15 November 2019

European DIGITAL SME Alliance

Position Paper

Responding to the applicability of the Radio Equipment Directive (RED, 2014/53/EC)

BACKGROUND

The Radio Equipment Directive 2014/53/EC (RED) establishes a regulatory framework for placing radio equipment on the EU market. Due to the digitalisation, this directive has gained in importance as the scope of the RED covers devices that use the radio spectrum for communication and/or radio determination purposes. All internet-connected wireless devices (including e.g. IoT devices) fall under this Directive. The RED ensures that radio equipment, at the moment of its placing on the market, respects the essential requirements of the Directive as regards e.g. health and safety, electromagnetic compatibility and radio spectrum[1]. Radio equipment can change its behaviour or be reprogrammed at the upload of new software – this is the key feature exploited by reconfigurable radio systems (RRS). A variety of equipment placed on the market can be reconfigured through software. There is an issue when it comes to legal certainty when placing RRS on the market. [2]

The European Commission is currently investigating the extent of the applicability and issues of liability related to the RED. This may lead to an update of the technical framework by drafting delegated acts based on its Article 3(3)(i). The Commission has

[1] Articles 3(1) and (2) of the RED sets out the essential requirements that radio equipment shall respect.

[2] See European Commission Impact Assessment: https://ec.europa.eu/info/law/better-regulation/initiative/2042/publication/380919/attachment/090166e5c0fe9ef0_en

therefore carried out an impact assessment that should provide input about problems[3] related to reconfigurable radio systems on the one hand and possible solutions and their consequences on the other hand.[4] Further, the European Commission has published an Open Public Consultation (OPC) which aims to gather feedback from relevant stakeholders about the market access conditions of wireless devices which are connected to the internet or wearable[5]. Specifically, the need for strengthening (i) data and privacy protection, and (ii) protection from fraud is being considered.

According to the feedback and the impact assessment as well as the input received via the RED expert group, the Commission may consider different policy options to strengthen the trust in the field of wireless devices and their applications. Specific mandatory requirements would concern the activation of one or more delegated acts pursuant to the RED**.**

In practice, these delegated acts would require that wireless devices (or some of their radio components) cannot be placed on the EU market unless a satisfactory level of protection of data and privacy and/or from fraud is demonstrated. If not done well, this may lead to a lockdown of reconfigurable systems due to concerns about data protection and fraud, thus limiting the innovative potential of the market.

[3] Potential problems: Software (e.g. firmware) can govern some aspects of the radio equipment or its components so to (i) enable/disable peripherals or components (e.g. fans), (ii) allow an increased power consumption or (iii) alter the transmitting power of radio equipment, having an impact on the electrical safety of the equipment.

[4] See European Commission Impact Assessment: https://ec.europa.eu/info/law/better-regulation/initiative/2042/publication/380919/attachment/090166e5c0fe9ef0_en

[5] Concerned products are "internet-connected radio equipment and wearable radio equipment". For instance, internet-connected radio equipment is smartphones, laptops, smart appliances, routers, radio-connected toys, wireless cameras, other wireless Internet of Things (IoT) devices, some of their radio components, etc. Examples of wearable radio equipment are smartwatches and fitness wireless devices.

European
DIGITAL SME
Alliance

WHAT'S AT STAKE FOR SMALL AND MEDIUM SIZED COMPANIES IN THE ICT SECTOR?

As in other fields, SMEs play a significant role in providing innovation, fostering competition and reducing product costs. Protecting SMEs means fostering the ability of the EU to innovate and to compete in global markets. **DIGITAL SME is concerned about the impact of potential revisions of the RED on the ability of SMEs to bring innovation to the radio equipment market.** Specifically, DIGITAL SME is concerned about any measure that could present an obstacle for SMEs to bring their product to the market and that could hinder the development of a dis-aggregated (horizontal) market. At the same time, DIGITAL SME believes that Article 4 needs to be updated in order to ensure software/hardware dis-aggregation.

A horizontal market is a market in which customers can buy hardware and software from different vendors combining them into a system. This process offers a great degree of flexibility and cost reduction. Thus, a horizontal market could lead to increased innovation, higher value, lower hardware costs, lower operating costs, lower switching costs and higher allocative efficiency.

Due to the global price competition on the hardware sector, most European SMEs are prone to innovate in software rather than on hardware. At the same time, software is the area where most of the innovation is taking place. As a consequence, SMEs rely on hardware manufactured by third-party enterprises. To continue their activity, they need a certain degree of openness. Therefore, DIGITAL SME advocates for a clear legal framework that sets the **foundation for hardware/software dis-aggregation**, which would allow SMEs to develop software on existing hardware. A review of the RED and potential delegated acts based on the RED have the potential to prevent or promote software/hardware disaggregation. Consequently, this may impact the development of a horizontal market for wireless devices which are connected to the internet or wearable in the EU. For this reason, any RED delegated act or other measures need to consider the possibilities and/or impact of preventing the creation of a horizontal market.

