DIGITALEUROPE

10 MARCH 2021

Feedback on draft standardisation request for Arts 3(3)(d/e/f) RED

Introduction

DIGITALEUROPE appreciates the opportunity to provide its feedback on the Commission's draft standardisation request in support of Arts 3(3)(d/e/f) of the Radio Equipment Directive (RED).[1] We are supportive of having harmonised standards available well before the delegated act applies.

This response provides our comments to document EG RE (09)09 as presented to the Expert Group on Radio Equipment.

[1] Directive 2014/53/EU.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Timely delivery of harmonised standards

Harmonised standards are essential

DIGITALEUROPE would like to stress again the importance of the timely delivery of harmonised standards. Not only are harmonised standards applied under the Module A approach ('self-declaration'), but in practice they are also applied as the basis of the conformity assessment under Modules B + C ('Notified Body route'). Although Notified Bodies should in theory only look at conformity with the essential requirements itself, they lack experience in the emerging field of cybersecurity and will need a basis to assess compliance of radio equipment. Lastly, the application of harmonised standards also ensures a level playing field in the European single market.

Time for updating/selling out models is needed

It is crucial for industry that harmonised standards be available in a timely fashion in order to allow for sufficient time to design, manufacture and place compliant products on the market.

In case of harmonised standards cited under the RED, typically a period of 18 months is given to manufacturers to assess their current products according to the technical requirements set in a revision of a harmonised standard, to modify the hardware and software where needed and to update the technical documentation.

For models that are continuously placed on the market, but might no longer meet the new requirements, time needs to be given to sell out the manufacturer's current stock instead of scrapping these products. For new models in the consumer electronics industry, usually a new variant or model is introduced on the market every year, while for professional products the renewal cycles are typically longer.

An absolute minimum timeframe of 18 months is necessary starting from the point of citation of the harmonised standards in the Official Journal of the European Union (OJ).

The critical path: 24 months + 18 months

Based on the above, we urge that the deadline for adoption by the European standardisation organisations (ESOs) be changed to 18 months before the date of applicability. Taking into account the usual development cycles of harmonised standards, we consider 24 months to be the fastest timeframe possible for ESOs.

Considering this critical path of 18 months for manufacturers to update or sell out their products, and 24 months for standards development by the ESOs, we urge that 42 months is the minimum time needed for the delegated act's date of applicability.

Proposed changes

Deadline for the adoption by the ESOs
[~~***10***~~ ***18*** months before date of applicability]

General requirements for harmonised standards

Legal requirements

Clear guidance from the Commission on the legal requirements to be met by the future harmonised standards will ensure a better understanding by the ESOs and avoid future discussions during the citation of harmonised standards in the OJ. With this approach, we trust that the Commission's evaluation under Art. 10(5) of the Regulation on European standardisation[2] will be done in the most efficient way.

However, while the standardisation request should give a clear indication of the expected requirements, the actual technical specifications should be left to the expertise of the ESOs' technical committees. The standardisation request should by contrast provide more general guidance on what the harmonised standards should cover, which can then be further detailed at technical level. Any specific requirements should only be given in the delegated act as non-mandatory advice for consideration by the ESOs, which would then develop a list of technical requirements as part of their harmonised standards activity. The more general guidance could benefit from the following suggestions:

For essential requirement 3(3)(d), addressing misuse of network resources:

- Mitigate the effects of denial-of-service attacks (cf. 2.1(d)).

For essential requirement 3(3)(e), addressing protection of personal data and privacy:

- Protect personal data (cf. 2.2(a)-(b));
- Use restrictive user access rights (cf. 2.2(f));

[2] Regulation (EU) No 1025/2012.

- Ensure the confidentiality of communications (cf. 2.2(h));
- Secure mechanism for updating software (cf. 2.2(m));
- Preserve settings after update procedure (cf. 2.2(o));
- Strong password protection (cf. 2.2(u),(w)-(x));
- Defence mechanism against exhaustive attempts (cf. 2.2(y));
- Do not use credentials that cannot be changed (cf. 2.2(aa));
- Protect passwords, access keys, etc. (cf. 2.2(bb));
- Disable data communication features that are not essential (cf. 2.2(ee)-(ff));
- Allow users to easily delete their stored personal data (cf. 2.2(hh)).

For essential requirement 3(3)(f), addressing protection from fraud:

- Implement secure connection (cf. 2.3(c));
- Protect financial or monetary data (cf. 2.3 (d)-(e)).

Proposed changes

Add ‘for consideration by ESOs’ on top of the detailed list of specific requirements for each harmonised standard or use only the more general requirements above as examples or candidate requirements.

Independently verifiable test methods

Requirements to manufacturers should be on a functional level and tests should be designed accordingly. Item 1.3 should better specify that each harmonised standard shall include methods and conditions to verify compliance and shall be verifiable ‘in an objective and reproducible way.’

This approach, which we support, might however not be achievable for all the specific requirements of Part B. While the essential requirements related to health and safety, electromagnetic compatibility and radio concern physical parameters that can be measured, in this case the parameters are more abstract and not always verifiable.

