Resolution Nr. 7 adopted at the EPP Congress, Rotterdam (The Netherlands), 31st May – 1st June 2022

For a cyber-secure Europe

"Cybersecurity is the flip side of digitalisation, therefore just as much a priority for us" (President Ursula von der Leyen).

1. Acknowledging that digitalisation and technological penetration are essential to our economic and societal prosperity and will lead to many opportunities such as revolutionising healthcare, boosting productivity, and saving lives.

2. Recognising that increased digitalisation means increased cyber risk. The growing reliance of our societies, economies, and public administration at EU and national levels on digital technologies, while beneficial, has increased the risk of cyberattacks and hacks, targeting our democratic institutions, elections, legislative procedures, economic processes, personal devices, law enforcement and justice, and critical infrastructure such as power plants, ports, and healthcare facilities.

3. Recalling that the COVID19 crisis intensified this reliance on digital technologies and connectivity, further exposing our vulnerability to cyber risks.

4. Recalling that the recent attacks and leaks of data of crucial entities, including the European Medical Agency, and healthcare systems such as in Ireland, Finland, and France, have caused significant damage to healthcare systems and patient care.

5. Considering that according to the European Union Agency for Cybersecurity (ENISA), the number of significant, malicious attacks against critical sectors in 2020 has doubled those recorded in 2019. This includes a 47% rise in attacks on healthcare facilities and networks — a trend which was accelerated by the pandemic.

6. Noting that cybercrime and particularly ransomware have become a top security threat, leading to the loss and theft of sensitive data that would cause significant costs for companies, governments, and individuals.

7. Underlining that rampant cyber espionage jeopardises European trade secrets and our industry as a whole.

8. Highlighting the low cybersecurity awareness among individuals and businesses, which still lack the appropriate defences in place to prevent malicious network infiltration; the shortage of skilled workers in the cyber sector, and the uneven capabilities across Member States.

9. Reiterating that those who attack our critical infrastructure attack Europeans, the competitiveness of our industry, and our European way of life — our values of freedom, democracy, and the rule of law.

10. Convinced, as the EU and its allies recognised, that cybersecurity is a priority for the post-pandemic recovery, as we move towards an ever more digital society and economy.

11. Supporting the EU's vision of cyberspace grounded in the rule of law to bring social, economic, and political development globally in full respect of fundamental rights. The Internet should remain an open, neutral, free, secure, and resilient space.

12. Welcoming the broader set of policies, investments, and projects fostered by the European Commission, such as the EU's Cybersecurity Strategy for the Digital Decade, the Proposal for a Directive on the Resilience of Critical Entities, and the Digital Europe Programme.

13. Supporting the European Commission President's pledge to create a European Cyber Defence Policy, including legislation on common standards under the new European Cyber Resilience Act.

14. Recognising the evident shortcomings of EU existing frameworks such as the Directive on the Security of Network and Information Systems (NIS).

15. Highlighting that cyber security needs to be a fully integrated part of our global EU strategy with regard to security and defence, as outlined in the EU Strategic Compass for Security and Defence.

16. Welcoming the revision of NIS as a decisive step forward to enhance our cyber and economic resilience by achieving a high common level of cybersecurity across the EU, and a united and harmonized European response to cyber threats.

17. Convinced that a common governance framework, based on harmonised cyber security standards, priorities, requirements and objectives across EU Member States is essential to ensure regular exchange at a high political level between EU bodies and Member States.

18. Looking forward to the forthcoming European Cyber Resilience Act, a regulation on measures for a high common level of cybersecurity for the Union institutions, Bodies and Agencies, which will mirror the level of ambition for Member States public administrations in the NIS2 directive and strengthen the cyber resilience of all EU-level administrations.

19. Supporting the Commission's policy objectives in the fields of cybersecurity and technological sovereignty, including investments of more than €1 billion, and the improvement of cooperation between EU and state institutions.

20. Supporting the European Parliament's June 2021 resolution on the EU's Cybersecurity Strategy for the Digital Decade, which called for enhanced cybersecurity standards for interconnected devices, operating systems and critical infrastructure.

21. Reaffirming its commitment to the OSCE's Resolution on Cyber Security in the 2013 Istanbul Declaration.

22. Supporting the 2018 Paris Call for Trust and Security in Cyberspace, as a significant and innovative step to bring together the international community - from governments, international organisations, civil society organisations, and the private sector - around 9 core cybersecurity principles to preserve a peaceful, open, and stable cyberspace.

23. Convinced that the Paris Call is an opportunity to create an international system of a collective international cyber security which can be the only guarantee of a sustainable digital peace.

24. Welcoming the more prominent role given to The European Union Agency for Cybersecurity (ENISA) through the Cybersecurity Act, in particular by helping the Member States to implement the European legal acts.

