European Parliament
2014 - 2019

Committee on the Internal Market and Consumer Protection

14/03/2018

AMENDMENTS: 42

Nicola Danti
Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Proposal for a regulation COM(2017)0477 - C8-0310/2017 – 2017/0225(COD)

Amendments created with

at4am

Go to http://www.at4am.ep.parl.union.eu

Amendments per language:

EN: 42

Amendment 1
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Title 0

Text proposed by the Commission	*Amendment*
Proposal for a	Proposal for a ***regulation*** on ENISA, the "EU ***Network and Information Security*** Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology ***IT security*** certification ("Cybersecurity Act")
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	(***This amendment applies throughout the text. Adopting it will necessitate corresponding changes throughout.***)
on ENISA, the "EU ***Cybersecurity*** Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology ***cybersecurity*** certification ("Cybersecurity Act")	
(***Text with EEA relevance***)	

Or. en

Justification

The prefix "cyber", derived from 1960s science-fiction works, has been increasingly used to describe the negative aspects of the Internet (cyberattack, cybercrime, etc.) but is legally very vague. Proposal to change the term "cybersecurity" to "IT security" for legal certainty.

Amendment 2
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 28

Text proposed by the Commission	*Amendment*
(28) The Agency should contribute	(28) The Agency should contribute

towards raising the awareness of the public about risks related to ***cybersecurity*** and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling reports with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting ***basic*** authentication and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices.	towards raising the awareness of the public about risks related to ***IT security*** and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling ***and publishing*** reports ***and guides*** with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions,bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting authentication***, encryption, anonymisation*** and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices ***and popularising at EU level security-by-design, privacy-by-design and the incidents and their solutions***.

Or. en

Justification

Detailing the objectives in line with the content of the articles.

Amendment 3
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 30

Text proposed by the Commission	*Amendment*
(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in ***cybersecurity***. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on ***cybersecurity*** aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the Agency's Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.	(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in ***IT security***. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on ***IT security*** aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the Agency's Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks. ***Partnerships should be established with academic institutions that have research initiatives in the relevant areas, while the input from consumer organisations and other organisations should have appropriate channels and be always analysed.***

Or. en

Justification

Introduction the notion that ENISA should benefit from the pool of available knowledge

Amendment 4
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 35

Text proposed by the Commission	*Amendment*
(35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal ***cybersecurity***. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet ***cybersecurity*** standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of ***cybersecurity*** of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including ***cybersecurity***, of their products and services.	(35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal ***IT security and refrain from allowing the sales or use of devices that do not meet minimum security conditions***. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet ***IT security*** standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of ***IT security*** of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including ***IT security***, of their products and services.

Or. en

Justification

In line with the introduction of a baseline IT security requirement

Amendment 5
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 41

Text proposed by the Commission	*Amendment*
(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional	(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional

expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board in order to ensure continuity in its work.	expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board in order to ensure continuity in its work. ***Due to the high market value of the skills required in the Agency work, it is necessary to ensure that the salaries and the social conditions offered to all Agency staff are competitive and ensure that the best professionals can choose to work there.***

Or. en

Justification

In order to have the appropriate level of expertise ENISA needs to be a competitive employer in a highly competitive market

Amendment 6
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 42

Text proposed by the Commission	*Amendment*
(42) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for ***cybersecurity***, and that the duties of the Executive Director be carried out with complete independence. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft	(42) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for ***IT security***, and that the duties of the Executive Director be carried out with complete independence. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft

statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.	statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative ***and gender*** balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.

Or. en

Justification

Introducing the modifications that add gender balance in some of the ENISA's layers.

Amendment 7
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 44

Text proposed by the Commission	*Amendment*
(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the	(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations***, academia*** and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the

attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure ***sufficient*** representation of stakeholders in the work of the Agency.

attention of the Agency***, providing input on which ICT products and services to cover in future European IT security certification schemes*** . The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure ***efficient and equitable*** representation of stakeholders in the work of the Agency.