This means that special test software might be appropriate that is not accessible to the user for the intended use of the equipment. In addition, where a test method is not possible, a declaration by the manufacturer would be necessary. As a consequence a standard doesn’t have to explicitly include ‘test methods’ but could also mention ‘procedures or methods to verify compliance.’

Proposed changes

Make the list of specific requirements a recommendation for consideration by ESOs. ESOs (including delegates from Member States) will be able to determine whether a requirement can be tested in an objective and reproducible way.

We propose changing the requirement for test methods (1.3) thus:

(b) ***suggestions for ~~test~~*** methods***, procedures or ~~and~~*** conditions to verify compliance of the products referred to in point 1.3 (a) of this Part with the corresponding specifications referred to in point 1.3 (a) of this Part;

Obligations for the economic operator

Item 1.4 mentions that the harmonised standards shall not address any procedures, responsibilities or obligations for any economic operator. In this respect, we note that some specific requirements (e.g. 2.1(k)-(l), 2.2(e),(g) and 2.3(g),(j),(l),(m)) are not related to the technical specifications of the product itself, but rather to procedural obligations for the manufacturer.

Clear examples of this are the requirement that a product should be secure by default and by design, monitoring of vulnerabilities and provision of up-to-date protection measures at the moment of placing on the market. These requirements are not technical requirements for the equipment, but rather manufacturer obligations that go beyond those of Art. 10 RED.

The requirement in 2.2(o) specifies that the update process can only result in improvements in the security of the device. In our opinion this goes beyond the RED requirements. When the product meets the essential requirement, this should suffice.

We believe that requirement 2.2(k) on the processing of location data is another example that applies to other actors, rather than being a technical requirement for the product.

With respect to remote management (e.g. 2.2(p),(ii)), this is not related to the radio equipment itself (‘remote’) and should hence be removed.

Proposed changes

Remove all requirements that are not related to the product itself, but rather obligations of the manufacturer or another economic operator.

Requirements of an administrative or organisational nature

Item 1.5(f) indicates that harmonised standards shall not make conformity with the standards dependent on requirements of an administrative or organisational nature. There are some examples in the specific requirements where information to the user needs to be provided.

For example, item 2.2(l) requires the provision of warning information, while item 2.2(n) requires informing the user of software/firmware changes. The need for simplified routines for installation and configuration in item 2.2(q) seems to go beyond a technical requirement of a harmonised standard and is rather part of the user instructions. Finally, the monitoring of known vulnerabilities is a clear requirement of an organisational nature.

Proposed changes

Remove all specific requirements that are of an administrative or organisational nature.

Coherence with other legislation

DIGITALEUROPE appreciates the Commission's intention to ensure coherence with other legislation such as the Cybersecurity Act[3] as well as codes of conduct and certification mechanisms under the GDPR.[4] However, coherence should be ensured through legislation, not through standardisation.

Item 1.4 Part A correctly states that the harmonised standards shall not support any legal requirements other than those set out in Arts 3(3)(d)-(f) RED. Were this not the case, there is a risk that the development of RED standards might be impacted in the final stages based on unforeseen developments.

Proposed changes

Remove requirements (1.3 and 1.4) that harmonised standards shall support the Cybersecurity Act and GDPR.

Specific requirements for harmonised standards

[3] Regulation (EU) 2019/881.

[4] Regulation (EU) 2016/679.

DIGITALEUROPE would further like to provide some comments to the specific requirements.

Security systems

Requirements 2.1(a) and 2.3(a) include security systems, such as for monitoring and controlling network traffic. Such mechanisms add to the energy consumption of devices in networked standby mode. In case sophisticated requirements are set, this could lead to difficulties in meeting ecodesign[5] or energy efficiency requirements for networked standby mode.

Proposed changes

Make the requirements on security systems optional taking into account ecodesign or energy efficiency requirements.

Limited hardware capabilities

Implementing an activity logging tool (2.2(t) and 2.3(o)) might be possible for radio equipment with advanced computing possibilities, but not for other consumer and B2B devices that often have limited memory space and processing power. Such limited hardware capabilities use cases must be taken into account.

Proposed changes

Make the requirements on activity logging optional taking into account the limited hardware capabilities of many consumer and B2B devices.

Hand-held mobile devices

Item 2.2(jj) sets specific requirements for smartphones. However, this is not a separate category as defined in the draft delegated act, and we believe this goes beyond the flexibility of the standardisation request.

Proposed changes

Remove the specific requirements for smartphones.

User interface

[5] Commission Regulations (EC) No 1275/2008 and (EU) No 801/2013.

It is important to understand that much radio equipment only contains very restricted user interface (UI) capability. As an example, many consumer and B2B devices just come with a single colour LED display. Such devices will not be able to meet requirements for very complex user interaction (e.g. 2.2(j),(n),(r)-(s)). Because of this, the text ‘where appropriate’ should be added.

Proposed change

Make the requirements on user interaction optional taking into account the limited UI capabilities.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK