Future PolicyShapers Programme • Vienna – Working Paper

Disclaimer: This is not an official document. This document was a product from the discussions among the participants of the training "Future PolicyShapers Programme" which was organized in Vienna, Austria by the European Multidisciplinary Organization for Training and international Consulting, with the support of the European Youth Foundation of the Council of Europe. The aim of this training program was teaching the participants about policymaking tools and instruments and putting these into practice through simulating a not-existing committee that resembles a European democratic institution.

Committee: *European States' Committee on Citizens' Rights*

Topic: *The Right to Privacy and Cybersecurity in the Digital Age and in Times of Crises*

The European States' Committee on Citizens' Rights,

Recalling the *Universal Declaration of Human Rights* (UDHR), the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, the *Council of European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention no. 108), the *EU Charter of Fundamental Rights*, the *General Data Protection Regulation* (GDPR) (Regulation 2016/678) and other prior EU regulations and directives concerning cybersecurity and the protection of privacy,

Profoundly concerned about the massive collection of data having a negative impact on human rights, especially on privacy and cybersecurity,

Considering that Member States present in this committee are dedicated and willing to protect the right to privacy to a full extent,

Desiring a strong, resilient and sustainable cybersecurity framework for all critical infrastructure, including energy, government bodies and health providers,

Keeping in mind that all processing of data must comply with the below mentioned six general data quality principles: (i) processed fairly, lawfully and transparently; (ii) collected for specific, explicit and legitimate purposes and not processed in a manner incompatible with those purposes; (iii) adequate, relevant and not excessive; (iv) accurate and, where necessary, up to date; (v) kept in an identifiable form for no longer than necessary; and (vi) kept secure,

Looking forward to establishing the uniform European security requirements in order to prevent foreign attacks,

Recognizing the importance of performing the surveillance and collecting data by governments for a reasonable, exhaustive and legitimate aims or reasons,

Recognizes that the research and knowledge on addressing **systemic cyber-violence** need to be strengthened including cyber violence exacerbated by the pandemic, sexual extortion, and displaying child sexual exploitation and sexual abuse material as well as greater awareness of cyber safety and the different impact it has on men and women need to be included throughout educational and training programs,

Calling attention to a specific need for digital education and literacy,
Noting further the importance of digital transformation in the digital age,

1. *Urges* Member States to raise awareness for digital education through the means of:

a. Using digital transformation as a tool to achieve social change at scale;
b. Investing in Research and Development (R&D) by European institutions (ENISA, European Regional Development Fund) and national governments;
c. Encouraging equal allocation of resources towards knowledge exchange between the Member States;
d. Targeting specific campaigns to raise awareness about cyberthreats, attacks and encourage a responsible cyber culture throughout society;
e. Adopting programmes and courses about Artificial Intelligence (AI) to also include Psychology into their curriculums;
f. Encouraging bi-annual training/workshops for all private and public organizations' staff, with the completion of a test at the end;
g. Allowing the free movement of cybersecurity experts for advisory purposes;

2. *Encourages* Member States to integrate data security and cybersecurity into curriculums from elementary to high school and university educational programmes;

3. *Calls upon* the implementation of innovative university level courses on cybersecurity at universities based in the European Union (EU);

4. *Claims* additional creation of courses on cryptography for implementation of end-to-end encryption for public and private digital safety;

5. *Demands* the education of information communication technology (ICT) skills among adults that are non-technology users through the Ministry of Education;

6. *Further requests* corporations and organizations with more than 50 employees to appoint an employee responsible for ensuring the accordance of the corporation's or organization's compliance with the right to privacy and Data Regulation Acts;

7. *Draws attention to* monitoring the system annually through the Ministry of Education of each Member State in the form of a report to be submitted to the ENISA monitoring and evaluation portal;

8. *Recognizes* the role of ENISA and existing EU training bodies to organize trainings for administrative workers and employees at critical infrastructure units in cooperation with Member States;

9. *Proclaims* a general mechanism for funding based on the following principles:

a. The implementation of the bodies and mechanisms established by this document are funded by the Member States;
b. Based on the preliminary calculations of expected costs for those bodies and mechanisms, the costs will be allocated to the Member States according to their real GDP-per-capita and the number of ENISA-interventions in each State;
c. The funding proposal will be evaluated by external independent Consulting firms as well as the European Court of Auditors, according to the results the mechanism might be adjusted/changed;

10. *Confirms* an increase of funding of ENISA (EU Agency for cybersecurity), the body established for cooperation between national security agencies;

11. *Establishes* an intelligence sharing network of existing national intelligence agencies for real-time data sharing while evaluating and sharing their results on an annual basis to detect any suspicious actions by people/ groups by:

a. The creation of a cross-border digital office, the cooperation between national agencies will be enhanced to monitor and anticipate signals of attacks;
b. Learning from the experiences of other major security agencies;
c. Transparency among the member states, but confidentiality against other actors (in particular non-member states);