Or. en

Amendment 8
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 47

Text proposed by the Commission	*Amendment*
(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the ***cybersecurity*** features of a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party, other than the product manufacturer or service provider. Certification cannot guarantee per se that certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain ***cybersecurity*** requirements laid down elsewhere, for example as specified in technical standards.	(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the ***IT security security*** features of a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party, other than the product manufacturer or service provider**.** ***While certification for lower assurance levels than high may require merely conformity assessment, for assurance level high, a profound security assessment and neutral certification is needed. Certificates on this assurance level therefore should be issued only by Cybersecurity Supervisory Authorities. The issuing of those certificates should be subject to mutual peer reviews by other Cybersecurity Supervisory Authorities***. Certification cannot guarantee per se that

certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain ***IT security*** requirements laid down elsewhere, for example as specified in technical standards.

Or. en

Amendment 9
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 52

Text proposed by the Commission	*Amendment*
(52) In view of the above, it is necessary to establish a European ***cybersecurity*** certification framework laying down the main horizontal requirements for European ***cybersecurity*** certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national ***cybersecurity*** certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.	(52) In view of the above, it is necessary to establish a European ***IT security*** certification framework laying down the main horizontal requirements for European ***IT security*** certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national ***IT security*** certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should ***be guided by security-by-design and the principles referred in Regulation 2016/679,*** be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

Or. en

Justification

Introducing the guiding principles for the certification schemes

Amendment 10
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 57

Text proposed by the Commission	*Amendment*
(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.	(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, ***baseline IT security requirements need to be mandatory and implemented on all consumer devices and services in order to tackle the challenges of an increasingly connected world. Such minimal requirements could include authentication, security of connections and patches for the discovered vulnerabilities.*** With a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

Or. en

Justification

The addition aims to quickly solve the current lack of harmonised baseline IT security requirements.

Amendment 11
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Recital 58 a (new)

Text proposed by the Commission	*Amendment*
	(58 a) Clear and mandatory baseline IT security requirements should be devised by the Agency, and should be proposed to the Commission as implementing acts if appropriate, for all IT devices sold in or exported from the Union. Those requirements should be developed within two years after the date of entry into force of this Regulation and revised every two years thereafter, in order to ensure constant and dynamic improvements. Those baseline IT security requirements should require, inter alia, that the device does not contain any known security vulnerability that it is capable of accepting trusted security updates, that the vendor notifies competent authorities of known vulnerabilities and repairs or replaces the affected device, or that the vendor informs when security support for such device will end.

Or. en

Justification

It is important to achieve a resilient IT environment to protect Cybercrime and protect fundamental rights of IT users. High level IT security objectives for a mandatory IT security base line within the Union should therefore be set in this regulation.

Amendment 12
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 1 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) lays down the objectives, tasks and organisational aspects of ENISA, the ***"EU Cybersecurity Agency", hereinafter 'the*** Agency***'***; and	(a) lays down the objectives, tasks and organisational aspects of ENISA, the ***EU Network and Information Security*** Agency ***(the "Agency")***; and

Or. en

Justification

Proposal to keep the original name of ENISA (the EU Network and Information Security Agency).

Amendment 13
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 2 – paragraph 1 – point 11 a (new)

Text proposed by the Commission	*Amendment*
	(11 a) "national certification supervisory authority" means an authority of a Member State responsible for carrying out monitoring, enforcement and supervisory tasks in relation to IT security certification on its territory;

Or. en

Justification

The notion was used in the text without proper definition.

Amendment 14
Jan Philipp Albrecht

on behalf of the Verts/ALE Group

Proposal for a regulation
Title 2

Text proposed by the Commission	*Amendment*
ENISA – the ***"EU Cybersecurity*** Agency***"***	ENISA – the ***EU Network and Information Security*** Agency

Or. en

Justification

In line with the proposal to keep the original name of ENISA (the EU Network and Information Security Agency).

