processing agreements pursuant to Art. 28 or joint-controllership agreements pursuant to Art. 26 GDPR – should be considered, whereby, regardless of the privacy rules, duties, obligations and responsibilities of the parties involved are clearly spelled out.

As far as Blockchain is concerned:

- ***Practical clarifications on the application of the GDPR to blockchain*** are very much needed for this technology and the law to coexist. It should be clarified how those systems could be specifically crafted, in careful consideration of the rules set by the principles of data protection by design and, specifically, of fairness by design, to ensure that individuals' privacy and real control over their data is afforded to them:
  - While some principles remain largely unaffected by the technology, such as the principle of lawfulness and purpose limitation, and others may even find themselves enhanced by the additional functionalities brought about by blockchain, such as the principle of fairness, others still appear to frontally collide with its 'set-in-stone' nature, namely the principles of data minimisation and storage limitation which, in turn, may affect the ability to effectively exercise some data subject rights regarding personal data stored 'on-chain' (such as the right to rectification or erasure).
  - It is also not a simple matter to identify and agree on the data processing roles played by the participants in a blockchain-based system.
  - An even more complicated matter is to ensure that the formal requirements tied into these roles are met, such as the need for a contract or other legal act containing a set of minimum obligations to be entered into with each processor engaged by a controller, in light of Art. 28 GDPR – this problem currently appears not to have a practically viable solution when considering public blockchains.
  - The matter of international transfers and the implementation of the requirements for their lawfulness raises similar difficulties in light of the decentralised nature of blockchain-based systems.

ANNEXES

ANNEX A. Survey and Recommendations for SMEs: the GDPR Temperature Tool

ANNEX B. Survey and Recommendations for Information notices

ANNEX C. Survey and Recommendations for R&I Projects

ANNEX D. Sample Survey for R&I Projects

ANNEX D. Glossary

ANNEX A. SURVEY AND RECOMMENDATIONS FOR SMES: THE GDPR TEMPERATURE TOOL

For SMEs who are an **EU organisation operating only in its country**, the following recommendation would pop up. Giving this answer would add one point to the SMEs' "GDPR Temperature".

"As an entity operating only in one Member State, please be cautious that this Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].

In short: make sure to stay updated with your country's implementation of the GDPR, especially looking into the points where the GDPR allows Member States to derogate from the GDPR.

For SMEs who are **an EU organisation operating across EU** (two or more EU countries) the following recommendation would pop up. Giving this answer would add two points to the SMEs' "GDPR Temperature".

As an entity operating across the entire EU, please be cautious that each Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or,
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].

In short: make sure to stay updated with the implementation law of the GDPR of the countries where your company operates, especially looking into the points where the GDPR allows Member States to derogate from the GDPR.

For SMEs who are **an organisation from an associated country** (Israel, Turkey, etc.) **operating in EU, or who are a non-EU organisation operating in EU** the following recommendation would pop up. Giving this answer would add two points to the SMEs' "GDPR Temperature".

As an entity not established in the E.U., but operating on the entire EU (meaning, processing the personal data of data subjects who are in the Union), the GDPR **may** apply to you where your processing activities relate to:

1. the offering of goods or services, irrespective of whether a payment of the data subject is required
2. the monitoring of the data subjects' behaviour. [Art. 3 (2) GDPR]

Additionally, if the above conditions apply to your entity, please be cautious that each Member State may define stricter or at least more specific rules on certain areas of the General Data Protection Regulation. For example, a Member State may:

- maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, [Art. 9 (4) GDPR]; or,
- lower the stipulated age of 16 years old in offering information society services directly to a child, with the lowest limitation at 13 years old [Art. 8 (1) GDPR].

In short: make sure to stay updated with the implementation law of the GDPR of the countries where your company operates, especially looking into the points where the GDPR allows Member States to derogate from the GDPR.

2) What is the total annual worldwide turnover of your entity?

Keep in mind that your exposure to GDPR sanctions varies depending on the circumstances of each case; however, it is important to note that for companies, the administrative fine may be up to 2% of your total worldwide annual turnover (for infringements on certain provisions) or even 4% of your total worldwide annual turnover (for infringements on more crucial provisions)."

For SMEs who have a total annual worldwide turnover between 0 and 150.000 euro, zero points would be added to their "GDPR Temperature".

For SMEs who have a total annual worldwide turnover between 150.000 and 500.000 euro, one point would be added to their "GDPR Temperature".

For SMEs who have a total annual worldwide turnover between 5000.000 and 1 million euro, two points would be added to their “GDPR Temperature”.

For SMEs who have a total annual worldwide turnover of 1 million euro and above, three points would be added to their “GDPR Temperature.

3. Does your organisation process special categories of personal data (i.e. sensitive data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or judicial data (such as personal data relating to criminal convictions and offences)?

If an SME responded positive to this question, the below recommendation would be proposed, and five points would be added to their “GDPR Temperature".

Seeing as your company processes special categories of personal data, there are additional obligations expected according to the GDPR. To be more precise, the GDPR stipulates that a data controller is prohibited to process special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, or any data concerning the health or a person’s sex life or sexual orientation) unless the data controller follows on one of the legal basis enlisted in article 9(2) of the GDPR.

More generally, if your company does process such special categories of personal data, the main way to do so is if you have received **explicit consent** to the processing of those personal data. Explicit consent will **not be needed** if one of the below applies to you:

- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the **field of employment** and **social security** and social protection law (i.e., only to be used in employment relationships, or when related to social security);
- the processing is necessary to protect **the vital interests of the data subject** (i.e., only to be used in life or death situations);
- the processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim- in the course of its **legitimate activities**, and, on condition that the processing related **solely** to **members**, **former members**, or to persons regularly contacting the foundation (i.e., a not-for-profit body processes the health data of its members for the purpose of providing them health insurance);
- the processing relates to personal data which are **manifestly made public** by the data subject (i.e., entered their data on a public database provided by a governmental or enforcement authority);

- the processing is necessary for the establishment, exercise or defence of **legal claims** (i.e., when a company must collect such data in order to defend themselves in court proceedings)
- the processing is necessary for the purposes of **preventive or occupational medicine** (i.e., a company that provides medical diagnosis, a company that manages healthcare or social care systems and services, or generally medicine-related companies that may collaborate with health professionals in order to cure a disease or a disorder);
- the processing is necessary for reasons of public interest in the area of **public health** (i.e., a company involved in the protection against serious crossborder threats to health)
- the processing is necessary for **archiving purposes in the public interest**, **scientific** or **historical research** purpose or **statistical** purposes. (i.e., a research company conducts in-depth research for statistical purposes).

In case none of the above applies to the processing activities your company conducts, "explicit" consent is required. "Explicit" refers to the way consent is expressed by the data subject, meaning that in the case where you collect special categories of personal data, the data subject must give an **express statement** of consent such as in a written statement (where possible), or via an electronic form, through the sending of an email, or by uploading a scanned document which is signed by the data subject.[46] Theoretically, oral statements may also be a way to obtain valid explicit consent, however, at a later stage, it may be difficult to prove that all conditions for a valid consent were met when the statement was recorded. [47]

If your organisation uses online software or obtains the personal data online, then two-stage verification of consent may also be a way to make sure explicit consent is valid. [48] An example of this method could be for the data subject to receive an e-mail notifying him/her of the controller's intent to process a record containing medical data, for example, and asking for his/her explicit consent. Then, if the data subject agrees to the use of his/her data, he/she will be asked to send an e-mail reply containing the statement "I agree". Once the reply is sent, the data subject will receive a verification link that must be clicked; either in a follow-up e-mail or via SMS with a verification code, to confirm his/her earlier agreement.[49] You are free to choose other methods to obtain explicit consent, however, it is recommended the ones mentioned above were those that have been suggested by the European Data Protection Board (also known as Working Party 29), in their Guidelines on Consent."

A negative response to this question would add zero points to their "GDPR Temperature.

If the answer to Q3. is yes:

3)B. Does your entity process *genetic data, biometric data,* or *data concerning health*?

[46] Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 18.
[47] Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 18.
[48] Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 19.
[49] Article 29 Working Party Guidelines on consent under Regulation 2016/679, as last Revised and Adopted on 10 April 2018, p. 19.

If an SME responded positive to this question, the below recommendation would be proposed, and one point would be added to their “GDPR Temperature".

Keep in mind that the Member State where you operate may maintain or introduce **further conditions**, or limitations, with regard to the processing of genetic data, biometric data, or data concerning health.

If an SME responded negatively to this question, then zero points would be added to their “GDPR Temperature".

4) Does your entity provide information to individuals (see Articles 12, 13 and 14 GDPR[1]) prior to processing their personal data (i.e. information notice, privacy policy, etc.)?

If an SME responded with a positive answer to this question, the below recommendation would be proposed, and zero points would be added to their “GDPR Temperature".

Providing an information notice to your data subjects is a great start! However, due to the importance of these communications, we have created a further tool that you can use in order to ensure that your privacy policy is compliant with the GDPR. If you would like to receive further recommendations, or simply check your information notice’s compliance to the GDPR click here[50] to be transferred to the additional short survey.

If an SME responded negatively to this question, the below recommendation would be proposed, and four points would be added to their “GDPR Temperature".

As an entity that processes personal data of data subjects, you have the obligation to inform your data subjects, **at the time when the personal data are obtained**, of specific aspects of the processing activity. The most valuable information that must be communicated to the data subject is:

- ❑ the identity and contact details of your entity (as a data controller)
- ❑ the contact details of your data protection officer (in case a DPO has been designated)
- ❑ the specific **purpose** of the processing

[50] The link will lead to the survey described in section 3.2 of this deliverable.

- ❑ the **recipients** or categories of recipients of their personal data
- ❑ the **period** that their personal data will be stored
- ❑ whether the personal data will be transferred outside of the European Union
- ❑ the data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing)
- ❑ The source from which the personal data originates (in case the data was not obtained from the data subjects)[51].

Additionally, it is not enough to simply provide some information about the processing of personal data, therefore we recommend that the information that you do choose to provide is also: 1) concise, transparent, intelligible and easily accessible; 2) written in clear and plain language, particularly if addressed to a child; and 3) free of charge.

Lastly, if you process the personal data based on the consent of the individual, then this consent should be freely given, specific, informed (as per the information described above) and an unambiguous indication of the data subject's intention. The consent should be done by a clear **affirmative action** or by a statement that is specific to the processing of personal data relating to him or her.

If this information is not provided, your company is open to a great risk that may result to a data subject sending a complaint to the supervisory authority, which will likely conduct an investigation into the processes of your company. Any infringements on the data subject's right to be informed about the processing of their personal data can be subject to administrative fines up to 20 000 000 euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

If you would like to receive further recommendations, or simply check your information notice's compliance to the GDPR click here[52] to be transferred to the additional short survey we have compiled.

5) Where needed (see Article 6 GDPR[1]), does your organisation collect individuals consent prior to processing their personal data?

If an SME responded with a positive answer to this question zero points would be added to their "GDPR Temperature".

Alternatively, if an SME responded with a negative answer to this question, the below recommendation would follow, and two points would be added to their "GDPR Temperature".

[51] Art. 14 (2(f)) GDPR.
[52] The link will lead to the survey described in section 3.2 of this deliverable.

According to the GDPR, where no other lawful bases may apply to the processing of personal data, **prior consent** is necessary in order for the processing to take place legally.

Under the GDPR consent has a two-fold criteria, the act of a **correct collection** of consent, but also the controller's ability to **demonstrate** that the data subject has consented to the processing; therefore as an SME you must ensure to have systems in place that collect and store the preferences for consent of the data subject. This evidence may be as simple as a screenshot of the date and time which consent was received or having a database that is regularly updated with all the latest customer preferences.