The European People's Party:

1. Urges the EU and Member States to adopt policies for the data economy that guarantee trust in products, applications, and infrastructure, and to develop a strong cybersecurity roadmap. We

want the digitisation of the economy and cybersecurity to go hand in hand. A data economy can only flourish when trust is guaranteed.

2. Calls for stronger cybersecurity protection and response mechanisms, as well as defence strategies, that factor in and keep pace with the growing concerns around cyber-insecurity and rapid digitalisation.

3. Believes that greater efforts are needed to develop more secure, future-proof, and reliable critical networks, information systems, services, and infrastructure across the EU.

4. Emphasises that cybersecurity is not only about the protection of personal data, but also about creating an environment that enables an efficient, safe, and undisrupted supply of services across all interactions between governments, businesses, and individuals.

5. Invites the EU and its Member States to strengthen the security of their common and respective critical infrastructures from repeated and increasingly sophisticated attacks, by ensuring each EU country has a digital security architecture that defends robustly against cyber-attacks.

6. Recommends effective monitoring and law enforcement to ensure that the privacy of citizens is not threatened.

7. Recommends all Internet-connected infrastructure and products in the EU be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.

8. Calls upon EU policymakers to ensure NIS2 rests on a consistent set of security requirements, to allow for its efficient implementation through national transpositions.

9. Stresses that it will be critical to ensure cybersecurity requirements are implemented across national laws in a way that avoids any ambiguity and any fragmentation of the Digital Single Market.

10. Calls upon EU policymakers to ensure NIS2 more efficiently establishes measures to achieve a common high level of security of networks and information systems in the EU to improve the functioning of the internal market.

11. Asks EU governments to work towards better coordination and greater sharing of best practices and information, given cybersecurity is a national competence, while providing a stronger role for ENISA.

12. Draws attention to the need to step up our efforts in terms of investments. Investments should target areas where the EU has a real added value in cybersecurity research and should boost the development of a European cybersecurity industry.

13. Recalls that the continuous battle against cybersecurity threats and cybercrime depends on stronger collective efforts through enhanced cooperation between public authorities and the private sector, which requires investing in technological innovation in a global context.

14. Recommends an EU agreement on cyber intelligence collaboration and collective response against cyber and hybrid attacks to ensure a coordinated prevention and response strategy.

15. Recommends a “whole-of-Europe” approach combining the efforts of cybersecurity experts and EU governments and encourages wider European and international cooperation with like-minded partners and relevant organisations such as NATO.

16. Calls upon Member States to pool their national cybersecurity powers more efficiently, including through rapid cyber response teams that can fight off hackers in real time.

17. Encourages the development of an EU-wide network of security operation centres, capable of detecting the signs of a cyberattack sufficiently early, thereby allowing pre-emptive action before damage is caused.

18. Welcomes the Commission’s newly proposed EU Joint Cyber Unit, which will be helpful in this respect.

19. Calls upon the EU to elevate investigations of ransomware attacks to a similar priority as terrorism. This can ensure necessary connections across global, European, and national cases and investigations, so as to develop a comprehensive picture of the economic security threats and enhance tracking within the EU. Authorities and agencies handling ransomware attacks would be able to share both updated case details and active technical information with each other. The EPP encourages such collaborations take place with like-minded allies and organisations like

NATO. Heightened reporting would help to deploy resources and identify common exploits used by cyber criminals more effectively.

20. Encourages the EU to continue to adopt a multistakeholder and consensus-based approach to addressing cybersecurity issues.

21. Encourages the EU to sustain its efforts to build stronger cyber diplomacy by establishing partnerships with like-minded countries on global digital governance and shared responses to cyberattacks.

22. Recommends, for instance, that ENISA deepens its work with the agencies of the EU's global, like-minded partners, such as the US National Institute of Standards and Technology (NIST), to establish appropriate standards, thereby ensuring that these can weigh in at the global level. Recommends governments seek to include academia and industry in this process.

23. Notes that the support of the Paris Call by all EU Member States has shown that a shared vision is within reach on how to protect the digital economy and society against cyber threats.

24. Asks signatories of the Paris Call to make some rapid operational progress to ensure their commitments do not remain purely incantatory.

25. Welcomes that the United States has joined the Paris Call, while expressing regret that China, India, Israel, North Korea, Russia, and Iran have not signed the text.

26. Encourages the EU to continue to engage in talks and deals with third countries to which cyber incidents were attributed, in order to tackle cyberespionage and cybertheft, and ensure that these counterparts abide by the terms of agreements.

27. Supports a stronger strategy to deter hostile actors and the consideration of diplomatic action or economic retaliation. The EU could enhance its cooperation with the United States, Japan, other OECD economies and NATO to apply political pressure. The EU should be increasingly firm towards states that fail to act to pursue cyber-criminal ransomware groups, or that enable and facilitate them.