Amendment 15
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 3 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Agency shall undertake the tasks assigned to it by this Regulation for the purpose of ***contributing to*** a high level of cybersecurity within the Union.	1. The Agency shall undertake the tasks assigned to it by this Regulation for the purpose of ***achieving*** a high level of cybersecurity within the Union.

Or. en

Justification

The change is setting the expectations higher, in line with the scope of the proposal.

Amendment 16
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 3 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding ***cybersecurity, and in any case, without prejudice to activities concerning public*** security***, defence, national security and the activities of the state in areas of criminal law***.	3. The objectives and the tasks of the Agency shall be without prejudice to the ***exclusive*** competences of the Member States regarding ***IT*** security.

Or. en

Justification

These should be no extensions to the limitations resulting from the treaties.

Amendment 17
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 4 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Agency shall promote cooperation and coordination at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to ***cybersecurity***.	4. The Agency shall promote cooperation and coordination at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, ***consumer organisations and other civil society organisations,*** on matters related to ***IT security***.

Or. en

Justification

The reference to the private sector needed proper extension to other important stakeholders, especially since the biggest impact is on consumers

Amendment 18
Jan Philipp Albrecht

on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. assisting the European Data Protection Board established by Regulation (EU) 2016/679 in developing guidelines to specify at the technical level the conditions allowing the licit use of personal data by data controllers for IT security purposes with the objective of protecting their infrastructure by detecting and blocking attacks against their information systems in the context of: (i) Regulation (EU) 2016/679[1a]; (ii) Directive (EU) 2016/1148[1b]; and (iii) Directive 2002/58/EC[1c];

[1a] 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) (OJ L 119, 4.5.2016, p. 1).

[1b] (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) (OJ L 119, 4.5.2016, p. 1).

[1c] 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).

Or. en

Justification

Establishing proper cooperation mechanisms.

Amendment 19
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 b (new)

Text proposed by the Commission	*Amendment*
	2 b. proposing policies with the objective of ensuring that ICT manufacturers act with due diligence regarding the timely fixing of IT security vulnerabilities in their products and services in order to avoid unduly exposing their users to cybercrime;

Or. en

Justification

Establishing a correct break down of responsibilities is essential to encourage all stakeholders to act with due diligence.

Amendment 20
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 c (new)

Text proposed by the Commission	*Amendment*
	2 c. proposing policies establishing a strong responsibility and liability framework for all stakeholders taking part in ICT eco- systems;

Or. en

Justification

Encouraging all stakeholders to act with due diligence.

Amendment 21
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 d (new)

Text proposed by the Commission	*Amendment*
	2 d. proposing policies strengthening regulation regarding the responsibilities of operators of critical network infrastructures in the case of an attack against their information systems affecting their users due to a lack of due diligence by some of the users of by the operator itself, where the operator has failed to take reasonable action to prevent the incident or to mitigate its effects on all users;

Or. en

Justification

Operators of critical infrastructures should be responsible for obtaining some assurance that only secure and trustworthy users/participants use their infrastructure and if needed should isolate un-secure ones to avoid incidents.

Amendment 22
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 e (new)

Text proposed by the Commission	*Amendment*
	2 e. proposing policies to limit the purchase and use of "Zero days" by public authorities with the purpose of

attacking information systems; promoting software audits and financing expert staff;

Or. en

Justification

By developing, buying up and exploiting back doors in IT systems with taxpayers' money, government bodies are putting the security of citizens at risk. In order to protect other stakeholders who deal responsibly with such vulnerabilities, the Agency should propose policies for the responsible exchange of information on "Zero days" and other types of security vulnerabilities that are not yet publicly known and that facilitate the closing of vulnerabilities.

Amendment 23
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 f (new)

Text proposed by the Commission	*Amendment*
	2 f. proposing policies for public authorities, private companies, researchers, universities and other stakeholders to publish all critical security vulnerabilities that are not yet publicly known within the framework of a responsible disclosure;

Or. en

Justification

Adequate EU policies are needed to implement a coherent responsible disclosure processes across the EU.