As a general concept, any procedure or mechanism that would increase the complexity or costs to combine software and hardware provided by different manufacturers may negatively impact SMEs innovating in this space.

+32 28930235 office@digitalsme.eu www.digitalsme.eu
123, Rue du Commerce, 1000, Brussels, Belgium
VAT: BE0899786252 EU Transparency Register: 082698126468-52

PROPOSALS ON THE IMPLEMENTATION OF ARTICLES 4 AND 3.3.(I) OF THE RED

In the following, DIGITAL SME presents its position on both topics of Reconfigurable Radio Systems (RRS), and privacy and fraud protection. This position paper examines Articles 3.3.(i) and 4 of the RED. The proposals aim to ensure that the applicability of the RED and delegated acts will allow for the creation of a horizontal market for wireless devices which are connected to the internet or wearable in the EU.

DIGITAL SME commentary on Article 4 and on options proposed in European Commission impact assessment

There is a need to clarify responsibility and liability. Otherwise, there is a high risk that the market will regulate itself on the basis of Article 4 and standard EN 301 893. The standard in combination with Article 4 states that if a software is loaded by the user, it could revoke the essential requirements set out in Article 3, and therefore make the hardware vendor liable. Therefore, vendors will likely decide to lock down the hardware in order to avoid compliance issues. There is a need to clarify this with a delegated act; otherwise, innovation and a horizontal market will be hindered. The standard is even worse: it clearly says that if a radio is configurable, it's not compliant.

SMEs need a clear legal framework in order to continue developing software that works on third party hardware. The status quo, instead:

- Does not provide clarity about liability. Without clarity, hardware vendors will be driven by the fear of possible liabilities generated by software vendors and will protect themselves with hardware lock-down. This may occur in particular if EN 301 893 applies.
- If Option 1, i.e. self-regulation, is adopted, the industry is left to self-regulate[6]. Without a framework that clearly protects hardware vendors from liabilities

[6] See European Commission impact assessment: https://ec.europa.eu/info/law/better-regulation/initiative/2042/publication/380919/attachment/090166e5c0fe9ef0_en

potentially generated by software, software-hardware dis-aggregation will not be possible.

How can this be avoided?

- Software vendors should be able to declare their software as conform, through a procedure that allows them to take responsibilities, without adding significant costs or delays to time-to-market, and without interference by third parties.

Conclusion: **Article 4 should not involve any upload filter and provide a simple liabilities-assignment framework via a delegated act. Software vendors may simply self-declare that their software does not compromise the essential requirements and take responsibility for this.**

Further recommendation: the RED application should be addressed in a way that strengthens the horizontal market not only via delegated acts, but also by inviting standardizing bodies to specifically avoid measures that damage the horizontal market in standards. This could have, in some cases, the side-effect of significantly reducing non-compliance, such as in the dynamic frequency selection (DFS) high non-compliance rate (see the EG RE (03)15 - ADCO RED report to EG 03[7]). This comes from the clear divergence between market needs for reconfigurability and the philosophy behind standard EN 301 893, which clearly does not envision the horizontal market with regard for the DFS aspect.

DIGITAL SME commentary on Article 3.3.(i)

With a clear framework defined in Article 4, there will be no need for a delegated act. However, as the European Commission also wants to regulate privacy and fraud protection, this should at least be done in a way that does not impact the horizontal market too much and avoids hardware lockdown.

[7] See CIRCABC: https://circabc.europa.eu/ui/group/43315f45-aaa7-44dc-9405-a86f639003fe/library/d2aaa898-316d-4e92-be0c-c669fc9b944a/details

- **Article 3.3.(i) should not be implemented**, as Article 4 should be enough to allocate responsibility to the proper party (be it the hardware manufacturer, the software manufacturer or the user), except for classes of devices that imply significant risk in relation to privacy and fraud protection.
- Regarding classification, it's important to state that **the risk class should depend not only on the device classification but also on the specific design**: a device of a specific class, e.g. IoT or Wi-Fi Routers, could be risky or not based on how the hardware and software are designed. A design that allows partial modification of software, with no ability to change the parameters that impact the essential requirements, should not be considered risky at all and then 3.3.(i) should not be applicable. Therefore, treating devices of the same class indistinctly of the design choice would represent an obstacle for the industry to find solutions that meet the required level of protection.
- If case 3.3.(i) is applied to any specific class of devices, it should be implemented in a way that does not negatively impact the creation of a horizontal market.