Additionally, the manner with which the request for consent shall be presented, collected, and granted is important in order to ensure a valid consent. Specifically, consent must be:

1. **Freely given**: implying that a real choice and control of the data subjects exists, therefore as a controller you must ensure that this freedom is communicated and able to be exercised by the data subject. For controllers who are **the employers** of data subjects **pay attention** into the inevitable imbalance that exists, therefore not truly allowing the data subject to freely give his consent; thus, before relying on it, assess whether another legal basis can be utilised instead (i.e. the performance of a contract or legal obligation). Attention should also be paid for the cases where the processing operations may involve more than one purpose, in which case the data subjects should be free to choose which purpose they accept rather than having to consent to a bundle or processing purposes.[53] Lastly, it shall be as easy to give consent as it should be to withdraw it.[54]
2. **Specific**: reiterating that consent must be given in relation to one or more specific purposes. Having that said, consent may still cover different processing activities (or operations), as long as these operations serve the same purpose. An example of this would include having a separate opt-in for each purpose, to allow users to give specific consent for each unique purpose. [55]
3. **Informed**: the requirement of transparency is fundamental, especially when relating to consent, because obtaining the relevant information is necessary in order to enable your data subjects to make informed decisions, understand what they are agreeing to, and what rights they may exercise. An example of informed consent is the inclusion of a summary of the privacy policy or at least a mention of the relevant consequences that will apply once the consent is given **and** a link to the full privacy policy.
4. **Unambiguous**: consisting of a statement from the data subject or a clear affirmative act, through an obvious active motion or declaration. As a data controller, you should be able to show that the consent was indeed granted in a clear way, either via a written or a recorded oral statement – **without the use of pre-ticked opt-in boxes**, which is invalid under the GDPR. Please keep in mind that consent cannot be obtained by the same motion as agreeing to a contract or accepting general terms and conditions of a service

[53] Guidelines on Consent, p.10.
[54] Art. 7 (3) the General Data Protection Regulation.
[55] Guidelines on Consent, p.11.

An example of unambiguous consent can be a privacy policy, accompanied by the request for consent through an optional box at the end – which the data subject can actively tick on "I consent.[56]

As a last note and as can be concluded from the above, consent is not an easy legal basis to implement and it brings upon many further requirements that can burden an SME. Consent may not always be the right legal basis, therefore, before counting on consent and creating systems to ensure that it is valid, you should first check:

- Is the processing necessary for the **performance of a contract** or to take steps **at the request of the data subject** prior to entering into a contract? (Art. 6 (1) (b) GDPR)
- Is the processing necessary for your compliance with a **legal obligation** to which you are subject to? (Art. 6 (1) (c) GDPR)
- Is the processing necessary for the **protection of vital interests** of the data subject or another natural person? (Art. 6 (1) (d) GDPR)
- Is the processing necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority vested in you**? (Art. 6 (1) (e) GDPR)
- Is the processing necessary for the purposes of the **legitimate interest** pursued by you or a third party? (Art. 6 (1) (f) GDPR)

If any of the above legal basis applies, then the legal basis of consent is not necessary and should be avoided.

Not implementing a valid consent into the processing activities is a serious risk, because it means that your company is processing personal data without a lawful basis. Under the GDPR, violations on such basic principles of processing may result to administrative fines up to 20 000 000 EUR, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[57] Additionally, some European Member States may also provide for additional sanctions (such as criminal sanctions). [58]

6) Does your organisation offer online services directly to children aged 13 or over?

If an SME responded with a positive answer to this question, the below recommendation would follow and two points would be added to their "GDPR Temperature".

[56] Guidelines on Consent, p.15.
[57] Art. 83 (5(a)) GDPR.
[58] Artt. 83 (9) and 84 GDPR.

Children, due to their nature and lack of maturity may be less aware of the risks, consequences and security when it comes to providing and protecting their personal data online, therefore a company that offers services to children should be aware that they are taking a greater risk and should introduce even more specific and enhanced safeguards. The GDPR creates an additional layer of protection for all types of collection of personal data of children regardless of its nature. Keep in mind that the age consideration to define "children" is where the child is at least 16 years old, however, the GDPR leaves leeway for each European Member State to decide whether to lower the age to the minimum of 13 years old or somewhere in between."[59]

If an SME responded with a negative answer to this question zero points would be added to their "GDPR Temperature.

If the answer to question 6) is yes:

6)B. Does your organisation collect the consent from the parent or from someone holding the parental responsibility for the child?

If an SME responded with a positive answer to this question, the below recommendation would be proposed, and zero points would be added to their "GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and two points would be added to their "GDPR Temperature".

[59] Art. 8 (2) GDPR.

Where the child is below the age of 16 years, or a lower age provided by each Member State law, the processing of the personal data of a child being offered information society services is only lawful if the consent is given or authorised by the holder of parental responsibility over the child.[60] Therefore, it is clear that receiving valid consent from parents is a crucial point when it comes to handling the personal data of children. If your company offers information society services directly to children, not having a procedure to **collect parental consent** will highly raise the risks to be sanctioned under the GDPR.

The administrative fines applicable in cases of violations to a data controller's obligation to receive valid consent for processing children's personal data may be up to 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7) Does your organisation put in place any form of automated processing of personal data that involves the use of personal data to evaluate certain personal aspects relating to a natural person, such as to analyse or predict its personal preferences, interests, behaviour, etc. (i.e. profiling)?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and four points would be added to their "GDPR Temperature".

Initially, the GDPR stipulates that the data subject shall have the right **not to be subject** to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [61] Therefore, if you plan to conduct any automated individual decision-making (that produces legal effects to the data subject), the only way to do so is if the decision:

[60] Guidelines on Consent, p.24.
[61] Art. 22 (1) GDPR.

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by European or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.[62]

If one of the above legitimate basis is used, as a controller, you must still implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including at least the right to obtain human intervention, to express his or her point of view, and to contest the decision (made through automated processing). [63] In short, this means that if you implement automated individual-decision making, the European legislators expect further rights to be available to data subjects.

Please keep in mind that automated decision-making that involves special categories of personal data is **only** allowed if the controller has received **explicit consent** from the data subject, or if there is a **substantial public interest** to conduct such decision making. Naturally, the safeguards implemented (and mentioned later) must be more suitable, and of a higher level. [64]

So, what exactly are the elements to assess whether you are conducting automated decision-making? Overall, a decision based solely on automated processing means that there is **no human involvement** in the decision process.

However, pay attention to the fact that even if there is a routinely human involvement, but it does not actually influence the result of the automatic decision making, this can still be considered a decision based solely on automated processing. In short, if you are unsure of whether your processing qualifies as an automated processing, then, we recommend assessing whether any human involvement has a meaningful oversight, such as someone who has authority to change the decision, rather than a mere formality. For example, if a tool is implemented on roads in order to verify the speed limit of cars and marks them as above the speed limit, the decision of imposing a speeding fine will be solely based on automated decision making. Continuing with this scenario, if a policeman is involved merely to notify the speeding fines to the car driver and does not have the power to influence the decision itself, this **cannot be** considered human intervention for the purpose of Article 22.

Further, a decision based solely on automated processing needs to produce 'legal' or 'similarly significant effects', meaning that the decision must include serious impactful effects for a data subject, in order for it to be covered under this definition.[65] On the one side, examples of this type of 'legal' effect may be something that affects a person's legal status, or their rights under a contract, such as the termination of a contract, the entitlement / denial of a social benefit

[62] Art. 22 (2) GDPR.
[63] Art. 22 (3) GDPR.
[64] Art. 22 (4) GDPR.
[65] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 21.

granted by law, etc. On the other side, other 'similarly significant effects' may also be sufficient to trigger the definition of automated decision-making, so long as such effects significantly affect the circumstances, behaviour or choices of the individuals concerned, and have a prolonged or permanent impact on the data subject. Examples of decisions that have 'similarly significant effects' may include intrusive profiling, automatic refusal of an online credit application, e-recruiting practices without any human intervention, or decisions that affect someone's access to health services, or to education (i.e., university admissions). [66]

Automated decision-making may partially overlap with profiling; since online advertising has increased reliance on automated tools. In many typical cases, the decision to present targeted advertising based on profiling will not have similarly significant effects on individuals (for example, an advertisement for an online shop based on simple demographic profile 'woman, in Italy, aged between 20 and 30'). However, it is possible that profiling falls under the definition of automated decision-making if the particular case a) implies intrusive profiling process (i.e., tracking individuals across different websites, devices and services), or, b) includes an obvious advert delivery, using knowledge of the vulnerabilities of the data subjects targeted. Additionally, differential pricing based on profiling characteristics and behaviors of the user may also have 'significant effects', if that person is essentially limited from buying certain goods or services. Therefore, automated decision-making may partially overlap with or result from profiling.

All in all, where the decision stemming from profiling activity is **solely** based on automated decision-making, and it produces legal effects, or similarly significant effects, then the profiling is also an automated decision-making processing.

As a controller, you may carry out profiling and automated decision-making so long as you respect all the principles and have a proper legal basis for the processing. When it comes to solely automated decision-making, including profiling, you must apply additional safeguards for all the general principles of the GDPR, such as:

- while providing data protection related information to the data subject (i.e., in the privacy policy), you must additionally provide meaningful information about the logic involved in the automated decision making, as well as the significance and envisaged consequences of such processing for data subjects, for example, how the automated decision-making process is built and how it is used for a decision concerning the data subject; [67]
- providing the right to object to the automated processing has to be explicitly mentioned to the data subject, presented clearly and separately from other information.[68]

Automated processing of personal data allows you to have a structured understanding of your data subjects that may be exploited in several ways, therefore the GDPR requires that automated processing should be accompanied by appropriate safeguards. Below you can find a list drafted by the European

[66] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 22.
[67] Art. 13 (2) (f) GDPR.
[68] Art. 21 (4) GDPR.

Data Protection Board (also known as Working Party 29), which has attempted to offer some good practice recommendations for controllers' safeguards[69]:

- quality checks of systems, regularly, to ensure that individuals are treated fairly;
- algorithmic auditing, by testing the algorithms used and developed by machine learning systems, to check their performance;
- incorporating data minimisation in the automated processes, by identifying clear retention periods for profiles and any other personal data used;
- implementing anonymisation or pseudonymisation techniques in the context of profiling;

the creation of a mechanism where data subjects can request human intervention when they are affected by a decision that is solely based on automated processing (i.e., providing an appeal process). For example, if you receive an e-mail that informs you of an automated decision made using your personal data, in the footer of this e-mail it should be notified that this decision was taken in this way, and also offering a link usable to request a human intervention to be involved in this decision.

If an SME responded with a negative answer to this question, then zero points would be added to their "GDPR Temperature".

8) Does your organisation transfer data outside the EU?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and two points would be added to their "GDPR Temperature".

Any transfers of personal data outside the European Union should always be made with caution, because the GDPR only allows for such transfers where they are subject to appropriate safeguards. The first check that must be done is that on the European Commission's adequacy decisions, which at the moment only offer safeguards for a small portion of non-EU countries.[70] The existence of an adequacy decision means you're your company can transfer to that country without any specific authorisation or extra safeguards than those implemented for transfers within the European Union. You may find a list of the adequacy decisions *here*.

However, for the majority of the cases, there is an absence of an adequacy decision; which means that as a controller or processor, you may only transfer personal data if you have provided appropriate safeguards to ensure the availability of rights and legal remedies for data subjects. Below are some tools that the GDPR offers to provide such safeguards:

[69] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 32.
[70] Article 45 (1) General Data Protection Regulation.

- Standard data protection clauses adopted by the Commission, which are probably the most common way of transferring personal data outside the European. These clauses are model clauses that give the necessary mandate and ensures that safeguards will be implemented in the transfers. It is the most preferred method of legally transferring personal data to non-EU countries because these model clauses can be attached to any contractual agreement or data protection agreement that is to be signed between the exporter (company sending the personal data) and the importer (company receiving the personal data).
- Codes of conduct, which have been approved by the competent supervisory authority (meaning, the supervisory authority that is on the territory of the main establishments of your company) – this may soon be available due to the efforts of Digital SME. If you comply with a code of conduct, you shall still have binding and enforceable commitments from the controller or processor in the non-EU country, in order to ensure that the appropriate safeguards are applied equally to their operations.
- Certification mechanisms, which have been approved by the competent supervisory authority (meaning, the supervisory authority that is on the territory of the main establishments of your company) – this may soon be available due to the efforts of Digital SME. If you comply with a certification mechanism, you shall still have binding and enforceable commitments from the controller or processor in the non-EU country, in order to ensure that the appropriate safeguards are applied equally to their operations.
- Binding Corporate Rules (also known as "BCRs"), is a transfer mechanism that may not be easily applicable to SMEs since it mostly applies to group of undertakings or enterprises that are engaged in a joint economic activity. However, if this is applicable to you, the Binding Corporate Rules are an internal binding contract for the purpose of ensuring that all data transfers within a corporate group are on an adequate level of protection, and must contain both privacy principles (i.e., transparency, data minimisation, purpose limitation) and tools of effectiveness (i.e., audit, training, or complaint handling systems) of the agreement. [71]
- In the absence of any of the above safeguards for transfers, there are specific derogations that may allow you to continue transferring the personal data to a third country; for example:
    - if the data subject has explicitly consented to the proposed transfer (after having been informed of possible risks), or
    - if the transfer is based on the performance of a contract at the data subject's request, or
    - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject, or
    - the transfer is necessary for important reasons of public interest, or
    - for the establishment, exercise or defence of legal claims, or
    - if the transfer is necessary to protect the vital interest of the data subject or of other persons, or

[71] Available on: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

- if the transfer is made from a register which according to Union or Member State law is intended to provide information to the public.[72]

If an SME responded with a negative answer to this question, then zero points would be added to their “GDPR Temperature".