Amendment 24
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 5 – paragraph 1 – point 2 g (new)

Text proposed by the Commission	*Amendment*
	2 g. proposing policies for the extension of the use of "verifiable open-source code" for IT solutions in the public sector as well as for the related use of automated tools to ease review of source code and to easily verify absence of backdoors and other possible security vulnerabilities;

Or. en

Justification

The use of open-source software should be encouraged in public administrations that should also accept the related responsibilities of checking the source code of the applications that they use (against the presence/absence of major IT security vulnerabilities).

Amendment 25
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 6 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. The Agency shall facilitate the establishment and launch of a long-term European IT security project to support the growth of an independent EU IT security industry, and to mainstream IT security into all EU IT developments.

Or. en

Justification

ENISA should advise legislators regarding the preparation of policies to allow the EU to catch up with IT security industries in third countries. The project should be comparable in scale to what has previously been achieved in the aviation industry (example of Airbus). This is needed to develop a stronger, sovereign and trustworthy EU ICT industry (see the Scientific Foresight Unit (STOA) study PE 614.531).

Amendment 26
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 7 – paragraph 8 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) put in place certification schemes deterring the implementation by ICT manufacturers and service providers of secret backdoors intentionally weakening the IT security of commercial products and services and having a detrimental impact on the global security of the internet.

Or. en

Justification

This should be recognised as one of the main objectives of the Certification schemes

Amendment 27
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 8 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(c a) put in place certification schemes deterring the implementation by ICT manufacturers and service providers of secret backdoors intentionally weakening the IT security of commercial products and services and having a detrimental impact on the global security of the internet;

Or. en

Justification

This should be recognised as one of the main objectives of the Certification schemes

Amendment 28
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 9 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for ***individual*** users aimed at citizens and organisations;	(e) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for users aimed at citizens and organisations;

Or. en

Amendment 29
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 9 – paragraph 1 – point g a (new)

Text proposed by the Commission	*Amendment*
	(g a) promote the widespread adoption by all actors on the EU Digital Single Market of preventive strong IT security measures and reliable data protection and privacy enhancing technologies as the first line of defence against attacks against information systems.

Or. en

Justification

Based on the EDPS opinion (for PETs). The role of ENISA should clearly extend beyond support to Member States, the EC and EU agencies, but should also be more visible in the industry and in the general public.

Amendment 30
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 10 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) advise the Union and the Member States on research needs and priorities in the ***area*** of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;	(a) advise the Union and the Member States on research needs and priorities in the ***areas*** of cybersecurity ***and data protection and privacy***, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

Or. en

Justification

Based on the EDPS opinion. Research tasks of ENISA in the field of data protection and privacy were in the previous Regulation 526/2013 but are no longer in the Commission proposal. The disappearance of this task in research and advice is likely to lead to the discontinuation of ENISA's work on privacy and data protection enhancing technologies (PET) and more in general on data protection by design and by default.

Amendment 31
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 13 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.	1. The Management Board shall be composed of one representative of each Member State***, three representatives of the Permanent Stakeholder Group, one of which must represent the consumer interest***, and two representatives appointed by the Commission. All representatives shall have voting rights.

Or. en

Justification

The proposal should ensure that the interests of all stakeholders are appropriately represented in the governance structure of ENISA.

Amendment 32
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Executive Board shall be composed of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote.	3. The Executive Board shall be composed of five members appointed***, in a gender balanced manner,*** from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote.

Or. en

Justification

Gender balance needs to be introduced.

Amendment 33
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Procedures for the Permanent Stakeholders' Group, in particular regarding the number, composition, and the appointment of its members by the	2. Procedures for the Permanent Stakeholders' Group, in particular regarding the number, composition, and the appointment of its members by the

Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency's internal rules of operation and shall be made public.	Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency's internal rules of operation and shall be made public. ***The procedures shall follow best practice in ensuring a fair representation and equal rights for all stakeholders and shall enforce a gender balanced approach.***

Or. en

Justification

Equitable and fair representation is needed to achieve the best results.