12. *Instructs* on main objectives when creating the stress-tests: exercises, where cybersecurity threats are simulated to prepare for future threats such as:

a. Regular cross-European joint exercises including several countries;
b. Cooperation with corporations, SMEs, organizations, governments and universities from these Member States;
c. Agreed upon frequency of tests as well as frequency of MS-participation in a given testing cycle;
d. Actions and results will be protocolled and have to be transparent and available to all MS;
e. Focus on evaluating the protection of critical infrastructure such as: hospitals, energy utilities; airports, public transport and ministries during the stress-tests;

13. *Resolves* to share recovery programmes from cyberattacks among Member States within the framework of ENISA;

14. *Recommends* sharing the knowledge of creating recovery programmes with non-EU Member States, especially developing countries;

15. *Recognizes* that national security agencies and ENISA have rights to access and retain in bulk data that was collected by private companies, in case national security is threatened;

16. *Requires* 24 hours real time monitoring and detecting of cyberattacks for critical infrastructure;

17. *Insists* on Member States to fine corporations, if they have breached the Data Protection Regulations;

18. *Notes with approval* that if Member State fails to fine corporations/companies for breaching the Data Protection Regulation, ENISA can sanction the MS up to the amount that would have been fined to the corporation;

19. *Decides* that the decisions of ENISA are:

a. Directly enforceable;
b. Via the executive bodies of each Member State, which are obliged to cooperate within their enforcement capacity;

c. Open to judicial review by the European Court of Justice;
d. Enforceable in a different Member State, in case that one Member State does not comply with the enforcement;

20. *Reiterates* that ENISA shall enforce the Common Security and Defence Policy (CSDP) by imposing economic sanctions upon non-EU countries and international organizations in case of data breach;

21. *Requests* that fines will be calculated based on the profit of the corporation within the last year, by:
a. A fixed fine at a minimum of 1% and a maximum 4% of the total worldwide annual turnover;
b. Relying on factors to establish the height of the fine such as:
i) Severity of the breach;
ii) Length of time of the breach;
iii) Intentionality of the breach;
iv) Degree of harm per individual;
v) Number of individuals harmed;

22. Proclaims that ENISA can impose fines on legal entities but not individuals;

23. *Authorizes* ENISA to multiply fines by two in case of repetition or ongoing breach within a time period of one month;

24. *Establishes* that fines by ENISA are not applicable to SMEs according to the EU definition;

25. *Further reminds* that the redistribution of the collected fines should be allocated as follows to:
a. investments in educational programmes and R&D;
b. compensating individuals for damages caused by a breach of data protection regulations, once awarded by a court;

26. *Endorses the call* to share best practices and struggles with cybersecurity and data security within ENISA;

27. *Solemnly affirms* that Member States are obliged to implement an independent board of experts with the following tasks:
a) to check whether applications that are based on artificial intelligence (AI) reinforces stereotypes and structural discrimination against minorities;
b) to check whether the application does not violate human rights;

28. *Reiterates its demand* for launching a platform through ENISA which allows for anonymous whistleblowers in regard to the right to privacy and cybersecurity in the digital age, where:
a. The identity of a whistleblower should be kept confidential for protection from unfair prosecution;
b. Any financial allocations to whistleblowers should be in accordance with Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons, who report breaches of Union law (“Whistleblower Directive”);

c. Financial allocations to whistleblowers serve the purpose of protecting the whistleblower against potential retaliation as well as avoiding a financial downside for the whistleblower (and family);
d. A legal team should be assigned to protect a whistleblower's rights;

29. *Fully supports* for the work of ENISA to be evaluated by the European Court of Auditors by sending regular reports, as well as by the European Parliament in the form of an annual formal presentation of all actions and projects;

30. *Establishes* an independent authority to be called Ombudsperson for transparent reporting;

31. *Requires* Member States to appoint an Ombudsperson for the duration of two years;

32. *Expresses its belief* that representation from each Member State will promote diversity and equal opportunity;

33. *Instructs* the independent authority to screen national and international corporations both in public and private sectors to prevent data breach cases;

34. *Urges* Member States to consider data neutrality when screening job applications:

a. All application related information should be stored in the internal storage of the company;
b. Applicants should be informed about collection of their data periodically;
c. Any further action taken by the company should be communicated to the applicant with no delays;

35. *Insists* Member States to contribute equally in financial terms covering the expenses to sustain this authority;

36. *Expresses its hope* that funding mechanisms will be efficient and transparent,

37. *Commits* to further engagements and actions for the topic of the right to privacy in the digital age and times of crises.