9. Does your company provide employees who carry out data processing activities on your behalf with written instructions (i.e. authorisation to processing of personal data) or training sessions on how to process personal data?

If an SME responded with a positive answer to this question, then zero points would be added to their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and two points would be added to their “GDPR Temperature".

The GDPR does not only focus on technical measures to protect personal data but also organisational safeguards that should raise attention and provide instructions on data protection for the entire company structure, from high level management to the employees or even candidates. Generally, the GDPR specifies that the controller or processor cannot process personal data, except when doing so under instructions from the controller.[73] Therefore, internal company alignment with the expectations and obligations each employee has is integral to lowering a company’s risk to compliance. We would recommend to provide short written instructions to employees when they are onboarding the company, including their responsibilities when processing personal data, as well as the necessary precautions they should take when doing their job.

Lastly, an accountable controller should ensure that its employees who are persons authorised are trained in handling personal data and are aware of the main risks that the processing operations may pose to the protection of the personal data. Additionally, these trainings should be demonstrated to the outer world, by for example, organising annual training sessions and keeping records of the participants of the training.

[72] Article 49 General Data Protection Regulation. For more details on the derogations are available on the Guidelines on 2/2018 on derogations of Article 49 under Regulation 2016/679.
[73] Article 29 General Data Protection Regulation.

10. Does your organisation use suppliers who process personal data on behalf of the organisation?

If an SME responded with a positive answer to this question, then the below recommendation would pop up and one point would be added to their “GDPR Temperature".

If your company has suppliers who process personal data on behalf of your organisation, then they have to act as data processors. An obligation of the GDPR that falls on the hands of the data controller is to give instructions to data processors and ensure that they comply with the obligations set forth in the GDPR and established by the controller. Therefore, your company, as a data controller should take steps such as signing a Data Protection Agreement, to ensure that the data processor will comply with the necessary safeguards.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and two points would be added to their “GDPR Temperature".

If the answer to question 10. is yes:

10.B. Does your organisation provide your suppliers with Data Processing Agreements?

If an SME responded with a positive answer to this question, then one point would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and two points would be added to their “GDPR Temperature".

As a data controller, you are responsible for the personal data you collect and process – as well as the data that is processed by your chosen data processors. Not having entered into any form of contractual agreements with your processors increases your exposure to sanctions of the GDPR.

We recommend ensuring that you enter into a contract with your processors, under the title of a Data Processing Agreement, which will strictly handle data protection matters and clearly stipulate the instructions of the controller towards the processor. A standard Data Protection Agreement must at least include:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data;
- the categories of data subjects;
- the obligations and rights of the data controller against the data processor. [74]

Please mind that violations to controller obligations, such as not properly defining data processors by signing a legally binding contract (or other appropriate legal act) with them, may be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[75]

11. Have you identified whether the appointment of a Data Protection Officer is mandatory for your organisation?

If an SME responded with a positive answer to this question, then zero points would be added to their "GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and one point would be added to their "GDPR Temperature".

Your company should at least identify whether having a Data Protection Officer is mandatory or not, seeing as even some SMEs may need to appoint a DPO due to the large-scale processing that they conduct. You will need to designate a data protection officer if[76]:

- your core activities consist of processing personal data, meaning that regular and systematic monitoring of data subjects is implemented; or
- the core activities consist of processing of special categories of personal data, on a large scale.

[74] Article 28 (3) General Data Protection Regulation.
[75] Article 83 (4) (a) General Data Protection Regulation.
[76] Article 37 (1) General Data Protection Regulation.

If the answer to question 11. is yes then:
11.B. Have you already officially identified and named the Data Protection Officer?

If an SME responded with a positive answer to this question, then one point would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and zero points would be added to their “GDPR Temperature".

If your company has determined that a DPO is necessary, then it is best that you either hire external advisors as your DPO or appoint an internal function as the DPO of your company. A point to keep in mind should be that whoever takes the role of the DPO should be independent in a way that the DPO does not receive any instructions regarding the exercise of his/her tasks, nor are there any conflicts of interests that may appear in his/her function to protect the personal data of the company’s data subjects. This entails that the DPO cannot hold another position within the company that it is expected to determine the purposes and means of the processing of personal data, such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of human resources or head of information technology departments.[77] Apart from identifying that the Data Protection Officer acts independently, it is also important that when chosen, the DPO acts in accordance with the tasks that are enlisted in the GDPR. In short, the DPO shall:

- inform and advise the controller and employees who carry out processing activities,
- monitor the data protection compliance of the company,
- provide advice to conduct data protection impact assessment,
- act as the contact person for cooperation with the supervisory authority.[78]

However, the controller remains the one responsible for taking the final decisions with regards to the processing operations.

12. Have you carried out a risk assessment for the processing activities that you conduct; and subsequently have you implemented appropriate technical and organisational measures to ensure and be able to demonstrate that your organisation processes personal data in accordance with GDPR?

[77] Guidelines on Data Protection Officers, of the Article 29 Data Protection Working Party, Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2016, p.16.
[78] Art. 39 (1) GDPR.

If an SME responded with a positive answer to this question, then two points would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and two points would be added to their “GDPR Temperature".

The risk-based approach that the GDPR has implemented requires all companies evaluate what the risk of each processing activity is, before the processing activity is carried out – that way the company can implement the appropriate technical and organisational measures to ensure a level of security **appropriate to the risk**. The important note for the evaluation of the risk is not only that it indeed occurs but that the company is also able to **demonstrate** that it has occurred.

Therefore, our practical recommendation is to conduct a risk assessment when you are mapping your processing activities. Furthermore, making a document that describes how the risk assessments are done, for the reason of being able to show the logic in cases of investigations. Additionally, you can make an internal document that describes the security measures that are implemented depending on the risk of the processing activity. Having the document on security measures can also serve helpful for when getting in contact with processors who will need to process personal data on your behalf – since you can immediately provide the security standards you expect from them.

Cyberwatching.eu has identified a list of solutions that are provided from cybersecurity projects, which can increase the level of compliance with the GDPR, of SMEs or other companies. We have analysed a few projects that we would recommend can be used in order for your organisation to demonstrate technical and organisational measures taken. Please note that some of these projects may not be directly applicable to you and may be specific to a sector in the wider market.

Consider that, nowadays, having GPDR measures will add value to your services. The controller has to demonstrate that he works with providers that they respect the GDPR – therefore if you are able to guarantee this, then your services will be more valuable.

CREDENTIAL is a Secure Cloud Identity Wallet, which provides end-to-end secure and privacy-preserving platform for managing and storing users’ digital identity information, ranging from authentication credentials over medical reports to tax data or similar. This solution uses cryptographic mechanisms, as well as determining which of their data goes where. If your SME involves data sharing services, this software may be leveraged as a way to extend your portfolio with privacy enhanced and authenticity.

13. Have you identified the processing activities subject to a Data Protection Impact Assessment ?

If an SME responded with a positive answer to this question, then one point would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and one point would be added to their “GDPR Temperature".

When a processing operation is likely to result in a high risk to the rights and freedoms of natural persons, a DPIA will be necessary. This is particularly the case when new technologies are being introduced within your company. Other examples of a processing operation that is "likely to result in high risks" are:

- An automated processing, meaning the systematic and extensive evaluation of personal aspects relating to natural persons, including profiling;
- A processing of special categories of personal data, or a processing relating to criminal convictions and offences on a large scale;
- A systematic monitoring of a publicly accessible area on a large scale.[79]

When it comes to conducting a DPIA, the French Data Protection Authority has offered a modular tool to conduct the assessment, through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector. This software is available in both portal and web versions, and can be found for free here.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, the GDPR has stipulated that **each Supervisory Authority must draft a public list for the kind of processing operations that should be or should not be subject to a data protection impact assessment**.[80]

If the answer to question 13 is yes, then:

13.B. Have you already conducted the Data Protection Impact Assessment?

If an SME responded with a positive answer to this question, then one point would be deducted from their "GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and half a point would be added to their "GDPR Temperature".

When it comes to conducting a DPIA, the French Data Protection Authority has offered a modular tool to conduct the assessment, through a step-by-step process, which can also be customised based on the specific needs of an SME or your business sector. This software is available in both portal and web versions, and can be found for free here.

[79] Guidelines on Data Protection Impact Assessment (DPIA) and determining whoever processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, pg. 8.
[80] Articles 35 (5) and (6) General Data Protection Regulation.

14. Have you assessed whether your organisation is obliged to keep records of processing activities ?

If an SME responded with a positive answer to this question, then one point would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and half a point would be added to their “GDPR Temperature".

The GDPR stipulates the obligation that each controller and processor must maintain a record of processing activities. Nevertheless, it has created an exemption for any enterprise or organisation that employs fewer than 250 persons.[81] However, if your company conducts one of the three following types of processing, then this exception does **not** apply to you:

- If the processing is likely to result in **a risk** to the rights and freedoms of data subjects (you can assess this by conducting a short risk assessment, to check if any risk at all occurs);
- If the processing is **not occasional**;
- If the processing **includes special categories** of data or personal **data relating to criminal convictions** and **offences**.

Therefore, as an SME, it is vital that you check whether one of the three above cases apply to you, since you will then be obliged to keep a record of processing activities. If you do not ensure that you indeed fall into the category of being exempt from the obligation of keeping record of all processing activities, then you will be subject to GDPR sanctions.

If the answer to question 14 is yes then:
14.B. If you have assessed it and you are obliged to keep the records of processing activities, have you already filled out the records?

If an SME responded with a positive answer to this question, then two points would be deducted from their “GDPR Temperature”.

[81] Working Party 29 Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Art. 30 (5) GDPR.

If an SME responded with a negative answer to this question, then the below recommendation would pop up and one point would be added to their “GDPR Temperature".

The record of processing activities should contain at least the following information, if you are a data controller[82]:

- The name and contact details of the controller;
- The name and contact details of the data protection officer, if applicable;
- The purposes of the processing;
- A description of the categories of data subjects;
- A description of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed;
- Transfers of personal data to a non-EU country, where applicable.

Furthermore, he records of processing activities should contain at least the following information, if you are a data processor[83]:

- The name and contact details of the processor or processors, and of each controller on behalf of which the processor is acting;
- The name and contact details of the data protection officer, if applicable;
- A description of the categories of processing carried out on behalf of each controller;
- Transfers of personal data to a non-EU country, where applicable;
- A general description of the technical and organisational security measures.

15. Has your organisation developed a personal data breach management procedure that includes the related notifications and communications?

If an SME responded with a positive answer to this question, then two points would be deducted from their “GDPR Temperature".

If an SME responded with a negative answer to this question, then the below recommendation would pop up and one point would be added to their “GDPR Temperature".

It is needless to say that when a data breach occurs, it is not a moment where a company can improvise its reaction, therefore, it is of extreme importance to have it figured out before it actually happens. The GDPR gives the timeline of notifying the supervisory authority of the data breach within 72 hours, unless

[82] Art. 30 (1) GDPR.
[83] Art. 30 (2) GDPR.

the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subjects. For these reasons you need to have protocol, or a procedure determined in order to recognises **when** a data breach has occurred, **how** it will be recognised, **how** the company will react to it, and **who** will be involved in these steps. The answers to the above questions will result to a procedure on data breach management.

In defining a procedure on data breach management, we suggest taking into consideration the evaluation of the likelihood that the breach results in risks to the rights and freedoms of the data subjects by applying:

- the accountability principle set forth in the GDPR in order to be able to demonstrate the responsiveness and actions taken as a result of a personal data breach to the supervisory authority, by at least documenting any personal data breaches and subsequent actions including: a) the facts relating to the personal data breach, b) its effects to data subjects and, c) the remedial action taken.[84]
- the methodology provided by the European Agency for Network and Information Security (ENISA) to assess the severity of personal data breaches by taking into account:
  1) the data processing context, i.e., the type of data breached, and the overall processing operation,
  2) the ease of identification of the data subjects from the data involved in the breach,
  3) the specific circumstances of the breach, for example, whether it is a loss of confidentiality, or any malicious intent that may be involved.[85]

In addition to notifying the supervisory authority, according to Article 34(1) of the GDPR, the data controller is also required to communicate a breach to the affected individuals, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons". The communication should be done as soon as possible (namely "without undue delay") and aims to provide individuals with specific information about the steps they should take to protect themselves. This could also be done by providing specific advice to individuals to protect themselves from adverse consequences of the breach (for instance, resetting passwords).
Furthermore, breaches should be communicated to the concerned individuals directly with dedicated and transparent methods of communication which can ensure individuals understand the information being provided to them (e.g., email, SMS or prominent website banners in relevant languages).

