POSITION PAPER

Brussels, 31 July 2020

Orgalim comments on the final report of the impact assessment study on internet-connected radio equipment and wearable radio equipment

1. EXECUTIVE SUMMARY

Orgalim, Europe's technology industries, would like to provide its views on the findings and conclusions of the impact assessment study on internet-connected radio equipment and wearable radio equipment, in particular concerning the policy options proposed and the recommendations for the way forward.

Orgalim members acknowledge the increase in the number and demand for connected devices on the market and the need to assess emerging security vulnerabilities in a robust manner. The final report highlights that the activation of delegated acts, relative to the protection of data and privacy, as well as protection from fraud, is the preferred option to address existing regulatory gaps in terms of protection of data and privacy, as well as protection from fraud. Orgalim believes that the proposed delegated acts would not deliver the intended protection goals, and at the same time, be incomplete in covering the aspect of cyber-security. A more holistic solution, such as an EU wide horizontal legislation covering cyber-security would be more effective in addressing current regulatory gaps.

The present position paper aims to focus on Orgalim's arguments against the activation of delegated acts for Articles 3(3) (d), (e) and 3(3)(f), providing an alternative proposal (in line with option 5) as well as a brief analysis (in the annex of the paper), of the recommendations made in the final report of the impact assessment study.

2. ORGALIM COMMENTS AND PROPOSAL

First of all, there is a lack of clarity as to how the objectives of **fraud** prevention and tackling misuse of network resources can be effectively addressed by a delegated act, given that there is no EU wide definition

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438

of fraud and that the term is almost exclusively used in national criminal law, nor a harmonised definition for network resources The impact assessment study refers to fraud as an abstract term without displaying realistic case-studies on fraud prevention. Without a sheer understanding of the internal and external situational context and the exploration of such case studies, a delegated act cannot address the fraud prevention effort in a suitable and effective manner. In addition without this clarity it will be difficult for standardisation activities to contribute in a meaningful manner to the regulatory objectives.

Morevoer, fraud prevention cannot be achieved on individual product level - a product needs to function in a secure system, otherwise it is not cybersecure. Our experience shows that 95% of all successful cyberattacks result from user negligence or error and not caused by lack of technical measures.

As regards **privacy**, most consumer concerns are already covered by the requirements of the General Data Protection Regulation (GDPR). The GDPR rules should first be implemented in full before deciding to adopt another regulatory measure aimed at addressing the same issues or concerns. Duplication of requirements should be avoided at all costs, as this may lead to inconsistent and/or conflicting rules, which are overall detrimental to a well-functioning single market.

We call on the European Commission to consider the following challenges connected to the activation of the two delegated acts:

- The delegated acts seem to address only wireless equipment, but regulatory gaps cannot be closed as long as wired equipment is excluded from the scope, which cannot be tackled under the Radio Equipment Directive alone.. On the other hand, a horizontal Cybersecurity legislation for networkable products could establish general European cybersecurity objectives, which are independent from the technical nature of the interface, and would therefore be more appropriate than delegated acts in closing current gaps in the RED.
- The responsibility for privacy and especially protection from fraud cannot be only the burden of the radio equipment manufacturer. Notably fraud by stolen or phished credentials cannot be prevented at the level of radio equipment itself.
- The activation of the acts delegated to the Art. 3.3 d/e/f may be inconsistent with Article 2 of Decision 768/2008/EC, which sets out the obligation to apply the principles of the New Legislative Framework when formulating legislation for the marketing of products and, where products are already subject to other legislation, to ensure consistency of all legislation concerning the same product.

Last but not least, the delegated acts under consideration would be incomplete in tackling European **cybersecurity** requirements. These would apply to one sector only (radio equipment) and to a limited set of cybersecurity aspects (data protection, privacy, fraud), whereas cybersecurity concerns are also relevant for non-radio equipment. Orgalim therefore urges the Commission to avoid proposing a patchwork of different pieces of legislation that focus on addressing the same cybersecurity issues.

As an **alternative proposal**, Orgalim supports a new **horizontal legislation covering the cybersecurity** of all networkable products which has the potential to successfully ensure the required level of protection and a secure operation of products, on the basis of a risk-based approach. This is compatible with the policy **option 5** which we strongly support. Furthermore, Orgalim recommends that basic cybersecurity requirements are proposed to establish essential cybersecurity goals, while the technical specifications are set out in relevant harmonised standards. Such a horizontal legislation and the voluntary certification framework of the Cybersecurity Act would complement each other

Annex I

1. *Recommendation 1 on the activation of the delegated acts*

Orgalim's main position on the delegated acts has been explained in the section above.

2. *Recommendation 2 - Bringing into scope of the delegated acts, all internet-connected radio equipment to strengthen security in terms of data protection and privacy as well as protection from fraud; with two possibilities: either from the outset, or incremental approach/ gradually bringing products into scope over time, on the basis of a risk assessment*

The European Commission should first identify the categories of equipment for which a delegated act would be necessary and sufficiently beneficial.

3. *European Commission to issue a standardisation mandate to the European Standardisation Organisations (ESOs) regarding the development of harmonised standards pertaining to both delegated acts.*

The ESOs already work on the issue of cyber-security and should continue to do so. However, there is an urgent need for more specific EU harmonised standards taking into account current available technologies. Orgalim does however fully support the recommendation 4 in terms of the need for ESOs to cooperate with industry to develop relevant harmonised standards.

Orgalim also agrees with the following recommendations:

- Avoiding duplication of costs between RED and other pieces of legislation, as this could lead to the duplication of conformity assessment procedures and costs of potentially contradicting requirements.
- Undertaking a study on the GDPR's on internet-connected radio equipment and wearables from a data protection and privacy perspective
- Identifying good practice sharing among manufacturers that already take their obligations seriously, in terms of security by design and default, and their data protection by design and default obligations

Orgalim is neutral towards recommendations 7 (*ENISA to carry out regular monitoring of new and emerging security vulnerabilities and threats, on behalf of the EC*) and 8 (*Radio Equipment Expert Group to provide a forum of regular discussions on how best to address security vulnerabilities in internet-connected radio equipment and wearable radio equipment - including the role of harmonised technical standards*), since these proposals can be implemented independently of the elaboration of delegated acts.