Centre for Strategy & Evaluation Services

Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment

716/PP/GRO/IMA/18/1133/10768 IMPLEMENTING FRAMEWORK CONTRACT 575/PP/2016/FC

Executive Summary

April, 2020

Centre for Strategy & Evaluation Services LLP
Westering House
17 Coombe Road
Otford, Kent TN14 5RJ
United Kingdom
E: enquiries@cses.co.uk
T: +44 (0) 1959 525122

1. Executive Summary

1.1 Objectives of the study to support an impact assessment

The study's purpose is to support an impact assessment (IA) to be produced by the European Commission. Specifically, the study objectives are to:

- analyse the different policy options - regulatory and non-regulatory - specified in the Tender Specifications to strengthen safeguards for internet-connected radio equipment (RE) and wearable RE as regards data protection and privacy and protection from fraud;
- verify whether a minimum level of "baseline" security requirements measures should be integrated into the Radio Equipment Directive 2014/53/EU (RED) through the activation of either one or both delegated acts pursuant to Art. 3(3)(e) and 3(3)(f) as a *"condition for market access for internet-connected radio equipment and wearable radio equipment";* and
- analyse the costs, benefits and impacts associated with the different options.

1.2 Methodological approach

The study was carried out between April 2019 and March 2020. The data collection tools were:

- **Desk research -** assessment of relevant EU legislation and wider literature pertaining to data protection and privacy, and protection from fraud of internet-connected RE and wearable RE;
- **Interview programme** - more than 70 interviews were carried out with relevant stakeholders, namely national and EU-level industry associations, manufacturers and other economic operators, market surveillance authorities (MSAs), national authorities, notified bodies (NBs), consumer associations, data protection authorities (DPAs), and other relevant stakeholders; and
- **Two online surveys (an Open Public Consultation (OPC) and a targeted consultation).** Whereas the OPC was open to all stakeholders, the targeted consultation was aimed at the stakeholders directly concerned. 42 responses were received to the OPC, and 56 respondents to the targeted survey.

In addition, three presentations were made to outline the methodology and to present study findings to the Radio Equipment Expert Group (RE EG). A virtual presentation was also made to the RED Administrative Cooperation Group (ADCO).

As regards data analysis, the stakeholder consultation feedback was analysed. This consisted of a combination of analysing interview notes, the feedback received through the two online surveys and an assessment of the 16 responses received to the Commission's online consultation undertaken in January - March 2019 as part of the inception impact assessment (IA).

2. Problem definition, identification and analysis of policy options

2.1 Problem definition

An assessment of the baseline situation was carried out across internet-connected radio equipment and wearables to assess the extent to which security vulnerabilities could be identified. Key findings were that:

- There is a rapidly growing number of internet-connected radio equipment (RE) devices and wearable RE on the European market;
- In the context of the Internet of Things (IoT), this trend is expected to increase even further in future, with an estimated 7.43 billion connected devices in the European Union (EU) by 2030. [1]
- As the number of such devices and products on the European market falling within the RED's scope has increased exponentially, this has brought into focus the lack of adequate safeguards to help prevent the penetration of internet-connected RE devices.
- Security vulnerabilities are present in many such products, for example due to the absence of minimum basic security functionality to protect users, such as authentication or encryption capabilities in chips, hardware and to ensure secure data transfer transmission of personal data via the internet.
- Security vulnerabilities were found to be especially problematic in consumer IoT devices, an important sub-category of internet-connected RE, as such devices often have a lower level of security and encryption compared with enterprise-grade devices (e.g. routers, laptops).
- Three main consequence of the penetration of internet-connected RE devices resulting from such security vulnerabilities were identified. Firstly, devices that had suffered security breaches could be cloned and/ or used mischievously or maliciously. Breaches could lead to unauthorised access to information about the location of a device or characteristics of its location (for example whether a home is occupied or not). Finally, and probably most importantly, breaches could lead to unauthorised access to personal and/or organisation information. This information could then be used in many untoward or fraudulent ways.
- Many security vulnerabilities and risks identified were found to be common across multiple different types of internet-connected RE and wearables RE, due to the risks of being directly internet-connected. Security vulnerabilities identified in the 802.11 wireless security standard (Wi-Fi) and other communications protocols (e.g. Bluetooth) necessitate the frequent updating of the associated security protocols and standards.
- In addition, security vulnerabilities were identified in specific types of internet-connected RE, as explored through the product-based case studies, which cover routers, laptops, smart toys, smart watches, smart TVs and security cameras and baby monitors.
- Evidence was also identified of increased frequency of cyberattacks globally in the past few years, and also growing sophistication and complexity of such attacks.
- There are also risks linked to RE devices and wearables that are indirectly connected to the internet, such as via Bluetooth. However, these are of a lower degree of magnitude in comparison with directly-connected devices, as an unauthorised third-party would have to be in relatively close physical proximity to be able to penetrate locally-connected RE devices / wearables.