Notification to individuals is not required when:

– the controller has applied appropriate technical and organisational measures to protect personal data prior to the breach (such as state-of-art encryption);
– immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to

[84] Guidelines on Personal data breach notification under Regulation 2016/679, p.23.
[85] Recommendations for a methodology of the assessment of severity of personal data breaches, p. 9.

materialise;
– it would involve disproportionate effort to contact individuals.

If controllers fail to notify the data breach to the supervisory authority or to communicate it to the data subjects (infringement of Articles 33 and 34 of the GDPR), the supervisory authority will have the possibility to issue administrative fines, whose value can be up to 10,000,000 EUR or up to 2 % of total worldwide annual turnover (Article 83 (4)(a)). Nevertheless, where the failure to notify a breach reveals an absence or inadequacy of existing security measures, the supervisory authority may also issue sanctions for the infringement of Article 32 of the GDPR.

ANNEX B. SURVEY AND RECOMMENDATIONS FOR INFORMATION NOTICES

Does the information notice contain the elements included in the following questions?

1. Who decides **how** the data subject's personal data can be used and for which **purposes**?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

Where the respondent picked the positive answer, the below recommendation would come up.

If your organisation decides how the data subject's personal data can be used, meaning the **means** with which it will be processed (i.e., software, hardware, specific instructions on the use of these data) and for which **purposes** it may be used (i.e., why is the processing of this personal data taking place), then most likely you are a data controller under the GDPR.[86] If you are a controller, as per the above definition, the obligation to provide information to the data subject concerning the processing of their personal data falls on you. Regardless of whether you have collected the personal data directly from the data subject, or, indirectly from another person, this obligation remains with the only difference being that in the latter case the controller shall provide the information either 1) within a **reasonable period** after obtaining the personal data, but at the latest within one month, or, 2) at the time of the **first communication** to that data subject.

From the other hand, if you do not fall within the definition of a data controller, but instead you receive instructions in order to process personal data on behalf of a controller (who determines the means and purposes of the processing), then your role is that of the data processor. In this case, you will need to count on the data controller to provide to the data subject the relevant information. Please be cautious of the cases where you may take the role of the data controller, meaning where you fail to fulfil the instructions given by the controller, or where you determine your own purpose and means of the processing – then you are

[86] Art. 4 (7) General Data Protection Regulation.

considered a data controller under the GDPR.[87] This means that for the cases where you are a data controller the obligation to provide information to the data subject will apply to you.

Where the respondent picked the negative answer, the below recommendation would come up.

If you receive instructions in order to process personal data on behalf of a controller (who determines the means and purposes of the processing), then your role is that of the data processor. In this case, you will need to count on the data controller to provide to the data subject the relevant information. Please be cautious of the cases where you may take the role of the data controller, meaning where you fail to fulfil the instructions given by the controller, or where you determine your own purpose and means of the processing – then you are considered a data controller under the GDPR.[88] This means that for the cases where you are a data controller the obligation to provide information to the data subject will apply to you.

2. The identity and the contact details of the controller?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

It is necessary for the controller's identity and contact details to be disclosed to the data subject; in that way the data subject may contact the controller if any questions, or complains arise in the handling of their personal data.

[87] Art. 28 (10) General Data Protection Regulation.
[88] Article 28 (10) General Data Protection Regulation.

3. If a DPO has been appointed, are its contact details provided in the information notice?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable (No DPO appointed)

Where the respondent picked the positive answer, the below recommendation would come up.

The contact details of the Data Protection Officer must be provided in the information notice, as can be found in Article 13 (1) (b), and Article 14 (1) (b) GDPR.

Where the respondent picked the answer that it is not applicable, the below recommendation would come up.

If you have not assessed whether you need to appoint a DPO, and you are an SME, click **here**[89] to fill out a further survey that will give you further advice on how to handle this matter, if you are a Research and Innovation Project click **here**. [90]

4. How are the personal data processed, meaning for which **purposes**?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

[89] The link will lead to the survey described in section 3.1 of this deliverable.
[90] The link will lead to the survey described in section 3.3 of this deliverable.

The purposes of the processing for which the personal data are intended is necessary to be disclosed, in order for the data subject to have the ability to understand why they shall give away their personal data to you.[91]

5. Which is the **legal basis** of the processing?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

The legal basis of the processing of personal data must be disclosed to the data subject, in this way utmost transparency is offered.[92] In order to ensure a smooth relationship with your data subject, and to enhance transparency, it will be vital for the data subject not only to understand what and how you process the personal data but also to know that it is done in a **legal** manner. There is a variety of legal basis that can be used in order to process personal data, such as consent, the performance of a contract, compliance with a legal obligation, or due to the legitimate interest of your organisation.

6. If any processing is based on the **legitimate interest** of your organisation, what does this legitimate interest involve?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

[91] Article 13 (1) (c) and Art. 14 (1) (c) General Data Protection Regulation.
[92] Article 13 (1) (c) and Art. 14 (1) (c) General Data Protection Regulation.

Where the respondent picked the negative answer, the below recommendation would come up.

It is important to note that where you choose to utilise the legal basis of **legitimate interest**, then the **specific legitimate interest pursued** must be explained to the data subject – this includes a description of the reason for this legitimate interest. [93]

7. Which personal data are processed? (i.e., name, contact details, official governmental documents, health data, etc.)
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

The disclosure of the personal data processed is not required in the scenario where you collected the personal data directly from the data subject.

However, in case where you have **not** obtained the personal data from the data subject directly (i.e., you have receive it from a third person), then this obligation to disclose the personal data is required. If it is not possible to disclose the exact personal data processed due to the large amount, or because it is determined in an ad hoc basis, then you may simply state the **categories of personal data** concerned.[94]

8. With whom are the personal data shared, if any?
   - ❑ Yes, this information is provided
   - ❑ No, this information is missed
   - ❑ Not applicable

[93] Article 13 (1) (d) and Art. 14 (2) (b) General Data Protection Regulation.
[94] Article 14 (1) (d) General Data Protection Regulation.

Where the respondent picked the negative answer, the below recommendation would come up.

The best case would be for the recipients of the personal data to be explicitly listed to the data subject. However, if this is not possible, then the GDPR allows for simply the categories of the recipients to be disclosed, as long as the clustering of the recipients is truthful and without excluding specific categories for internal purposes.

Where the respondent picked the negative answer, the below recommendation would come up.

9. If you intend to transfer the personal data outside the European Union? If yes, does it additionally include the appropriate safeguards on which the is transfer based?
   - ❑ Yes, this information is provided
   - ❑ No, this information is not provided
   - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

If you **intend** to transfer personal data outside the European Union, this needs to be clearly disclosed to the data subject. It is especially important to further explain the existence of the safeguards implemented in order for the transfers to legally take place – safeguards may include: an adequacy decision by the Commission, or binding corporate rules, standard contractual data protection clauses adopted by the Commission, an approved code of conduct, or an approved certification mechanism. [95]

[95] Article 13 (1) (f), Art. 14 (1) (f) and Art. 46 (2) (b), (c), (d), (e), (f) General Data Protection Regulation.

10. For how long are the personal data stored?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

In order to ensure a fair and transparent processing in respect of the data subject**, the period** for which the personal data will be stored **for each purpose** earlier identified should be explained to the data subject. This specification is due to the fact that it is logical that different purposes of processing may also have a different retention period. Sometimes, **the criteria used** to determine the retention period may be sufficient, if it is not possible to describe the retention period to the data subject.[96]

11. The existence of automated decision-making used to make decisions based solely on automated processing (including profiling), which produces legal effects concerning the data subject or similarly significantly affects him / her?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

[96] Article 13 (2) (a), Article 14 (2) (a) General Data Protection Regulation.

Profiling is composwed of three elements: 1) it has to be an **automated** form of processing; 2) it has to be carried out on **personal data**; 3) the objective of the profiling must be to **evaluate personal aspects** about a natural person.[97] An example of profiling may be a data broker collecting data from different public and private sources, on behalf of its clients or for its own purposes, with the purpose of compiling the data to develop profiles on the individuals in order to eventually place them into segments.

Solely automated decision-making has a different scope, in that it is the ability to make decisions by technological means, without human involvement. For example, giving out speeding fines purely on the basis of evidence gathered from speed cameras.

If you employ solely automated decision-making, including profiling, which produces legal effects concerning the data subject, or similarly significantly affecting him / her, then you must ensure to explain **clearly** and **simply** to individuals how the profiling or automated decision-making works. [98] In short: you must offer meaningful information about the logic involved.

If the processing involves profiling-based decision making, then it must be clarified to the data subject that the processing takes place for **both purposes** (a) profiling, and (b) making a decision based on the profile generated. [99]

Additionally, the data subject should be informed not only about a right *to be informed* about but also, in certain circumstances, a right *to object to* **profiling**, regardless of whether it is solely automated individual decision-making based on profiling takes place.[100]

[97] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.6-7.
[98] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.
[99] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.16.
[100] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.17.

If answer to Q11. is Yes:

12. As a result of the automated decision-making, an explanation of the consequences for the data subject?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

You must provide information about intended or future processing, and how the automated decision-making might affect the data subject – the significant and the envisaged data protection consequences. [101] In order for this information to be understandable by any data subject, it must be accompanied with examples of the type of possible effects. Taking the example given by the Working Party 29 in the Guidelines on Automated individual decision-making and Profiling: an insurance company uses an automated decision-making process to set motor insurance premiums based on monitoring customers' driving behaviour. It provides an app comparing fictional drivers (including ones with dangerous habits) in order to illustrate the significant and envisaged consequences of the automated-decision processing they would like to use. [102] The Guidelines on Automated individual decision-making and Profiling further advice that other visual techniques may be used to explain how a paste decision has been made, that way the data subject can clearly conceive the consequences.

[101] Art. 13 (2) (f), Art. 14 (2) (g) General Data Protection Regulation.
[102] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last Revised and Adopted on 6 February 2018, p.26.

13. Are my data further processed for a purpose other than that for which they were obtained?
- ❑ Yes, this information is provided
- ❑ No, this information is missed
- ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

Where you plan to further process the personal data for a purpose other than the one for which the personal data were **initially collected**, firstly you must ensure that the further processing is **compatible** with the original purposes. In order to do so you must assess the elements stated in Art. 6 (4) GDPR (such as, the link between the initial and further purpose, the context of the personal data, the nature of the personal data, etc.)

If the further processing is indeed compatible, then prior to the further processing, you must inform the data subject on the purpose and any other relevant information that changes due to the additional purpose of processing. Additionally, according to the Article 29 Working Party, you must provide further information on the **compatibility** analysis carried out (and as stated above). In this way, you give the opportunity to the data subject to consider the compatibility of the further processing and decide whether they want to exercise their rights (e.g., the right to restriction of processing or the right to object to processing).[103] The point is that the data subject should reasonably expect that at the time and in the context of the collection of personal data a processing for a particular purpose may take place.[104] Examples of further processing may be for scientific or historical research purposes or statistical purposes.

14. Where the personal data is collected from third-parties, or in another way other than directly from the data subject - is the source of collection of the personal data specified?
- ❑ Yes, this information is provided
- ❑ No, this information is missed
- ❑ Not applicable

[103] Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.24.
[104] Recitals 47 and 50 General Data Protection Regulation.

Where the respondent picked the negative answer, the below recommendation would come up.

Seeing as the data subject has not directly given out their personal data to you, the information notice will need to specify from which source the personal data originates, and if applicable, whether it came from publicly accessible sources.[105]

15. The existence of the right to request from the controller access to and rectification, or erasure of personal data, or restriction of processing concerning the data subject, or to object to processing, as well as the right to data portability and the right to withdraw consent, where applicable?

Where the respondent picked the negative answer, the below recommendation would come up.

The data subject must clearly be informed about their rights under the GDPR, including the[106]:

- Right to obtain a confirmation from the controller of the personal data concerning him or her that are being processed, **and** access that personal data;
- Right to rectify or erase their personal data without undue delay;
- Right to restrict the processing of their personal data where the personal data is inaccurate or the processing is unlawful, or the controller no longer needs the personal data for the purpose(s) of the processing;
- Right to object, at any time, when the processing of their personal is based on the legitimate interest of the controller, **or** on the performance of a task carried out in the public interest;
- Right to data portability in a structured, commonly used and machine-readable format
- Right to lodge a complaint with a supervisory authority;
- Right to withdraw their consent, at any time, if the legal basis used by the organisation is consent (or explicit consent).