Amendment 34
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 20 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2 a. The composition of the Permanent Stakeholders' Group shall include a minimum of five consumer organisations and civil society organisations.

Or. en

Justification

In the current Permanent Stakeholders' Group, only one expert out of thirty members of the Group represents the consumers' views and that is not enough.

Amendment 35
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 22.	2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the ***debates and the*** results of its work. It shall also make public the declarations of interest made in accordance with Article 22.

Or. en

Justification

Transparency needs to be enforceable, taking into account the application of art.24

Amendment 36
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 34 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Management Board shall adopt a decision laying down rules on the secondment to the agency of national experts.	2. The Management Board shall adopt a decision laying down rules on the secondment to the agency of national experts***, amongst others disallowing no-cost practices and promoting fair remuneration***.

Or. en

Justification

Equal pay for equal work: in order to get the best staff it is unacceptable for EU to demand experts from various MS to work with different national pay levels on the same tasks.

Amendment 37
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 41 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.	2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the ***headquarters and other offices*** location ***by international airport***, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Or. en

Justification

While the host state is a matter external to this regulation, ensuring the best conditions to for the Agency to function is within the scope and for that guidance is provided here.

Amendment 38
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 43 a (new)

Text proposed by the Commission	*Amendment*
	Article 43 a
	Security by design and by default
	1. Taking into account the state of the art, producers and service providers shall ensure the security by design and by default of their ICT products and services. Manufacturers and service providers must ensure that the software running on their ICT product or service is secure and does not have any known security vulnerability considering the state of the art technology at the time. ICT products and services

must implement the following technical measures:

(a) ICT products and services must be provided with up to date software and must include mechanisms to receive secure, properly authenticated and trusted software updates on a regular basis;

(b)remote access capabilities of the ICT product or service must be documented and secured against unauthorised access during the installation at the latest;

(c) ICT products shall not have the same default hardcoded standard passwords for all devices;

(d) Data stored by ICT products and services must be securely protected by state of the art methods such as encryption;

(e) ICT products and services shall only accept high-security methods for authentication.

2. Manufacturers and service providers must notify the competent authority of any known security vulnerabilities as soon as they are discovered. In addition, they must provide a timely repair and/or replacement to overcome any new security vulnerability discovered.

3. ICT products and services placed on the market shall comply with the obligations in paragraph 1 during their foreseeable and normal period of use.

4. The Commission shall by means of implementing act, and in cooperation with ENISA, adopt detailed rules on the specificities of the security requirements provided in paragraph 1.

5. Where the market surveillance authorities have reasons to believe that the ICT product or service does not comply with the requirements laid down in this Regulation, they shall without delay require the relevant manufacturer

or service provider to take appropriate corrective action to bring the product into compliance with those requirements, to withdraw the product from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as they may prescribe.

6. Where the manufacturer or service provider does not take adequate corrective action within the period referred to in paragraph 5, the market surveillance authorities shall take appropriate provisional measures to prohibit or restrict the product being made available on their national markets, to withdraw the product from that market or to recall it.

7. Market surveillance authorities shall organise appropriate checks on product compliance and oblige the manufacurers or service providers to recall non-compliant products from the market. When identifying the products that will be subject to compliance check, national certification authorities shall prioritise high risk products for consumers, products embedded with new technologies and/or products with high selling rates.

Or. en

Justification

One of the key reasons behind the increase of cyberattacks is the lack of security functionalities incorporated in the design of the connected products and/or services. Today, most of the connected devices available in the EU's single market are designed and manufactured without the most basic security features embedded in their software. In order to trust the Internet of Things, consumers must be assured that the connected products they purchase or services they use are secure and protected from software and hardware vulnerabilities. To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market. Such a horizontal and binding framework should be established as a complement of existing and pending legislation that requires cybersecurity measures such as the General Data Protection Regulation and the proposal for a European Electronic Communication Code.