[1] Tech4i2. 2016. Identification of the market for radio equipment operating in licence-exempt frequency bands to assess medium and long-term spectrum usage densities. SMART 2014/0012. https://publications.europa.eu/en/publication-detail/-/publication/9994777b-2ba9-11e6-b616-01aa75ed71a1

- There is also a risk of physical (offline) penetration of internet-connected RE, not only online penetration, and an attendant potential risk of data loss.
- Whilst there are many examples of security vulnerabilities, there are equally many different technical solutions available, as mapped by European Standards Organisations (ESOs) such as CENELEC and ETSI, which between them have identified approximately 170 relevant existing standards. Furthermore, industry has also developed many different technical solutions both at the level of individual firms and at industry sector level.

2.2 Identification and analysis of policy options

Four policy options were identified by the European Commission for the purposes of this study. Additionally, a fifth option was added to reflect suggestions by some stakeholders that a horizontal legislative approach to addressing security vulnerabilities in internet-connected RE and wearable RE could be effective. The different options analysed are:

- **Option 0 - Baseline scenario (status quo, default option) based on existing EU legislation** (e.g. GDPR, e-Privacy Directive, forthcoming e-Privacy Regulation).
- **Option 1 – A voluntary approach**
  - **Option 1.1 – Voluntary approach, such as industry self-regulation, and national governments promoting awareness of consumer IoT security.**
  - **Option 1.2 – Voluntary measures to support the implementation of a regulatory approach.** Non-mandatory accompanying measures, e.g. awareness-raising measures, development of (voluntary) sectoral codes of practice on data protection and privacy (e.g. Art. 40 / 41 of the GDPR).
- **Option 2 – Adoption of a delegated act based on Article 3(3)(e) - safeguards to ensure data protection and privacy of users and subscribers.** Baseline security requirements as a condition for market access.
- **Option 3 – Adoption of a delegated act based on Article 3(3)(f) - ensuring protection from fraud**. Baseline security requirements as a condition for market access.
- **Option 4 – Adoption of two delegated acts based on Articles 3(3)(e) and 3(3)(f).** The requirements in both Articles 3(3)(e) and 3(3)(f) would have to be demonstrated to secure market access.
- **Option 5 – Horizontal approach - development of a mandatory Cybersecurity Act**. Over the medium-term, the possibility that an overarching regulatory approach could help to avoid regulatory divergence between wireless and wired products.

The findings from the analysis of policy options are structured around each option:

2.2.1 Policy Option 0 – relying on existing EU legislation.

A regulatory gaps analysis was undertaken to ascertain the extent to which existing EU legislation provides adequate safeguards to ensure data protection and privacy, and protection from fraud. The findings were that:

- There is already significant EU legislation in place to ensure safeguards for data protection and privacy through the GDPR and e-Privacy Directive (e-PD) respectively. These will be strengthened in future through the adoption of the e-Privacy Regulation (e-PR).
- The GDPR is already applicable to manufacturers designated as data controllers prior to internet-connected RE being placed on the market. For example, Art. 25 (data protection by design and default) and Art. 24 (putting in place organisational and technical measures to ensure data protection and privacy) of the GDPR already requires consideration of such issues by manufacturers (unless they are not intending to collect any personal data).
- The e-PD covers the transmission of personal data over communications networks, and once the e-PR is adopted, will extend protection to communications data held on the device itself, and transmitted via the internet.

- The majority of manufacturers therefore fall within the GDPR's scope as they collect personal data in their capacity as data controllers, and responsibility has also been extended across the value chain to data processors (although complex value chains mean it may not always be fully transparent and clear who is processing personal data, given the complexity of value chains).
- However, the study has nevertheless identified several regulatory gaps that could warrant the activation of the two delegated acts under Article 3(3)(e) and Article 3(3)(f).
  - Under the RED's essential requirements, MSAs cannot presently remove products from the market (or prevent them being placed on the market) unless the delegated acts are activated.
  - Instead, MSAs and consumers are reliant on data protection authorities issuing fines under the GDPR. Once the future e-PR has been aligned with the GDPR sanctions regime, it will also be possible for fines to be issued relating to the transmission of personal data via communications networks). Therefore, insecure internet-connected RE and wearable RE may legally remain on the European market, as there is presently no explicit requirement for minimum security functionality to be integrated.
  - This omission in the regulatory enforcement toolbox risks undermining the Single Market, as some national authorities have used a patchwork of different types of national legislation to remove insecure products from the market.
  - Moreover, EU industrial product legislation does not presently make an explicit connection between product safety and security. This is not surprising as the body of legislation pre-dates the advent of the IoT and the trend towards smart products with a radio device integrated to enable them to be internet-connected.
  - A further gap is that if a manufacturer (or OEM supplier) of internet-connected radio equipment and wearables does not intend to collect and / or process any personal data, they would not be deemed to be a "data controller" under the GDPR.
  - Therefore at the product design and engineering stages, if there is no intention to collection any personal data (including personal identifiers), the manufacturer is not then under any legal obligation to consider such issues. There is consequently a risk that the manufacturer not intending to collect any personal data may overlook security considerations (relating to data protection and privacy).
  - Further down the value chain, there could be a risk that such internet-connected RE generates personal data collected by third parties, such as service providers. It may then be unclear within the value chain who is the responsible data controller.
  - Presently, no EU legislation explicitly addresses the issue of ensuring protection from fraud in the context of industrial products.
  - The problem of fraud being perpetrated by third-parties accessing personal data via unlawful breaches of internet-connected RE devices, for instance through hacking, ransomware and malware attacks and cryptojacking has been getting steadily worse.
  - Accordingly, the study found that users of internet-connected RE and wearable RE therefore need greater legal protection to prevent devices and other types of RE from being at risk of online penetration in the first place. This could be achieved in many cases through authentication and encryption.
  - Whilst national criminal legislation tackles the problem of fraud, it does so retrospectively. Moreover, such legislation is a national competence, with regulatory divergence meaning that there is uneven legal protection. There was found to be a strong argument that Internet-connected RE and wearable RE need a harmonised legal framework as many products placed on the European market are sold in multiple countries or across the EU-27 as a whole. This

would also help to strengthen legal protection for users (consumers, professional users).

In conclusion, EU legislation already provides some safeguards for users of internet-connected RE and wearable RE, but only in respect of data protection and privacy, and not as a condition of market access. There remain some regulatory gaps, such as the inability of MSAs to remove products from the market if they don't integrate adequate security safeguards to ensure minimum security functionality. Therefore, reliance on existing EU legislation would only be partially effective. As will be shown in policy options 2, 3 and 4, relying on existing EU legislation is sub-optimal due to the outstanding regulatory gaps mentioned above.

2.2.2 Policy Option 1 – a voluntary approach

- The benchmarking analysis identified examples of a voluntary approach having been implemented by some stakeholders through the development of codes of practice and good practice guidance *(e.g. ENISA at EU level, NIST in the US and DCMS in the UK).*
- The development of such guidelines could be useful in setting baseline security requirements and in promoting a culture of security among manufacturers of internet-connected RE and wearable RE and encouraging further attention to data protection and privacy / protection against fraud from the outset of design, engineering and manufacturing processes.
- A voluntary approach has already been tried in some jurisdictions (e.g. the UK), but has not been viewed as having been successful enough to exclude the possibility of regulation in future.
- Voluntary approaches could also provide a useful testing ground for possible subsequent mandatory approaches. For instance, voluntary certification schemes being developed under the Cybersecurity Act (CSA) with close industry participation could be useful as regards developing testing approaches, standards and certification that could be useful if the delegated acts were to be activated.
- Industry codes of practice and guidance on product security to ensure adequate safeguards for data protection and privacy and protection from fraud could also potentially support the implementation of a regulatory approach in future (e.g. PO2, PO3 and PO4).

2.2.3 Policy Options 2, 3 and 4 – a regulatory approach

- A regulatory approach was identified as being the most effective option as this would close the regulatory gaps identified (see PO0).
- However, there are divergences in stakeholder views as to whether a regulatory approach is necessary. Whereas most national authorities, MSAs and consumer associations were in favour, some industry stakeholders and firms were either against, or said that it could impose some additional costs.
- Representatives from the cybersecurity industry argued that the delegated acts could be implemented using technical solutions that need not always be costly, such as requiring authentication to access an IoT device, and avoiding recourse to either default or low strength passwords.
- Among industry, there were concerns around compliance costs, the coherence of addressing RE (wireless) only not wired, and also a concern that if data protection and privacy were to be tackled through the RED in addition to the GDPR and the e-PR, this could risk some duplication in costs.
- However, there would be a differentiation between the RED and existing EU legislation as under the RED, data protection by design and default would become a condition of market access. This would mean that MSAs could remove products post-market placement if internet-connected RE and wearable RE were found to be non-compliant.
- Stakeholders were not always able to provide feedback on the costs, benefits and impacts of a

regulatory approach, as they requested further details as to what minimum security requirements would be incorporated into the delegated acts, and which technical solutions would be integrated into the development of future possible harmonised technical standards before they could give a clearer response.

- Activating Article 3(3)(e) could help to complement existing protection under the GDPR and the e-PD by making it more explicit that manufacturers must design products that integrate baseline security requirements as a pre-condition for market access.
- Arguably, a further benefit is that by making all manufacturers of internet-connected RE and wearable RE directly responsible for ensuring data protection and privacy (even if they do not intend to collect personal data themselves), it could overcome uncertainty within the value chain as regards how GDPR compliance applies to manufacturers, technology providers, and third-party service providers.
- Policy option 3, the activation of Article 3(3)(f) would have the advantage that as protection from fraud is not presently covered in EU legislation, this would address a regulatory gap that national criminal legislation is presently only able to address retrospectively.
- Among the advantages of having an essential requirement on protection from fraud are improved resilience against cyber-attacks, and helping to combat different types of fraud (e.g. financial, identity theft).
- However, Art. 3(3)(f) lacks a definition of fraud in the legal text of the RED and one would need to be developed that is sufficiently clear but broad enough to accommodate the ever-changing nature of online fraud (including that perpetuated through the penetration of internet-connected RE and wearable RE). Examples identified are *inter alia* 1) Near Field Communication (NFC) related frauds (contactless payments) 2) authentication-related frauds and 3) ransomware and cryptojacking.
- Although some stakeholders questioned whether fraud could be addressed effectively through the RED, criminal law addresses the problem retrospectively. If essential requirements were to be activated RED could prevent data breaches from occurring in the first place. Prevention of breaches will stop the main undesirable consequences of device fraud, identity fraud and location information breaches.
- Stakeholders were unclear how specific technical measures could be taken to ensure protection from fraud, as opposed to safeguards to ensure data protection and privacy, given the interconnectedness between Art. 3(3)(e) and Art. 3(3)(f).
- Whilst some security measures – and technical solutions - could explicitly target fraud prevention, if online (and / or physical) penetration of internet-connected RE and wearable RE devices is prevented through security measures such as authentication and encryption, that would solve the great majority of current problems, be they relating to data protection and privacy, fraud or both.
- In order to close regulatory gaps, Policy Option 4 – activating both Delegated Acts – was found to be the most effective policy option. From a coherence perspective, activating both DAs would be more effective than activating one alone.
- Option 4 is advocated provided that a proportionate and risk-based approach is adopted to developing the detailed text of the delegated acts, and of the accompany technical solutions and future harmonised standards that could be used to implement the DAs.
- Option 4 would provide the ability to take non-compliant products off the market and act to prevent data breaches of internet-connected RE and wearable RE from occurring that could lead to a loss of personal data, privacy being compromised or fraud being perpetuated. There could be broader benefits from a cybersecurity perspective of tackling these issues by extending the RED's essential requirements (i.e. basic security functionality in internet-connected RE will not only

prevent personal data losses and fraud but also prevent a broader range of problems).