[105] Art. 14 (2) (f) General Data Protection Regulation.
[106] Art. 13 (2) (b), (c), (d) and Art. 14 (2) (c), (d), (e) General Data Protection Regulation.

The GDPR does not only require for the correct **elements** (as found in the questions above) to be included in the information notices, but also for the **way** it is communicated to be transparent. In a recent investigation by the French Data Protection Authority ("CNIL") the tech giant Google LLC got fined 50 million euros for **lack of transparency**, and **inadequate information** due to the excessive multi-layered approach they took in providing information.

This goes to show that in order to follow the GDPR **principle of transparency** a controller must ensure to have an effective means of providing information to the data subject. If you want to find out your compatibility with it, answer the following questions.

16. Is the information notice concise, transparent, intelligible and easily accessible?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

The information must be presented in an efficient manner ("concise and transparent"), in order to avoid information fatigue. For this reason, the privacy policy should be differentiated from other non-privacy related information (i.e., contractual provisions or general terms of use). In the cases where the information notice is provided online, it is also possible to use a layered approach, which will allow the data subject to navigate to particular sections that may be of interest to them without having to read the whole text. The Guidelines on Transparency by the Working Party 29 state that the information should be understood by an average member of the intended audience ("intelligible") – meaning that you may need to try different mechanisms to find the most appropriate manner of presenting the information. Lastly, the information notice should be able immediately apparent to the data subject, for example, providing it directly to them, linking them to it, or having it appear in Frequently Asked Questions (FAQs).

17. Is the information notice written in clear and plain language?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

Where the respondent picked the negative answer, the below recommendation would come up.

You should aim to provide the information in as simple a manner as possible, without including complex sentences and legal language. Furthermore, the information should be concrete, not leaving any space for doubts or misunderstandings or other interpretations by the data subjects.[107] It is especially important that the purposes and the legal basis for the processing is clear. Please keep in mind that the requirement for clear and plain language is even more important when the information is provided to children, therefore the vocabulary, tone, and style of the language should be adapted so that the children understand the information that is being presented to them.[108]

18. Is the information notice provided free of charge?
    - ❑ Yes, this information is provided
    - ❑ No, this information is missed
    - ❑ Not applicable

As a data controller, you cannot charge data subjects simply for providing them information in a general manner; or in a way that seems as a condition for the purchase of services or goods.[109]

[107] Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.6.
[108] Article 12(1) General Data Protection Regulation.
[109] Guidelines on Transparency under Regulation 2016/679, as last Revised and Adopted on 11 April 2018, p.6.

ANNEX C. SURVEY AND RECOMMENDATIONS FOR R&I PROJECTS'

1) Does your project involve the processing of personal data of individuals?

A positive answer would result in the recommendation that since the project processes personal data of individuals, this means that it will need to comply with the GDPR.

A negative answer would result in the recommendation that since the project does not process personal data of individuals, this means that it will not necessarily need to comply with the GDPR.

1A - Does your project respect the general personal data protection principles as contained in Article 5 GDPR (lawfulness, purpose limitation, transparency, fairness, data accuracy and minimization, safety, data protection by design and by default)?

A negative answer would result in the following recommendation.

Every entity that processes personal data must adhere to the core principles of Article 5 GDPR.

Firstly, the project must ensure that it has a lawful ground to process personal data. Consent is not an easy legal basis to implement and it brings upon many further requirements that can burden your project. Consent may not always be the right legal basis, therefore, before counting on consent and creating systems to ensure that it is valid, you should first check:

- Is the processing necessary for the **performance of a contract** or to take steps **at the request of the data subject** before entering into a contract? (Art. 6 (1) (b) GDPR)
- Is the processing necessary for your compliance with a **legal obligation** to which you are subject to? (Art. 6 (1) (c) GDPR)
- Is the processing necessary for the **protection of vital interests** of the data subject or another natural person? (Art. 6 (1) (d) GDPR)
- Is the processing necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority vested in you**? (Art. 6 (1) (e) GDPR)
- Is the processing necessary for the purposes of the **legitimate interest** pursued by you or a third party? (Art. 6 (1) (f) GDPR)

If any of the above legal basis applies, then the legal basis of consent is not necessary and should be avoided.

Furthermore, the personal data must be collected for specified, explicit and legitimate purposes; meaning that the data cannot be further processed in a manner that is incompatible with those original purposes. If, however, the further processing is for archiving purposes in the public interest, scientific or historical research

purposes or statistical purposes it may not be considered to be incompatible with the initial purposes if there are sufficient safeguards in place (check out article 89 GDPR).

Also, the data that the project collects must be stored only for as long as is necessary to fulfil the purposes for which they are processed. This principle includes both an exercise (prior to collection) of limiting the data requested from a data subject to that which is relevant, as well as the retention of the data for the minimum amount possible. Closely related with this principle is the practice of checking that the form - in which the personal data permits the identification of the data subject is stored- does not exceed the time necessary to fulfil the purposes. Therefore, the personal data can only be stored for longer than necessary if the personal data will be used for archiving, scientific or historical research, or statistical purposes. In these last cases, the personal data would need to be secured in organisational and technical ways, in order to ensure that the identification of the individual is not compromised (i.e. pseudonymisation, hashing, or anonymisation).

When personal data is collected, the project must take all necessary steps in the context of the processing of the personal data, to ensure that the data is also kept up to date and remains accurate. This should include the immediate erasure or rectification of any irrelevant or inaccurate data.

As is more commonly known, the personal data must be appropriately secured from unauthorised or unlawful processing, or from the accidental loss, destruction or damage. This is an important component as part of the overarching principle of accountability and the risk-based approach. The risk-based approach essentially requires that any entity that processes personal data undergoes an evaluation of the risks that are involved in the processing activities. As a result of this assessment, the appropriate security measures will be taken -both organisational and technical – in order to lower the risk as much as possible (also taking into consideration the costs of implementing such measures and whether they are proportionate with the activities and abilities of the entity).

1 B - Was information provided to data subjects (see Articles 12, 13 and 14 GDPR) and their consent collected (if needed, see Article 6 GDPR) prior to data processing?

A negative answer would result in the following recommendation.

As a project that processes personal data of data subjects, it has the obligation to inform data subjects, **at the time when the personal data are obtained**, of specific aspects of the processing activity. The most valuable information that should be communicated to the data subject is: the identity and contact details of your project (as a data controller), the contact details of your data protection officer (if you process personal data **occasionally**), the specific purpose of the processing, the recipients or categories of recipients of their personal data, the period that their personal data will be stored, whether the personal data will be transferred outside of the European Union, and their data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing).

Additionally, per the GDPR, it is not enough to simply provide some information about the processing of personal data, therefore it is recommended that the information that the project do chooses to provide is also: 1) concise, transparent, intelligible and easily accessible; 2) written in clear and plain language, particularly if addressed to a child; and 3) free of charge.

Lastly, if the project processes the personal data based on the consent of the individual, then this consent should be freely given, specific, informed (as per the information described above) and an unambiguous indication of the data subject's intention. The consent should be done by a clear **affirmative action** or by a statement that is specific to the processing of personal data relating to him or her.

1 C - How did you ensure data subjects' rights (such as right to access, to rectification, to erasure, to restriction of processing, to data portability, to object and to not be subject to a decision based solely on automated processing)?

This was an open answer and therefore did not include a standard recommendation because it would be a direct recommendation to the answer of the project at hand (via e-mail). The most probable recommendation is the following.

In order to ensure the data subjects' rights, it is necessary to include an information notice, and demonstrate an e-mail address that can be used in order for data subjects to reach out to the project for data protection matters. Within the privacy policy, the project must explain that under the GDPR every data subject may:

- Access their personal data being processed, as well as information on the processing of your personal data;
- Correct or update their personal data, where it may be inaccurate or incomplete;
- Request erasure of their personal data, if they believe that the processing is unnecessary or unlawful;
- Request the restriction of the processing, where it can be proven that the processing is inaccurate, unnecessary or unlawfully processed, or where the data subject has objected to the processing;
- Exercise their right to portability, by asking for a copy of their personal data in a structured, commonly used and machine-readable format, as well as the transmission of that personal data to another data controller;
- Object to the processing of your personal data;
- Withdraw their consent to processing which is done for marketing or profiling purposes.
-

Additionally, the project must ensure to state the procedure for exercising data subject rights, such as e-mailing the address stated. Further, a short internal procedure that shows the method of managing data subject requests can be created, in order to ensure that the answer is provided to the data subject within 1 month.[110]

1 D - Does your project involve the processing of special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or judicial data (such as personal data relating to criminal convictions and offences)?

A negative answer would result in the following recommendation.

Seeing as the project processes special categories of personal data, there are additional obligations from the regular consent that was discussed above. To be more precise, the GDPR stipulates that a data controller cannot process special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic or biometric data, or any data concerning the health or a person's sex life or sexual orientation) unless the one of the conditions set forth in Art. 9(2) is met. However, if the project does process such special categories of personal data, the only way to do so is if it has received **explicit consent** to the processing of those personal data. Explicit consent will not be needed if:

- the processing is necessary to protect the vital interests of the data subject (i.e., only to be used in life or death situations),
- the processing relates to personal data which are manifestly made public by the data subject,
- the processing is necessary for the purposes of preventive or occupational medicine,
- the processing is necessary for reasons of public interest in the area of public health,
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purpose or statistical purposes.

Explicit refers to the way consent is expressed by the data subject, meaning that in the case where the projects receive special categories of personal data, the data subject must give an **express statement** of consent such as in a written statement, or via an electronic form using an electronic signature, through the sending of an email, by uploading a scanned document which is signed by the data subject. Theoretically, oral statements may also be a way to obtain valid explicit consent, however, at a later stage, it may be difficult to prove that all conditions for a valid consent were met when the statement was recorded.

[110] Article 12(3) General Data Protection Regulation.

If the project uses online software or obtains the personal data online, then two-stage verification of consent may also be a way to make sure explicit consent is valid. This method could be for the data subject to receive an e-mail notifying him/her of the controller's intent to process a record containing medical data, for example, and asking for his/her explicit consent. If the data subject agrees to the use of his/her data, they will be asked to send an e-mail reply containing the statement "I agree". Once the reply is sent, the data subject will receive a verification link that must be clicked (in a further, delayed e-mail) or an SMS with a verification code, to confirm his/her agreement.

There are many methods to obtain explicit consent, however, it is recommended to use one of the above as they have been suggested by the Article 29 Working Party.

1 E - Does your project involve decisions based solely on automated processing, including profiling?

A negative answer would result in the following recommendation.

Initially, the GDPR stipulates that the data subject shall have the right **not to be subject** to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [111] Therefore, if the project plans to conduct any automated individual decision-making (that produces legal effects on the data subject), the only way to do so is if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by European or Member State law to which the controller is subject to and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.[112]

If one of the above legitimate basis is used, as a controller, the project must still implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including at least the right to obtain human intervention, to express his or her point of view, and to contest the decision (made through

[111] Art. 22 (1) GDPR.
[112] Art. 22 (2) GDPR.

automated processing). [113] In short, this means that if the project implements automated individual-decision making, the European legislators expect further rights to be available to data subjects.

Please keep in mind that automated decision-making that involves special categories of personal data is **only** allowed if the controller has received **explicit consent** from the data subject, or if there is a **substantial public interest** to conduct such decision making. Naturally, the safeguards implemented (and mentioned later) must be more suitable, and of a higher level. [114]

So, what exactly are the elements to assess whether you are conducting automated decision-making? Overall, a decision based solely on automated processing means that there is **no human involvement** in the decision process.

However, pay attention to the fact that even if there is routinely human involvement, but it does not actually influence the result of the automatic decision making, this can still be considered a decision based solely on automated processing. In short, if the project is unsure of whether its processing qualifies as automated processing, then, it is recommended to assess whether any human involvement has a meaningful oversight, such as someone who has authority to change the decision, rather than a mere formality. For example, if a tool is implemented on roads to verify the speed limit of cars and marks them as above the speed limit, the decision of imposing a speeding fine will be solely based on automated decision making. Continuing with this scenario, if a policeman is involved merely to notify the speeding fines to the car driver and does not have the power to influence the decision itself, this **cannot be** considered human intervention for the purpose of Article 22.