Conclusion: DIGITAL SME recommends limiting the application of 3.3.(i) to devices that have a significant privacy/fraud protection risk, where the risk is evaluated also accounting for the product design. Where 3.3.(i) should be applicable, DIGITAL SME considers the following points as the main requirements for any 3.3.(i) implementation to avoid the destruction of a horizontal market:

a. **The 3.3.(i) mechanism should not provide any veto power to hardware vendors.** Even with a proper liabilities-allocation framework, large multinational hardware vendors may not have a strong reason to promptly address SME software vendors' requests to enable their software (e.g. distributing a key or signing a firmware), and actively or passively obstruct them, delaying and in the worst case sending them out of business. **For a true horizontal market to thrive, software vendors should be able to install their software on third party hardware without any kind of interference by hardware vendors.**

b. **The 3.3.(i) mechanism should not increase costs** sustained by the software manufacturers. A self-certification may be acceptable.

c. **The 3.3.(i) mechanism should not delay the go-to-market.**

d. **The 3.3.(i) mechanism should not create extra complexity for the user** who intends to combine software and hardware (it should ideally work in a click), as any complexity increase may represent an obstacle to adopt a disaggregated solution and to benefit from its cost-reduction.

e. **The 3.3.(i) mechanism should ideally work on offline devices.** Installing new software on offline hardware units may become significantly more expensive if those units request to be configured and go online before they can receive the new software. The person installing would be required to configure each of the Wi-Fi routers deployed, e.g. 50 routers to be installed in a school, to have these online before uploading the new software. Instead, the same operation may be executed with a single click in case configuration is not required. This latter option would be operationally more efficient and would reduce the costs for the school to adopt a horizontal software on 50 units. See the last paragraph for a detailed example.

The above list defines the requirements of a "horizontal-market friendly" implementation of 3.3.(i). To conclude, we would like to focus on a specific use case, i.e. the *Installation of a Wi-Fi network in a school with limited budget*. Enabling the horizontal market means significant cost savings, increasing efficiency and serving the underserved ones. For this reason, we recommend that these types of use cases are taken into account when implementing 3.3.(i).

Case study: Benefits provided of horizontal market in providing Wi-Fi access in schools

The typical school in low-income European regions can only afford off-the-shelf Wi-Fi routers, which use radio chipsets similar to vastly more expensive high-end Wi-Fi routers. A third-party software can upgrade them and add features such as protection from viruses/pornography at a fraction of the cost of high-end Wi-Fi solutions that provide similar features. This can cut the cost on hardware by a factor of up to 20 and the total cost of ownership can be reduced to a fifth[8]. The following example theorises two options of a school that requires 30 Wi-Fi routers:

PROPRIETARY SOFTWARE/HARDWARE SOLUTION (NO HORIZONTAL MARKET)

Hardware: €500 x 30 units = €15,000 (capex)

Installation: €5,000 (capex)

Software cost: €100 /year/unit (opex)

TCO FOR 5 YEARS: €500 x 30 + €5000 + €100 x 30 x 5 = €**35,000**

DISAGGREGATED SOLUTION (HORIZONTAL MARKET)

Hardware: €20 x 30 units = €600 (capex)

Installation: €5,000 (capex)

Software cost: €5/year/unit (opex)

TCO FOR 5 YEARS: €20 x €30 + €5000 + €5 x €30 x €5 = €**6,350**

A complex software installation process, would discourage the user from adopting a software/hardware disaggregated solution, leading to a horizontal market failure. The school would miss an opportunity to save money by using a software solution that can be provided by the software manufacturer at marginal cost.

[8] Price estimation based on market research by expert contributing to this paper.

About the European DIGITAL SME Alliance

DIGITAL SME is the largest network ICT small and medium sized enterprises in Europe, representing about 20,000 digital SMEs across the EU. The alliance is the joint effort of national and regional SME associations from EU member states and neighbouring countries to put digital SME at the centre of the EU agenda.

DIGITAL SME members

BULGARIA, BASSCOM – Bulgarian Association of Software Companies,

BELARUS, INFOPARK

BELGIUM, Agoria

DENMARK, it-forum midtjylland

FRANCE, DIGITAL SME France (EBEN – Fédération des Entreprises du Bureau et du Numérique and ACEDISE – Association des Constructeurs Éditeurs Distributeurs Installateurs de Systèmes d'Encaissement)

GERMANY, BITMi – Bundesverband IT-Mittelstand,

IRELAND, SkillNet Ireland

ITALY, CNA - Comunicazione e Terziario Avanzato, Confederazione Nazionale dell'Artigianato e della Piccola e Media impresa,

Italian Digital SME Alliance (ASSINTEL Associazione Nazionale Imprese ICT, Blockchain Italia, CNA Milano, CONFIMI Industria Digitale, Digital Building Blocks, Unione Artigiani della Provincia di Milano, ANACAM). CLUSIT – Italian Association of Information Security

SPAIN, CONETIC – Confederación Española de Empresas de Tecnologias de la Información, Communicaciones y Electrónica,

LATVIA, GREECE, ROMANIA, **ALBANIA, BOSNIA AND HERZEGOVINA, BULGARIA, MONTENEGRO, SERBIA, KOSOVO, REPUBLIC OF NORTH MACEDONIA,** Balkan – Black Sea & Baltic ICT Clusters Network

UK, UKITA, United Kingdom IT Association

+32 28930235 office@digitalsme.eu www.digitalsme.eu
123, Rue du Commerce, 1000, Brussels, Belgium
VAT: BE0899786252 EU Transparency Register: 082698126468-52