2.2.4 Policy Option 5 – a horizontal approach

- Some industry associations and individual manufacturers perceived that a differentiated regulatory approach between wireless products falling under the RED's scope and wired products could undermine the level regulatory playing field principle.
- However, circa 70% of internet-connected products are wireless and integrate RE, and therefore, a significant percentage of the total market would be covered.
- Medium term, it was suggested by many stakeholders that a horizontal regulatory approach across different types of industrial products to ensure product security not only safety could be considered.
- However, this would go beyond the scope of the proposed extension of the RED's essential requirements as this would cover cybersecurity in a broader sense rather than data protection and privacy and protection from fraud alone.

2.3 Costs and benefits

A **Cost-Benefit Assessment (CBA)** was undertaken which sought to quantify, to the extent possible, the costs of the different policy options, with a focus on the preferred policy option identified of going ahead and activating both delegated acts.

Some **costs data** was obtained on the costs of compliance of internet-connected RE were the delegated acts to be activated. A key finding was that the costliest administrative cost type was testing, with costs ranging from €5,000-10,000 for a simple product, €20,000-25,000 for a more complex product, and €50,000 or more for a product that embeds a lot of software and requires software checking. As regards administrative burdens for regulatory authorities and market surveillance authorities involved in testing, costs will depend on whether they can carry out testing internally, or require a third-party. If the latter, costs may be in the order of €10,000-20,000 per product for a more thorough test or €5,000 for a couple of days of very basic tests.

Whilst economic operators perceived going ahead with the activation of the two DAs as being costly in the targeted consultations, in the interview programme, there was a recognition that manufacturers already take the security of internet-connected RE very seriously, and therefore, there could be high Business as Usual (BaU) costs of circa 50-70% in many cases. However, an uncertainty is that it is unclear how far BaU costs would be applicable, as this depends on how far previous product testing results could be used to demonstrate conformity with the essential requirements in the RED's Article 3(3)(e). This is less the case for Article 3(3)(f) as there are fewer specific standards to prevent fraud, however, often security measures such as requiring authentication and using encryption could help to prevent a combination of data breaches, privacy and strengthen fraud protection in parallel.

Aggregating costs across all categories of internet-connected RE and wearable RE is problematic at this stage. In particular, there were major challenges in obtaining estimated costs and it was seen as difficult to provide any estimates until various elements have been made clearer, such as: 1) the detailed requirements for economic operators under the RED 2) the extent to which future these obligations for economic operators would differ from existing requirements under the GDPR and voluntary certification schemes under the Cybersecurity Act[2], 3) whether technical standards and minimum baseline security requirements will be generic (such as the ETSI Consumer IoT standard) or product specific and 4) whether all categories of internet-connected RE and wearable RE would be brought within scope, or only those identified as being 'high-risk'.

[2] However, this concern could be overcome if the harmonised standards drafted for the new essential requirements contain relevant technical requirements that have been identified in the voluntary certification under the CSA.

As regards **benefits**, strengthening security requirements for internet-connected RE (data protection and privacy and protection from fraud) may have some benefits for European manufacturers in the medium to longer-term. The reason for this is that several other jurisdictions are already investigating whether certain types of products – often consumer IoT-related – could be subject to regulatory requirements in future. Europe could benefit from first-mover regulatory advantage, as it already enjoys some competitive advantages globally in the cybersecurity field.

Some benefits could be quantified by using benchmarks obtained from secondary literature regarding firstly the impact of enhanced consumer trust on sales and secondly, willingness to pay for more secure products. The research found that across internet-connected RE as a whole, there might be an increase in sales of circa 5-10% due to enhanced consumer trust in the security of products, devices and apparatus falling under the RED. Additionally, consumers appear willing to spend 20%-40% more for secure products in consumer preference studies on internet-connected IoT. The study team's assessment was that this is rather high, and relates to users choosing between a low-cost, poor-security product with less functionality compared with a medium-cost product with improved security and functionality. A more realistic estimate is that users of internet-connected RE might be willing to pay 10%-20% extra for more secure products.

2.4 Impacts

A review of the socio-economic impacts associated with the different policy options was undertaken. This concentrated on the preferred policy option identified, i.e. the activation of the two DAs.

The main **economic impacts** identified were (1) scope for improved functioning and harmonisation of the Internal Market in RE (2) strengthened resilience against fraud and avoidance of economic loss to consumers and industry of fraud (3) strengthened competitiveness of EU industry by focusing on cybersecurity as a competitive strength and (4) perhaps of greatest significance, increased sales of internet-connected RE and a shift to higher value products due to security concerns. Evidence for the latter comes mainly from consumer 'stated preference' and WTP studies.

The main **social impacts** identified are firstly increased security of EU citizens when using internet-connected RE and wearable RE, strengthened protection of their personal data and privacy to complement existing EU legislation (e.g. GDPR, e-PD), strengthened consumer trust in the Digital Single Market, and improved cyber-resilience (given that many EU citizens have limited cybersecurity awareness and skills to prevent data loss and fraud.

As regards the **environmental impacts**, in the context of the circular economy, there are potential benefits in removing insecure internet-connected RE and wearable RE products and devices from the market as these will tend to be at the cheaper end of the market and not designed to last very long. Encouraging manufacturers in Europe and globally to invest in security could encourage them to shift up the value chain and make more durable products, thereby improving environmental sustainability and reducing electronic equipment waste.

3. Conclusions and Recommendations

The key study conclusions and recommendations to support an impact assessment are now outlined.

3.1 Overall conclusions

- Stakeholders recognise the problem of security vulnerabilities in internet-connected RE (including wearables). However, there are divergent views as to how best to address the problem.
- There was support for the principle of the integration of security by design and default principles into the design, engineering and manufacturing of internet-connected RE and wearable RE, which could build on existing legal requirements in the GDPR regarding data protection by design and default.
- As regards the adequacy of the existing EU regulatory framework, whereas the GDPR and e-PD already partially incorporate safeguards for data protection and privacy, there remain some regulatory gaps, notably: (1) the inability to remove insecure internet-connected RE from the market (2) the fact that not all manufacturers explicitly set out to collect and process data and therefore, not all manufacturers are designated data controllers.
- It is too early to assess the effectiveness of recent EU legislation to strengthen data protection and privacy, especially the GDPR, but also the alignment of the e-Privacy Directive (e-PD) with the GDPR through the e-Privacy Regulation (e-PR), which has not yet been adopted.
- There is an absence of a legal framework to combat fraud at EU level. Activating the essential requirements in the RED for internet-connected RE would be innovative, given the prevalence of online fraud. However, only the prevention of device penetration for RE would be covered, and it should be recalled that a lot of online fraud is committed via online scams post-product placement i.e. via internet browsers, email scams and phishing etc. which are outside the RED's scope.
- Whereas more than one policy option is viable, a regulatory approach activating both Article 3(3)(e) and 3(3)(f) would be the most effective means of closing outstanding regulatory gaps. This would cover the estimated 70-80% of the market that is wireless, as opposed to wired.
- Although there was some stakeholder support for a horizontal law to provide a more comprehensive approach to ensuring the security of internet-connected RE placed on the European market, this was only viewed as being realistic in the medium term. Whereas the delegated acts are already mentioned in the 2014 RED, possible legislation on cybersecurity might take 5-10 years to develop. Activating the DAs would therefore be a positive step in the right direction even if wired products would remain unregulated.
- If the two above-mentioned delegated acts were to be activated, a check of ongoing coherence of the overall legislative framework would be needed.
- As regards how a regulatory approach might be implemented, there are already many technical solutions to build upon, were the two delegated acts to be activated. For example:
    - The concept of minimum security baseline requirements appears to enjoy stakeholder support. Examples of such requirements are being developed by ENISA, NIST, ETSI, CEN / CENELEC and other stakeholders. This concept could provide a means of developing a proportionate, risk-based approach as regards product-specific technical requirements;
    - Authentication and encryption could solve up to 80-90% of identified security vulnerabilities relevant to ensuring improved safeguards for data protection and privacy and protection from fraud; and

- The European Standards Organisations (ESOs) are already engaged in working on strengthening the security of internet-connected RE and wearable RE. They could help to meet the challenge of operationalising the two delegated acts by contributing to the development of technical requirements following a minimum security baseline requirements approach.

- However, there is a concern as to whether there is adequate capacity to introduce mandatory requirements across all categories of internet-connected RE simultaneously. Therefore, an incremental, risk-based approach could be adopted to the implementation of the DAs, as some products were found to carry higher levels of risk than others.
- The ESOs could play a role in assessing which types of internet-connected RE should be prioritised and brought within the scope of Art. 3(3)(e) and Art. 3(3)(f) on a phased basis. However, the picture is complex, as some internet-connected RE products / devices may be higher risk, but already have a greater level of industry/ sub-sector maturity in addressing security vulnerabilities at product level.

3.2 Recommendations

Recommendation 1: The preferred policy option (Option 4) would be to activate both delegated acts under Article 3(3)(e) and 3(3)(f) of the RED. This would strengthen the RED's essential requirements to close regulatory loopholes, and making an explicit link between product safety and security (data protection and privacy and protection from fraud).

Recommendation 2: All internet-connected RE should be brought within scope to strengthen security in respect of data protection and privacy and protection from fraud. However, there are two options for the Commission in implementing the future delegated acts under the above-mentioned Articles.

- Under the first Option, all internet-connected RE devices and products should be brought within the scope of the delegated acts from the outset.
- Under the second Option, an incremental approach should be adopted based on activating the two DAs followed by gradually bringing more products within scope over time, based on a risk-based assessment. *Reference should be made to the product-based assessment of security vulnerabilities, risks and the likelihood of these occurring.*

Recommendation 3: The European Commission should issue a standardisation mandate to the European Standardisation Organisations (ESOs) pertaining to the two delegated acts. Mapping by the ESOs to date (e.g. ETSI, CENELEC) suggests that there are already a lot of technical solutions to build upon, although there are also challenges as some existing standards relate to generic security measures rather than product-specific solutions.

Recommendation 4: The ESOs should work closely with industry in developing harmonised technical standards and build on existing technical solutions and industry standards where these already exist. This would minimise potential future compliance costs for industry of ensuring safeguards relating to the security of internet-connected RE and wearable RE, with a focus on data protection and privacy and protection from fraud.

Recommendation 5: The requirements under the RED Art. 3(3)(e) and Art. 3(3)(f) will need to be clearly delineated in the drafting of the delegated acts, and supported by a clear explanation as to how in the case of Art. 3(3)(e) coherence will be ensured with existing legal obligations in respect of data protection and privacy in EU legislation (e.g. the GDPR, and the e-PD / e-PR). Clear definitions are provided in the GDPR in respect of key concepts such as data protection, privacy, consent, data subject, etc. These already help to provide protection for users of internet-connected RE, and these definitions could lay the basis for the development of the activation of the delegated acts, which would need to be aligned with the GDPR.

Recommendation 6: Duplication of costs between the RED and other EU legislation should be avoided. To assuage manufacturers' concerns regarding administrative compliance costs (especially due to testing and conformity assessment procedures), the extent to which compliance processes carried out by manufacturers under existing legislation and under voluntary certification schemes within the CSA could be used to demonstrate compliance towards the RED's essential requirements under future harmonised technical standards should be made clear.

Recommendation 7: Regular monitoring of new and emerging security vulnerabilities and threats should be carried out by ENISA on behalf of the European Commission. ENISA already has experience in monitoring and mapping security vulnerabilities. ENISA, and possibly also working groups from relevant national authorities, could advise the Commission on whether harmonised standards still represent the state-of-the-art.

Recommendation 8: Regular discussions on how best to address security vulnerabilities in internet-connected RE and wearable RE - including the role of harmonised technical standards - should take place regularly within the framework of the Commission's Radio Equipment Expert Group.

Recommendation 9: Greater attention should be given to monitoring the implementation and strengthening the enforcement of existing EU legislation with the potential to contribute to regulatory objectives linked to Article 3(3)(e) and 3(3)(f) of the RED to ensure ongoing coherence. There should be a focus on further strengthening compliance by manufacturers of internet-connected RE and wearable RE with certain Articles of the GDPR that are especially relevant, such as Art. 25 (security by design / default). If DPAs were to issue fines to non-compliant manufacturers, then over time, a combination of such fines and case law could help to further embed compliance.

Recommendation 10: A study on the GDPR's on internet-connected RE and wearables from a data protection and privacy perspective should be undertaken in future. This would help to develop a better evidence-based understanding as to how far GDPR has already led to changes in business processes and the embedding of security features in products at the design, engineering and manufacturing stages to ensure higher levels of data protection and privacy.

Recommendation 11: Good practice sharing among manufacturers that already take security by design and default, and their data protection by design and default obligations seriously (including their integration into business processes) should be identified, collected and shared in the form of good practice guidance.