Further, a decision based solely on automated processing needs to produce 'legal' or 'similarly significant effects', meaning that the decision must include serious impactful effects for a data subject, for it to be covered under this definition.[115] On the one side, examples of this type of 'legal' effect may be something that affects a person's legal status, or their rights under a contract, such as the termination of a contract, the entitlement/denial of a social benefit granted by law, etc. On the other side, other 'similarly significant effects' may also be sufficient to trigger the definition of automated decision-making, so long as such effects significantly affect the circumstances, behaviour or choices of the individuals concerned, and have a prolonged or permanent impact on the data subject. Examples of decisions that have 'similarly significant effects' may include intrusive profiling, automatic refusal of an online credit application, e-recruiting practises without any human intervention, or decisions that affect someone's access to health services, or to education (i.e., university admissions). [116]

Automated decision-making may partially overlap with profiling; since online advertising has increased reliance on automated tools. In many typical cases, the decision to present targeted advertising based on profiling will not have similarly significant effects on individuals (for example, an advertisement for an online shop based on simple demographic profile 'woman, in Italy, aged between 20 and 30'). However, it is possible that profiling falls under the definition of automated

[113] Art. 22 (3) GDPR.
[114] Art. 22 (4) GDPR.
[115] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 21.
[116] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 22.

decision-making if the particular case a) implies intrusive profiling process (i.e., tracking individuals across different websites, devices and services), or, b) includes an obvious advert delivery, using knowledge of the vulnerabilities of the data subjects targeted. Additionally, differential pricing based on profiling characteristics and behaviours of the user may also have 'significant effects', if that person is essentially limited from buying certain goods or services. Therefore, automated decision-making may partially overlap with or result from profiling.

All in all, where the decision stemming from profiling activity is **solely** based on automated decision-making, and it produces legal effects, or similarly significant effects, then the profiling is also an automated decision-making processing.

As a controller, the project may carry out profiling and automated decision-making so long as you respect all the principles and have a proper legal basis for the processing. When it comes to solely automated decision-making, including profiling, the project must apply additional safeguards for all the general principles of the GDPR, such as:

- while providing data protection related information to the data subject (i.e., in the privacy policy), the project must additionally provide meaningful information about the logic involved in the automated decision making, as well as the significance and envisaged consequences of such processing for data subjects, for example, how the automated decision-making process is built and how it is used for a decision concerning the data subject; [117]
- providing the right to object to the automated processing has to be explicitly mentioned to the data subject, presented clearly and separately from other information.[118]

Automated processing of personal data allows you to have a structured understanding of the project data subjects that may be exploited in several ways, therefore the GDPR requires that automated processing should be accompanied by appropriate safeguards. Below the project can find a list drafted by the European Data Protection Board (also known as Working Party 29), which has attempted to offer some good practice recommendations for controllers' safeguards[119]:

- quality checks of systems, regularly, to ensure that individuals are treated fairly;
- algorithmic auditing, by testing the algorithms used and developed by machine learning systems, to check their performance;
- incorporating data minimisation in the automated processes, by identifying clear retention periods for profiles and any other personal data used;
- implementing anonymisation or pseudonymisation techniques in the context of profiling;
- the creation of a mechanism where data subjects can request human intervention when they are affected by a decision that is solely based on automated processing (i.e., providing an appeal process). For example, if an e-mail is sent informing data subjects of an automated

[117] Art. 13 (2) (f) GDPR.
[118] Art. 21 (4) GDPR.
[119] Guidelines on Automated individual decision-making and profiling, for the purposes of Regulation 2016/679, pg. 32.

decision made using their personal data, in the footer of this e-mail it should be notified that this decision was taken in a specific way, and also offering a link usable to request a human intervention to be involved in this decision.

2) On the official website of your project is there a registration form?

A positive answer would result to the following recommendation.

A registration form is a source where personal data is being collected. The first recommendation would be to reconsider what kind of information the project needs to obtain from this registration, usually, this is the e-mail address, the name, and possibly some other contact details. The most important question to ask is what information is **mandatory** for the services or results to be accurate and efficient. Therefore, the recommendation would be to not require many fields of information in order for the registration to be completed. These methods will ensure that you follow and comply with the principle of minimisation (gather as little personal data as possibly necessary), as well as the principle of data protection by design (design your processes in a way that personal data is being taken into account). The second recommendation regards check-boxes concerning a sign up to your newsletter, results or similar subscription information. According to the principle of data protection by default, the data subjects should be protected **by default** of the data processes; which in the case of the check-boxes is to not have them pre-checked but allow for the data subject to consent to the subscription of the newsletter or for sharing marketing information.

3) On the official website of your project, is there Privacy and Cookie Policy?

A positive answer would result to the following recommendation.

The fact that the project already has a Privacy and Cookie Policy is a great start. However, it is recommended ensuring that it is compliant to the GDPR. The relevant information that should be included in the Privacy and Cookie Policy will depend on what type of personal data the project gathers, and the kind of cookies are implemented on the website.

The most valuable information that should be communicated to the data subject includes:

- the kind of personal data that is collected and processed
- the identity and contact details of your project (as a data controller),
- the contact details of the data protection officer (if the project processed personal data **occasionally**),
- the specific purpose(s) of the processing,
- the recipients or categories of recipients of their personal data,
- the period that their personal data will be stored,
- whether the personal data will be transferred outside of the European Union,
- their data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing).

Additionally, per the GDPR, it is not enough to simply provide some information about the processing of personal data, therefore we recommend that the information that the project does choose to provide is also: 1) concise, transparent, intelligible and easily accessible; 2) written in clear and plain language, particularly if addressed to a child; and 3) free of charge.

When it comes to the cookie policy, the project should provide all the relevant information regarding the type of cookies used by the Website (i.e., browsing cookies, analytics cookies, function cookies or profiling cookies), including whether these are third-party cookies, meaning that they are from websites and web servers other than the Website, which is owned by a third party. If such third-party profiling cookies are used, then a cookie pop-up banner should be added at the top or bottom of the website, in order to inform the data subjects. Lastly, in the Privacy Policy, it should be clear to the data subject how they may block or delete the cookies used on the Website.

A negative answer would result to the following recommendation.

It is very unlikely that the project website does not gather any personal data. According to the GDPR, personal data means any information relating to an **identified or identifiable natural person**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. If the Website gathers IP addresses, then this is considered to be personal data. We recommend that the relevant information included in the Privacy and Cookie Policy will depend on what type of personal data you gather, and the kind of cookies are implemented on your website.

The most valuable information that should be communicated to the data subject includes:

- the kind of personal data that is collected and processed
- the identity and contact details of the project (as a data controller),
- the contact details of your data protection officer (if you process personal data **occasionally**),
- the specific purpose(s) of the processing,
- the recipients or categories of recipients of their personal data,
- the period that their personal data will be stored,
- whether the personal data will be transferred outside of the European Union,
- their data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing).

Additionally, per the GDPR, it is not enough to simply provide some information about the processing of personal data, therefore it is recommended that the information that the project chooses to provide is also: 1) concise, transparent, intelligible and easily accessible; 2) written in clear and plain language, particularly if addressed to a child; and 3) free of charge.

When it comes to the cookie policy, the project should provide all the relevant information regarding the type of cookies used by the Website (i.e., browsing cookies, analytics cookies, function cookies or profiling cookies), including whether these are third-party cookies, meaning that they are from websites and web servers other than the Website, which is owned by a third party. If such third-party profiling cookies are used, then a cookie pop-up banner should be added at the top or bottom of the website, in order to inform the data subjects. Lastly, in the Privacy Policy, it should be clear to the data subject how they may block or delete the cookies used on the Website.

4) Does your project have a newsletter?

A positive answer would result to the following recommendation.

The most important factor to consider is how can a data subject subscribe to the newsletter. The first and most foremost recommendation is to ensure that if a data subject may register for the newsletter, then according to the principle of data protection by default, the data subjects should be protected **by default**; which in the case of the check-boxes is to not have them pre-checked but allow for the data subject to consent to the subscription of the newsletter themselves. The second recommendation is to not add data subjects to the newsletter's mailing lists if they have not consented to it, or if they have not come into contact with the

project whatsoever." Additionally, the indication of the privacy policy should be made - where it will be clearly explained how data will be processed in the context of the newsletter. Lastly, the footer of the newsletter should also be mentioned that the data subject can oppose to the newsletter anytime.

5) Does your project involve the implementation of any tool (software, application, etc.) that could process personal data and how?

A positive answer would result to the following recommendation.

If the project involves or plans to implement a tool to process personal data, then there is an important starting point to any processing of personal data that should be in mind throughout the whole implementation process. That is the principle of data protection by design and by default, which has two sections: firstly, that data protection issues should be part of the design and implementation of such tools, and secondly, that data protection is an essential component of the core functionality of the tool and automatically implemented within the tools.

6) Does your project offer essential services (public or private entity in energy, transport, health, banking, etc.) or digital service?

A positive answer would result to the following recommendation.

Essential services consist of any public or private entity that offers services in the energy, transport, banking, financial market infrastructures, health, drinking water supply distribution, or digital infrastructure.[120] In addition to these sectors, the essential service needs to be relying on network and information systems. Additionally, it is important to note that digital services are also included in the requirements of the Network and Information Security Directive (so-called NIS Directive). Digital Services, for the purpose of this legislation, are defined as "any Information Society service, provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

Unlike the GDPR, which is a regulation, the NIS Directive is a different instrument, a Directive - which requires the Member States to implement it in their national legislation and through national strategies. For this reason, it is important that the project is aware of the fact that the individual Member States must identify the specific operators of essential services within their region – this means that the project must keep an eye out to this portal, which has been created by the European Commission, in order to track the transposition of the NIS Directive of Member States.

If the project falls under the two categories mentioned above (essential services or digital services), then it will most likely be within the NIS Directive. The NIS Directive enlists several responsibilities and requirements towards these two categories the most important of which are explained below.

[120] Annex II of the NIS Directive.

Operators of essential services must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their activities. Additionally, operators of essential services must take appropriate measures to prevent and minimize the impact of incidents, in order to ensure the continuity of services as much as possible. On the same note, they must notify, without undue delay, the competent authority of its member state or the computer incident response teams (CSIRTs) of incidents having a significant impact on the continuity of the services.

Due to the localisation of this Directive into national legislation, only minimal information can be recommended from the data protection perspective.

ANNEX D. SAMPLE OF SURVEY FOR R&I PROJECTS

SURVEY ON LEGAL COMPLIANCE TO THE GENERAL DATA PROTECTION REGULATION

2nd Concertation Meeting, 4th June 2019

Welcome to the Survey on Legal Compliance to the General Data Protection Regulation!

The aim of this survey is to collect relevant information, from European Projects of Research and Innovation (R&I) about their level of legal compliance, in light of the Regulation EU 2016/679 (the "GDPR").

As you may know, the Cyberwatching.eu project aims to contribute to a safer and more trusted Digital Single Market, by promoting the understanding of cutting-edge cybersecurity and privacy services, which emerge from R&I initiatives. The role of the R&I Projects is very important in this effort. On one hand, by submitting to the Cyberwatching.eu Catalogue of Services (you can find the full list of the Services at https://cyberwatching.eu/services/catalogue-of-services), R&I Projects get to communicate their objectives and disseminate their results to a broader audience. On the other hand, since R&I projects are likely process personal data, it is paramount that these processing activities carried out are compliant with the Data Protection Laws; more precisely with the GDPR. The GDPR is directly applicable in all the European Member States since the 25th of May 2018. The GDPR is the most recent European Legislation on Data Protection, updating and harmonizing the various legal frameworks existing around the EU.

The GDPR applies to organizations:

- established in the European Union, that process personal data (information related to individuals, e.g., names, surnames, email addresses, physical addresses, telephone numbers, bank account details, and also – as consistently maintained by Supervisory Authorities and relevant Courts - IP addresses, MAC addresses, etc.).

- NOT established in the European Union, that that process personal data of individuals, who are in the European Union, in the context of

(a) the offering of goods or services, irrespective of whether a payment is required; or

(b) the monitoring of the behaviour of such individuals as far as their behaviour takes place within the European Union.

Your contribution to this survey is necessary as your feedback will help us analyse the EU Cybersecurity & Privacy framework, also with reference to the R&I Projects. The objective is to provide recommendations to R&I Projects in order to support them in addressing compliance with the GDPR.

A public deliverable containing the results of this survey will be published in 2019. By participating to this survey, you will be able to obtain early access to the recommendations that will be given to projects in the context of the deliverable (D3.4).

Name: _____

R&I Project name: _____

Contact information (preferrably e-mail): _____

Having read and understood the privacy policy below, I hereby

- ❑ **agree**
- ❑ **do not agree**

to the processing of my personal data for the purpose of receiving recommendations on the compliance of the GDPR for Research & Innovation Projects.