Amendment 39
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 44 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Following a request from the Commission, ENISA shall prepare a candidate European ***cybersecurity*** certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States ***or*** the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.	1. Following a request from the Commission, ENISA shall prepare a candidate European ***IT security*** certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States**,** the European Cybersecurity Certification Group (the 'Group') established under Article 53 ***or the Permanent Stakeholders Group established under Article 20*** may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.

Or. en

Justification

It is of the outmost importance that all experts are systematically and regularly consulted during the preparation of a certification scheme within ENISA.

Amendment 40
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 44 – paragraph 2

Text proposed by the Commission	*Amendment*
2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the	2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group ***as well as with the consumer organisations, Article 29 Working Party and the European Data Protection Board***.

preparation of the candidate scheme, including by providing opinions where necessary.	The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.

Or. en

Justification

Based on the EDPS opinion. It is of the utmost importance that technical and governance synergies be created so that certifications under the European Cybersecurity Certification Framework and under the GDPR are not perceived as contradictory or unrelated by the organisations striving for compliance with the relevant instruments.

Amendment 41
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 44 – paragraph 4

Text proposed by the Commission	*Amendment*
4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.	4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation. ***The Commission may consult the European Data Protection Board and take account of its view before adopting such implementing acts.***

Or. en

Justification

Based on the EDPS opinion. This amendment ensures consistency between certifications under the European Cybersecurity Certification Framework and under the GDPR.

Amendment 42
Jan Philipp Albrecht
on behalf of the Verts/ALE Group

Proposal for a regulation
Article 48 a (new)

Text proposed by the Commission	*Amendment*
	Article 48 a
	Baseline IT security requirements
	1. The agency shall, by ... [two years after the date of entry into force of this regulation], propose to the Commission clear and mandatory baseline IT security requirements for all IT devices sold in or exported from the Union such as:
	(a) the manufacturer providing a written certification that the device does not contain any hardware, software or firmware component with any known security vulnerabilities;
	(b) the device relies on software or firmware components capable of accepting properly authenticated and trusted updates from the vendor;
	(c) documented remote access capabilities of the device that are secured against unauthorized access during the installation at the latest; no default hardcoded standard passwords for all devices, a documented possibility for updates which clearly points out responsibilities in case the user does not update the device;
	(d) an obligation of the manufacturer of the internet-connected device, software, or firmware component to notify the competent authority of any known security vulnerabilities;
	(e) an obligation of the manufacturer of the internet-connected device, software, or firmware component to provide a repair in respect to any new security

vulnerability discovered;

(f) an obligation of the manufacturer of the internet-connected device, software, or firmware component to provide information on how the device receives updates, the anticipated timeline for ending security support and a notification when such security support has ended.

g) an obligation of the manufacturer to release the source code and documentation after the end of support date;

2. The Agency shall review and, where necessary, amend the requirements referred to in paragraph 1 every two years, and submit any amendments as proposals to the Commission.

3. The Commission may, by way of implementing acts, decide that the proposed or amended requirements referred to in paragraphs 1 and 2 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 55(2).

4. The Commission shall ensure appropriate publicity for the requirements which have been decided as having general validity in accordance with paragraph 3.

5. The Agency shall collate all proposed requirements and their amendments in a register and shall make them publicly available by way of appropriate means.

6. While manufacturers are responsible for ensuring product compliance of an ICT product or service, importers must make sure that the products they place on the market comply with the applicable requirements and do not present a risk to the European public. The importer has to verify that the manufacturer outside the EU has taken the necessary steps and that the product or service complies with the

provisions of paragraph 1. Distributors of ICT products or services must have a basic knowledge of the legal requirements and the accompanying documentation. Distributors should be able to identify products that are clearly not in compliance. They must also be able to demonstrate to national authorities that they have acted with due care and have affirmation from the manufacturer or the importer that the necessary measures have been taken. Furthermore, a distributor must be able to assist national authorities in their efforts to receive the required documentation.

Or. en

Justification

It is important to achieve a resilient IT environment to protect Cybercrime and protect fundamental rights of IT users. High level IT security objectives for a mandatory IT security base line within the Union should therefore be set in this regulation.