cyberwatching.eu

The European watch
on cybersecurity & privacy

2nd cyberwatching.eu
Concertation Meeting report

Disclaimer

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.

2nd cyberwatching.eu Concertation meeting

The 2nd Cyber Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy" saw over 60 representatives from all projects in the unit 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.

1. 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.

1.1. 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 following challenges for the future of cybersecurity skills and training for SMEs were identified:

- 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.

These challenges 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.

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

- **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 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.

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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

1.3. 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 of cyberwatching.eu D3.4 EU Cybersecurity legal and policy aspects: preliminary recommendations and road ahead. 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

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

2. 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.

2.1. 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.

2.1.1. 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.

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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 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 andthe 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[1] 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**

[1] For more details see: https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018- digital-transformation_en.pdf

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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[2].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, theneed 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

[2] Art. 9(4) GDPR.

Cyberwatching.eu has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 740129.

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[3].

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.

[3] 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.

Cyberwatching.eu has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 740129.

2.1.2. 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[4], 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.

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

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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 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.

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

2.2. 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

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

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

2.3. International cooperation priorities

Facilitators: Yolanda Ursa, 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

2.4. 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;

Cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.

- 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.

2.5. 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 and market readiness level analysis (see cyberwatching.eu 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.
Discussion led to the following recommendations 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.

Cyberwatching.eu has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 740129.

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

UNIVERSITY OF OXFORD

ICT LEGAL CONSULTING
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY
360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Third party

CITIC
Centro Andaluz de Innovación y Tecnologías de la Información y las Comunicaciones

www.cyberwatching.eu

@cyberwatchingeu

/in/cyber-watching/

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.