_____

Signature

Information notice

Data Controller. *The Cyberwatching.eu Consortium, coordinated by Trust-IT Services Limited (hereinafter, "Trust-IT"), established in Chase Side 42 Chase Green House, Enfield, EN2 6NF, United Kingdom, which is the legal representative of the Cyberwatching.eu Consortium is also the data controller for the project related activities.*

Purposes of the processing and legal basis. *Your data is collected only for the purpose of providing you with customised and specific recommendations for your compliance to the General Data Protection Regulation (GDPR). The legal basis for this processing is your explicit consent, which will be rendered at the end of this form. You can withdraw your consent by contacting the data controller, as described below under Exercise of your data protection rights.*

Recipients of your data. *We may share your data with the following entities:*
Affiliates and Partners. We may share your data with any partner to the Consortium, as well as with its affiliates-companies that control, are controlled by, or are under common control with any of the Consortium's Members. These entities may receive your information only to the extent necessary for the proper execution of the research activities, or for the administration of the project. Users' personal data will neither be communicated nor anyhow processed for marketing or profiling related purposes.
Data Processors. We may share your data with partners providing technological services, which were formally bound by means of a data processing agreement, pursuant to article 28 of the Regulation (EU) 2016/679.
Persons in charge of data processing activities. We may share your data with persons authorised and instructed by the data controller to data processing activities. Precise instructions were given to them, pursuant to Article 29 of the Regulation (EU) 2016/679.

Period of storage. *Your personal data will be kept for no longer than is necessary for the specific purpose for which the personal data are processed. More precisely, personal data is kept as long as follow-up actions to the cyberwatching.eu deliverable (D3.4.) are necessary with regard to the purpose of the processing of personal data.*

Exercise of users' data protection rights. *You may contact us, via email at **info@cyberwatching.eu**, in order to assert your rights, as described in Articles 15 to 22 of the Regulation (EU) 2016/679, namely to demand: the confirmation of the existence of data concerning yourself and their origin and processing and the purposes thereof; the erasure (Article 17) or the rectification of data (Article 16); the restriction of processing (Article 18); the right to object (Article 22) and the right to data portability (Article 20).*
We inform you that you have the right to lodge a complaint to the competent data protection authority, pursuant to Article 77 of the Regulation (EU) 2016/679, if you believe that your personal data have been processed in violation of any applicable law concerning data protection.

SURVEY ON LEGAL COMPLIANCE TO THE GENERAL DATA PROTECTION REGULATION

The definitions of the words deemed in red can be found at a short glossary at the end of the Survey.

Country: _____

Select your geographical scope of operations:

- ❑ EU organization operating only in its country
- ❑ EU organization operating across EU globally (two or more EU countries)
- ❑ Organization from an associated country (Israel, Turkey, etc.) operating in EU
- ❑ Non-EU organization operating in EU

Website: _____

1. Does your project involve the processing[1] of personal data[2] of individuals?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

If the answer is **yes,** please answer 1A, 1B, 1C, 1D and 1E**:**

1 A. Does your project respect the general personal data protection principles (lawfulness, purpose limitation, transparency, fairness, data accuracy and minimization, safety, data protection by design and by default)?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

1 B. Was information[3] provided to data subjects (see Articles 12, 13 and 14 GDPR) and their consent[4] collected (or based on another legal basis) prior to data processing?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

1 C. How did you ensure data subjects' rights (such as right to access, to rectification, to erasure, to restriction of processing, to data portability[5], to object and to not be subject to a decision based solely on automated processing[6])?

_____
_____
_____
_____

1 D. Does your project involve the processing of special categories of personal data[7] (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or judicial data[8] (such as personal data relating to criminal convictions and offences)?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

1 E. Does your project involve decisions based solely on automated processing, including profiling[9]?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

2) On the official website of your project is there a registration form?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

3) On the official website of your project, is there Privacy and Cookie Policy?

- ❑ Yes
- ❑ No

Additional Notes:

_____
_____
_____

4) Does your project have a newsletter?

❑ Yes
❑ No

Additional Notes:

_____
_____
_____

5) Does your project involve the implementation of any tool (software, application, etc.) that could process personal data and how?

❑ Yes (Please, give us information about the tool in the notes below)
❑ No

Additional Notes:

_____
_____
_____
_____

6) Does your project offer essential services (public or private entity in energy, transport, health, banking, etc.) or digital service?

❑ Yes (Please, specify essential services offered in the notes below)
❑ No

Additional Notes:

_____
_____
_____

GLOSSARY:

[1] **Processing**: Pursuant to Article 4(2) GDPR, 'processing' means *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[2] **Personal data**: Pursuant to Article 4(2) GDPR, 'personal data' means *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

[3] **Information**: The Articles 12, 13 and 14 GDPR set out the information that controllers should supply and when individuals should be informed.

The information to supply is determined by whether or not the personal data were obtained directly from individuals or not.

The information supplied about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The information should at least include:

- the identity and contact details of your entity (as a data controller)
- the contact details of your data protection officer (in case a DPO has been designated)
- the specific **purposes** of the processing
- the **recipients** or categories of recipients of their personal data
- the **period** that their personal data will be stored
- whether the personal data will be transferred outside of the European Union
- the data subject rights (right to access to and rectification or erasure of their personal data, or the right of restriction of processing or right to object to the processing).
- The source from which the personal data originates (in case the data was not obtained from the data subjects).

[4] **Consent**: Pursuant to art. 4(11) GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For more information on the conditions for consent see Article 7 GDPR.

[5] **Right to data portability**: The data subject shall have the right to receive his/her personal data, which he or she has provided to a controller, in a **structured, commonly used and machine-readable format** and have the right to transmit those data to another.

[6] **Automated individual decision-making, including profiling**: The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

[7] **Processing of special categories of personal data**: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[8] **Processing of personal data relating to criminal convictions and offences**: Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[9] **Profiling**: Pursuant to art. 4(4), 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.

ANNEX E. FUTURE CHALLENGES FOR CYBER SECURITY SKILLS AND TRAINING FOR SMES

- ICT skills gap now shrinking (almost 1 mln experts missing), fast growing need for cybersecurity professionals (professionals needed not only in ICT industry but in all vertical sectors)
- Lack of low to middle level of cybersecurity skills by most mid-level managers in various industries
- lack of resources in SMEs (especially micro companies) to hire consultants/professionals, thus skills have to be developed in-house but there are many barriers for this (not enough education since school level, still low awareness, not enough knowledge who to train what, etc).
- growing difficulties for SMEs to understand what they need – more and more various trainings, tools and other services offered, but SMEs don't understand what they need.
- Lack of common language – different skills obtained through very different education programmes and paths, are often called different names.

ANNEX F. PROJECTS' PRESENTATION AT BREAK-OUT SESSION ON: STANDARDS AND CERTIFICATION FOR CYBERSECURITY

Four projects were presented, as follows:

- EUSEC
- Specialprivacy
- CANVAS
- Impact

(a) EUSEC project

The **EUSEC project** "EU Security Certification" was presented by the representative of Fraunhofer FOKUS. A summary of this project as taken from the web site: https://www.sec-cert.eu/ is given below:

> *"The EU-SEC Project aims to create a framework, under which accepted and recognised certification and assurance approaches can co-exist. The framework will be trustworthy as it is open to stakeholders by providing transparent governance processes. These drive and support the continuous development of the mutual recognition between different certification schemes. Furthermore, the governance processes provide a reference architecture including a set of tools which enable for the contribution to the international standardisation of compliance initiatives."*

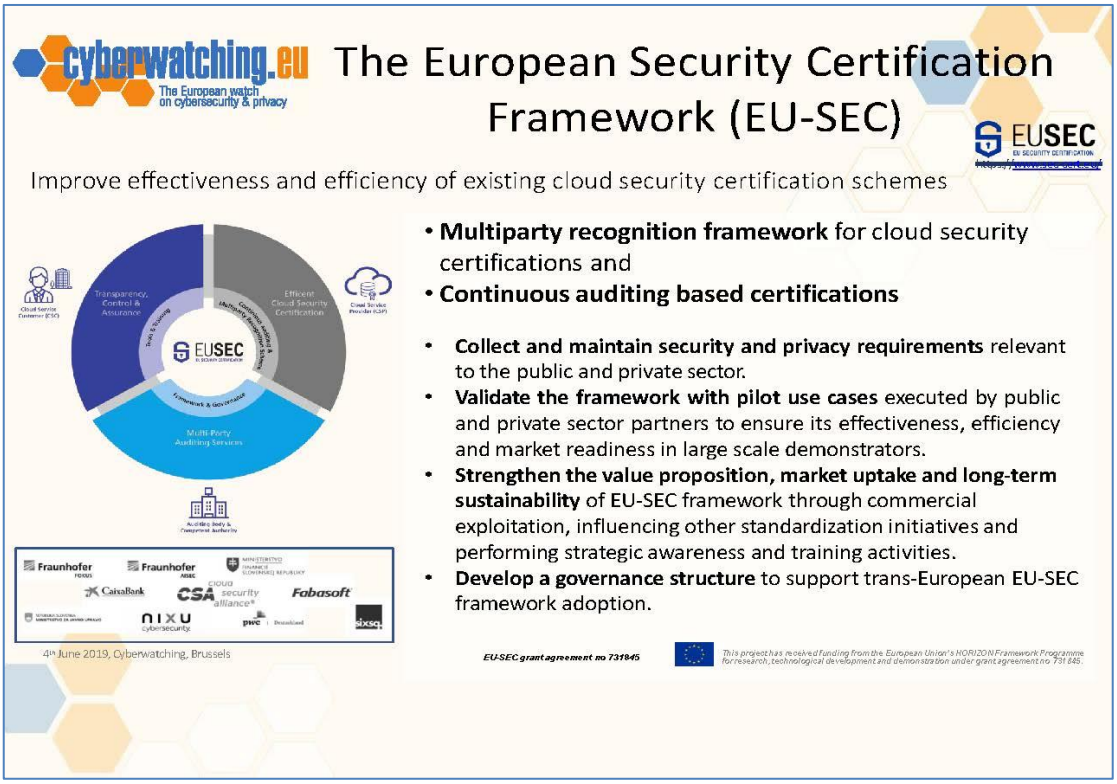


Figure 3: Summary presentation of EUSEC project

EUSEC project highlighted outputs:

EUSEC described its two main innovations :

- Multiparty recognition framework https://www.sec-cert.eu/eu-sec/Multi-Party_Recognition_Framework

- Continuous auditing based certifications
  https://www.sec-cert.eu/eu-sec/Continuous_Auditing_Certification

There was keen interest in the above two innovations and many questions followed concerning these innovative tools.

(b) Specialprivacy project

The **Specialprivacy project** was presented by the representative of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). A summary of this project as taken from the web site: https://www.specialprivacy.eu/ is given below:

> "*The **SPECIAL** project (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance) addresses the contradiction between Big Data innovation and data protection compliance requirements by proposing a technical solution that makes the achievement of both of these goals realistic. SPECIAL allows citizens and organisations to share more data, while guaranteeing compliance with data protection, thus enabling both trust and the creation of valuable new insights from shared data.*"

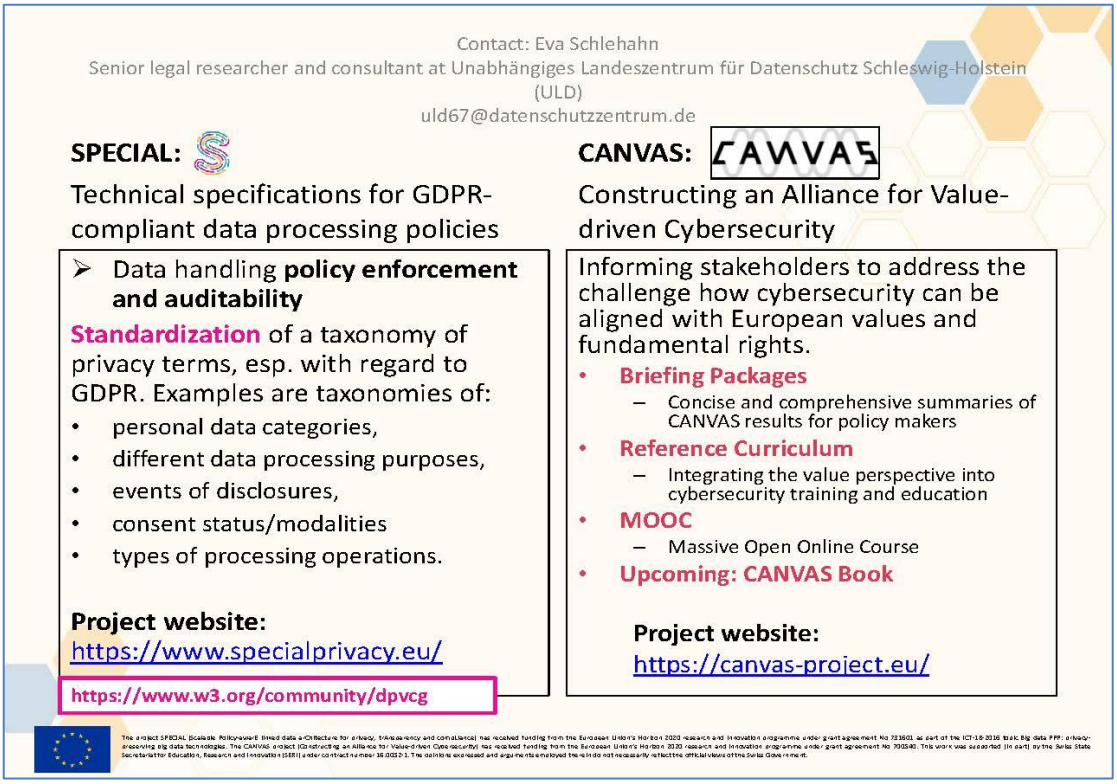


Figure 4: Summary presentation of Specialprivacy and CANVAS projects

Specialprivacy project highlighted outputs:

Engagement with W3C Community group on data privacy controls and vocabularies

(c) CANVAS project

The **CANVAS project** was also presented by the representative of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). A summary of this project as taken from the web site: https://canvas-project.eu/ is given below:

> "*The growing complexity of the digital ecosystem in combination with increasing global risks entail the danger that enforcing cybersecurity may bypass other fundamental values like equality, fairness or privacy, whereas downplaying cybersecurity would undermine citizens' trust and confidence in the digital infrastructure. For tackling this challenge, the European Commission has chosen the CANVAS Consortium – Constructing an Alliance for Value-driven Cybersecurity – to unify technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. Within three years, CANVAS aims to bring together stakeholders from key areas of the European Digital Agenda – the health system, business/finance, and law enforcement/national security – for discussing challenges and solutions when aligning cybersecurity with ethics. A special focus of CANVAS is on raising awareness on the ethics of cybersecurity through teaching in academia and industry*."

CANVAS project outputs:

- Policy output in terms of briefing packages
- Reference curriculum
- MOOC
- Upcoming CANVAS Book

(c) IMPACT project

The **IMPACT project** was presented by the representative of CISPA Helmholtz**.** A summary of this project as taken from the web site: http://impacteurope.eu/ is given below:

> *"IMPACT Europe is developing an evaluation toolkit that draws on a state-of-the-art knowledge database on radicalisation factors, existing counter violent radicalisation interventions, and approaches to evaluating these interventions. Making the database easily accessible to a wide range of public and voluntary sector users, the toolkit is ultimately geared at encouraging practitioners to properly evaluate their counter violent radicalisation activities and to build good practices into the design of any future interventions."*

Figure 5: Summary presentation of imPACT project

imPACT project outputs:

- Attaining privacy in tomorrow's internet, e.g. social networks, forums, search engines.

ANNEX G. CHALLENGES AND PRIORITIES IN STANDARDISATION AND CERTIFICATION IN CYBERSECURITY

During this interactive breakout session, the following areas were identified as areas with real challenges in cybersecurity:

- **Harmonization and certification** between member states remains a huge issue. Reference was made to the cyberwatching.eu deliverable (distributed as a white paper at this event) in which a gaps analysis on standards and certification has been performed[121].
- **Single and coordinated understanding of what cybersecurity means for Europe.** It was pointed out that significant work has already been accomplished in H2020 in building a cybersecurity atlas, and a taxonomy was developed by JRC for this purpose.
- **Affordability of cybersecurity for SMEs** remains an evergreen. It is hard to compete with large companies where the cost of cybersecurity is not an issue.
- Reporting vulnerability threats in a coordinated and standardized manner was difficult
- **Relationship of cyber security and data protection and privacy** presents some issues. There are some conflicts in perspectives in legal requirements. A privacy scheme needs to be identified under the certification framework.
- In order to gain momentum, funding and reporting should occur right across member States. When there is more **focus and funding,** then, things move quickly.
- **Affordable base line security certification** is lacking
- **Enforcing base line security in software** is challenging because there is a notion of "Duty of care" which some software providers may not have
- **In IoT, there is a huge absence of baseline security** and it is the fastest growing area of things connecting the Internet
- **Accreditation of certification schemes (which is in the GDPR)** – needs to be recognized by the EU Data Protection Board. For international clients, there is a need to speed up on this initiative, and make it known what the criteria will be for these data protection schemes (internationally). Accredit those organisations which provide the certification. One of the schemes moving in that direction is the Common Criteria
- **Free flow of non-personal data is a regulation** entered into force last week (related to cloud) and how does compliance fit in.

[121] https://www.cyberwatching.eu/d33-white-paper-cybersecurity-standard-gap-analysis

ANNEX H. THE CHALLENGES AND HOW R&I CAN IMPROVE THE WAY THAT THEY PREPARE FOR THE MARKET

Challenges:

- How can Cyberwatching help in communicating project advances in MTRL status?
- How can we improve the MTRL questionnaire to better identify the MTRL status, and what could we do for attracting projects to update their MTRL status periodically (through a webform)?
- How could we implement a correction factor to assign the proper color code based on the type of project (IA, RIA, CSA, etc.)? What particularities could affect the MTRL status and how could this be estimated?

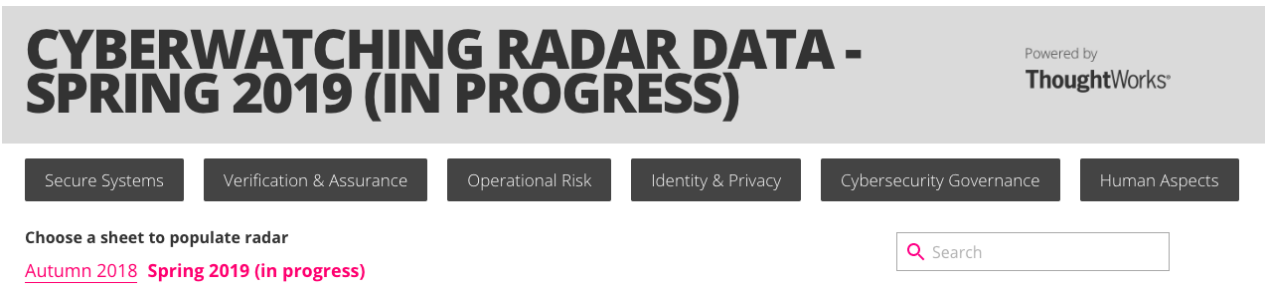
In order to assess how close the R&D projects are to the market, cyberwatching.eu sent the MTRL questionnaires to more than a hundred European projects, gathering 32 answers to date. Three of the projects are out of the scope for the Technology Radar, since they are using cybersecurity and privacy, but they are not really creating new tools or services. That makes a sum of 29 projects to analyse, all of them currently ongoing.

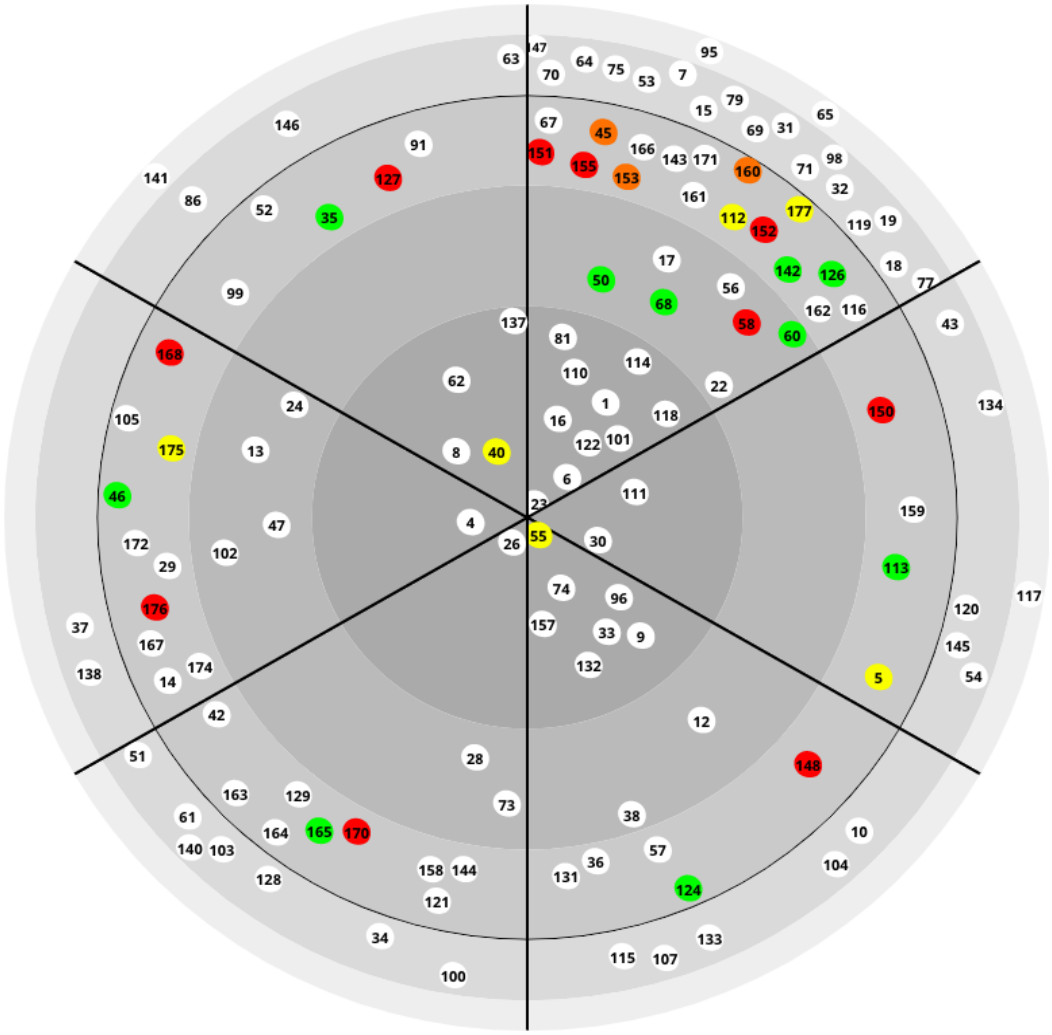
The next tables show a brief summary of the TRL and MRL scores for each category of cyberwatching.eu taxonomy L1:

	N. pr.	TRL avg	MRL avg
Apps & user-oriented services	17	3	3
Governance, Ethics, Trust	7	4	4
Found. of tech & risk management	5	5	4

	TRL 0-3 Idea	TRL 4-5 Prototype	TRL 6-7 Validation	TRL 8-9 Production
N. projects	15	5	8	1
	MRL 0-3 Ideation	MRL 4-5 Testing	MRL 6-7 Traction	MRL 8-9 Scaling
N. projects	16	11	2	0

Taking this into the Technology Radar and factorizing each MTRL score according to projects in the same ring (duration of the project) and segment (subdomain of cyberwatching.eu taxonomy), we get this Radar Data Status, that will be soon reflected in cyberwatching.eu site.




147
63
64
95
70
75
53
7
79
15
65
69
31
67
45
146
91
166
143
171
98
151
155
153
160
71
141
127
161
32
86
52
35
112
177
119
19
152
17
18
99
50
142
126
77
56
68
162
116
137
58
60
43
81
168
110
114
62
22
24
1
134
105
16
118
150
175
13
8
40
122
101
6
46
111
23
159
4
47
55
26
30
172
102
113
29
74
96
117
176
157
33
120
37
9
167
132
145
138
174
5
54
14
42
12
51
28
148
163
129
73
38
61
164
165
170
10
140
103
57
36
104
158
144
131
128
124
121
34
133
115
107
100

ANNEX I. GLOSSARY

Term	Explanation
AI	Artificial intelligence
DEP	Digital Europe Programme
DPIA	Data Protection Impact Assessment
DSP	Digital Service Providers
EDPB	European Data Protection Board
EPBS	European Data Protection Supervisor
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
IoT	Internet of Things
NIS	The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016*
OES	Operators of Essential Services
R&I	Research and Innovation Projects, consisting of the European Projects
WP29	Former Article 29 Working Party, now the European Data Protection Board