EUROSMART
The Voice of the Digital Security Industry

Eurosmart's feedback on Radio Equipment Directive's delegated act

Eurosmart feedback on **COMMISSION DELEGATED REGULATION (EU) supplementing of Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements for radio equipment referred to in Article 3(3), points (d), (e) and (f),**

EUROSMART welcomes the latest draft of the DA, proposed with the intention and in the context to ensure that RF electronics are trustworthy in safeguarding against cybersecurity hacks, fraud, and safeguards privacy. This reinforced the message of the Commission to address cybersecurity risks in all connected products and associated services and throughout their entire lifecycle, as defined in the December's 2020 Joint Communication on the "EU's Cybersecurity Strategy for the Digital Decade"[1]? In this Communication, the Commission announced considering a comprehensive approach, including possible new horizontal rules to improve the cybersecurity of all connected products and associated services placed on the Internal Market.

Eurosmart wants to bring to the attention of the Commission a number of areas where we believe there is a need for further improvement or clarifications within the draft DA.

Many issues that are arising from the interpretation and applicability of RED, are related to the scope definition. For example, the term "radio equipment" is ambivalent in the DA: daily use equipment by adult consumers and children implies "connected devices", terms like inter-connected and "smart" are interlinked, at least to define the toy's product category, etc. while it's important to notice that not all "connected devices" use radio signals for communication. Therefore, it's necessary to adapt harmonised definitions across the EU documentation. This will reduce the confusion, enable adequate adoption, and facilitate the work of standardisation bodies and regulators alike.

Eurosmart recommends a consistent language that helps to scope the applicability of the act and the affected products while removing uncertainty on the language of the DA. In this respect, the RED-EG[2] should be tasked with updating the RED guide[3] of December 2018, which should clearly mention and identify the products falling under the scope of the delegated act.

[1] Joint Communication to the European parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade - JOIN/2020/18 final

[2] RED-EG: Commission expert group on Radio Equipment (E03587)

[3] Guide to the Radio Equipment Directive 2014/53/EU

The DA includes "childcare" equipment in its scope as more and more products used by or for children are now connected. This product category raises specific concerns (e.g., parental control). The DA text limits the definition for "child-care-devices" only to devices that are specifically sold for childcare. This would exclude additional devices that might be used for child monitoring as well, like for example smart speakers, "smart" surveillance devices, etc. Someone may overcome this restriction by officially targeting devices for other natural human groups. The same issue may occur for other vulnerable category of end users (e.g., old or sick persons).

Eurosmart recommends elaborating the product categories, in a harmonized language that prevents loopholes and adds clarification to the European industry. To that end, the equipment designed or intended not exclusively for childcare should also be covered by the DA (in symmetry to the wording used for wearables, as a matter of legal coherence and clarity). Moreover, it is advisable to address other natural human groups might also be vulnerable for example, senior care, ill people.

Harmonised standards that make the compliance assessment requirements along all the EU cybersecurity regulations consistent would be necessary to ensure adoption and deployment. An ecosystem of trust is possible only if the regulations are supported by appropriate compliance requirements such as third-party testing. Also, the security level needs to be defined and what is in scope (i.e. physical attacks and dynamic security countermeasure testing) …

Eurosmart recommends adopting a risk-based approach for standards development. Moreover, security compliance must be assessed by third party evaluations. These aspects deserve to be clearly mentioned in the future standardisation mandate to the ESOs.

The EU framework related to 5G by the Commission, clearly makes direct references to the CSA as the mechanism for strengthening cybersecurity in the EU. The 5G framework, as described in the documentation, is part of the URWP and currently in formation as an ad-hoc working group by ENISA. Moreover, the "framework" concept is managed as the regulatory stack. In that context, the NISD2, also listed here, makes direct reference to the CSA as the mechanism for achieving regulatory compliance. The delegated act can be interpreted as acknowledging the CSA as the regulatory compliance mechanism for 5G equipment and critical infrastructure as defined by NISD and by syllogisms, making it applicable for RED. There is a need for clarification in the text with regards to the commission intention. Fragmentation or duplication of certification of 5G under RED (related to the placement of products on the market) needs to be avoided, especially where CSA covers more than just the radio elements of 5G.

The CSA is complementary regulation. For example, regulations like NISD will be looking to enforce certification of devices in use on critical infrastructure, utilizing certification schemes or frameworks created under the CSA umbrella. Therefore, cybersecurity certification is not voluntary, as stated by the DA; what is voluntary is the use of this certification in domains where it is not mandatory. This also means that while the CSA cannot and shouldn't be enforced as the mechanism for demonstrating conformance with the RED requirements, it doesn't exclude it from using it as a reference framework providing evidence of conformance. Adopting such an approach will help to avoid overlapping requirements. However, there might be contradicting security and certification requirements from CSA, and this needs to be explicitly noted to avoid contradiction.

Eurosmart recommends using certificates issued under European Certification schemes, to demonstrate the presumption of conformity with requirements of the RED Delegated Act (as provided by art. 54.3 of the Cybersecurity Act).

Upholding and safeguarding the high level of security needed in Smart meters and public communications networks requested at national level is paramount. However, the DA seems to leave open the security level definitions for Privately owned communications networks.

Eurosmart suggests excluding smart meters and public communications networks whose security requirements are managed by national authorities and already covered by NISD. Meanwhile, own private operations of critical infrastructures should be part of the DA scope.

It is necessary to ensure that the security in all connected devices is trustworthy. For example, we do not accept a self-certified Door-lock as trustworthy as compared to a door lock tested and certified by professionals. Eurosmart is of the opinion that for the harmonised standards for the RED Delegated Articles 3(3), d, e, f, it is necessary that 3rd party conformity assessment is mandated. Also, it is necessary that the testing is dynamic rather than static to ensure that cybersecurity hacking capabilities are overcome as close as possible to real-time. A definition of 'sufficient security level is necessary, and also the scope of assessment is required that should include countermeasures to appropriate mechanisms, e.g., Physical attacks on devices and device components, in order to build a TRUST-worthy cyber-secure ecosystem of devices and device components. Moreover, it's important to clarify the intention of the DA with regards to the life cycle as per definition, RED focus on placing the product on the market, and it's not clear how post-sales vulnerabilities will be addressed.

An example of this is given on attacks to the supply chain beyond the control of the OEM. They could derivate on cyber vulnerabilities exploitable on a large scale and therefore affecting the network performance. Since such kinds of vulnerabilities require deepest analysis of the processes involved in the development cycle (process, administration, etc.), and they are not considered by the regulation.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High-Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys**, **Thales**, **Tiempo Secure, TrustCB, Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom – IMT, ISEN – Institut Supérieur de l'Électronique et du Numérique Toulon**), and associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's expert groups: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at the EU level, such as CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, Global Platform, ISO, SIA, TCA and TCG.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com

@Eurosmart_EU

@Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com