Data protection and cybersecurity compliance in Emerging Technologies

Insights and recommendations from Cyberwatching.eu

2021

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

aeicibersegurridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Table of content

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 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.

1 Introduction

Cybersecurity services increasingly rely on the use of emerging technologies, such as AI and IoT. However, **new EU legislation** often comes with a challenging implementation period, during which **European Member States** must, efficiently and coherently, **adapt their national laws** to the requirements of the new piece of EU legislation.[1] An example of such a challenge and changing environment is related to the difficulties of the COVID contact tracing apps to comply with the GDPR.

Due to this acknowledged challenge, EU institutions and agencies have looked into **how these difficulties can be overcome**. One example is through enforcement: consider the designated national authorities responsible for enforcing the terms of the GDPR[2] and the Directive on Network and Information Security (NIS-D).[3] However, both the GDPR and NIS-D provide additional challenges which are inherent to their domains of regulation, in particular where they are considered as applicable to **innovative fields of technology, such as Emerging Technologies** – the complexities and intrusive nature (in terms of personal data collection and further processing) of AI and IoT-based products and services **create theoretical and practical issues when looking to enforce the obligations of the GDPR or NIS-D** against technology service developers/providers and users.

Since the GDPR and NIS-D have different scopes,[4] the concerns raised when they are considered vis-à-vis the Emerging Technologies are also different. Generally speaking, the main concerns related to the GDPR revolve around understanding **which GDPR obligations are relevant to developers/providers and users of Emerging Technologies**, and which need to be adapted so that they can remain relevant, and whether any conflicts so intensely with the particularities of the Emerging Technologies that they cannot regulate their use to any degree of usefulness. In contrast, the main concerns related to the NIS-D lie in the **implications around injecting Emerging Technologies into the operations of the Operators of Essential Services (OESs) and Digital Service Providers (DSPs)**, and to what extent this can be done without sacrificing security, usability and traceability of networks and information systems.

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

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

[3] Art. 8 NIS-D.

[4] See Section **Error! Reference source not found.** and Section **Error! Reference source not found.**,available at: https://cyberwatching.eu/sites/default/files/D3.5_Risk_and_Recommendations_on_Cybersecurity_Services_v1.0_Final.pdf

2 Ethics and Trustworthy AI

One particular problem raised by Emerging Technologies, which seemingly cannot be offset by way of current regulations alone, is seen in its relationship with **transparency and ethics**. Consolidating this connection, in 2019, the European Commission High-Level Expert Group on AI (AI HLEG) published their "**Ethics guidelines for trustworthy AI"** that would aid in the development of trustworthy AI in the European context. [5] In addition, a practical tool has been developed by the Commission in July 2020, with the aim of supporting and revising the guidelines.[6]

According to the AI HLEG, 'Trustworthy AI' is comprised of **three major elements** which should "*be met throughout the system's entire life cycle*:

1. *it should be **lawful**, complying with all applicable laws and regulations;*
2. *it should be **ethical**, ensuring adherence to ethical principles and values; and*
3. *it should be **robust**, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm*."[7]

The AI HLEG Guidelines provide with a useful framework, based on **seven requirements** for artificial intelligence in order for it to be considered **to be trustworthy**.[8] Trustworthiness can be seen as a necessary prerequisite for the ultimate success of the Emerging Technologies as, in absence of trust, the Emerging Technologies may not see widespread use.
These requirements include

1. the involvement of human agency and oversight, calling for AI to empower individuals and promote their fundamental rights;
2. technical robustness and safety, ensuring that AI is both secure and resilient;
3. privacy and data governance, guaranteeing compliance with law and also fostering acceptable data governance mechanisms;
4. transparency, with respect to the data used, the system itself and the actual business model of the AI;
5. diversity, non-discrimination and fairness, circumventing bias and promoting diversity;
6. societal and environmental well-being which calls for AI to positively contribute to society; and finally,
7. accountability, which calls for the implementation of mechanisms that ensure AI systems are accountable and responsible.

On 17 July 2020, AI HLEG published "The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment"[9], which is a tool that supports the afore-mentioned "Ethics Guidelines for Trustworthy Artificial Intelligence" (AI) and the seven key requirements of trustworthy AI). Through an accessible and dynamic checklist provided in this web-based tool[10], businesses and organizations, developers and deployers of AI, can self-assess through concrete steps their systems under development, in order to ensure that their users can benefit from AI without being exposed to unnecessary risks.

[5] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[6] European Commission, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment, 17 July 2020, available at: https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.
[7] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), p. 5, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[8] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for a trustworthy AI* (8 April 2019), pp. 14-20, available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[9] *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* available at https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment
[10] Web-based self-assessment AI tool available at https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence

3 Risk Assessment for Emerging Technologies

The public sector outside of Europe, as exemplified by the Canadian Government, has also made efforts in order to provide a solution to the difficult nature of carrying out risk assessments on Emerging Technologies, through the development of an **Algorithmic Impact Assessment (AIA)**.[11] The AIA was designed in order to assess and manage risks related to **automated decision-making**, and was born from the Canadian Directive on Automated Decision-making, aiming to "*ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian law*".[12]
In this way, the Canadian Government has demonstrated its commitment to the principles of "*transparency, accountability, legality, and procedural fairness*", [13] principles which are also enshrined in European legislation.

Another kind of risk assessment that could be developed and carried out by market operators is one that specifically takes into consideration the rights of individuals, potentially inspired by the already-used fundamental rights impact assessment. The **fundamental rights impact assessment** is a product of the **Charter of Fundamental Rights of the European Union's implementation**, and their relative Operational Guidance was adopted by the European Commission in 2010.[14] It provides an assessment method that allows for the analysis of the influence a specific policy may have on the fundamental rights of EU citizens, thereby seeking to ensure the compliance of that policy with the Charter.[15] The development of a risk assessment framework for industry that is based on the EU's fundamental rights risk assessment, taking into consideration the real and potential risks to the rights and freedoms of individuals that are implicated in AI systems, could help mitigate such risks and ensure the development of transparent and ethical Emerging Technologies.

The **EDPB** has also issued **relevant Guidelines** on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data[16] and a toolkit,[17] from which inspiration could also be taken for the development of an **Emerging Technologies risk assessment** (as well as the ALTAI tool as described above). This assessment could evaluate both necessity, through the identification of the fundamental rights and freedoms potentially impacted, looking clearly at the objectives of the system and the relevant interests behind it, and ensuring that the system is the least intrusive in order to avoid negatively affecting rights and freedoms; and proportionality, insofar as a balancing test should be carried out, ensuring that the results of the system are actually in line with its objectives, that the data processing is evaluated in terms of scope,

[11] Government of Canada, *Algorithmic Impact Assessment (AIA)*, available at: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html.

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

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

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

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

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

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

extent and intensity, and that adequate safeguards are in place to improve proportionality if needed.[18]

4 Related Cyberwatching.eu Publications

- Emerging technologies in the age of GDPR – Findings & recommendations from EU & R&I projects[19]
- Decentralized operation and security in the IoT Space[20]
- Cybersecurity risk management: How to strengthen resilience and adapt in 2021[21]

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

[19] https://cyberwatching.eu/publications/emerging-technologies-age-gdpr-%E2%80%93-findings-recommendations-eu-ri-projects

[20] https://cyberwatching.eu/publications/decentralized-operation-and-security-iot-space

[21] https://cyberwatching.eu/publications/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021

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