European Commission

INCEPTION IMPACT ASSESSMENT

Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to share any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	Commission delegated regulation on Internet-connected radio equipment and wearable radio equipment
LEAD DG – RESPONSIBLE UNIT	DG GROW, C3
LIKELY TYPE OF INITIATIVE	Legislative (Delegated Regulation)
INDICATIVE PLANNING	Q4 2019
ADDITIONAL INFORMATION	-

The Inception Impact Assessment is provided for information purposes only. It does not prejudge the final decision of the Commission on whether this initiative will be pursued or on its final content. All elements of the initiative described by the Inception Impact Assessment, including its timing, are subject to change.

A. Context, problem definition and subsidiarity check

Context

Large numbers of radio equipment are used on a daily basis, not only by adult consumers or professional users, but also by vulnerable users and children. For the latter users, in December 2016, the Norwegian Consumer Council looked at the terms and the technical features of selected radio-connected toys[1]. The findings show a possible lack in the protection of children's rights to privacy and security. These toys are "smart" and can interpret speech, making them capable of interacting with the child. They may also record not only photos, videos, geolocalisation data, data linked to the play experience, but also heartrate, sleeping habits or other biometrical data, according to the integrated sensors. To enable these new features, these products are equipped with speakers, and microphones and other sensors, and they can be connected to phones/tablets or directly to the internet. The ability of these products to record, store and share information raises concerns about safety, security, privacy and social development.

In the same way, some smart wearable devices allow to use an application to keep in touch with and/or track the location of the users. A specific example of these products are smartwatches intended for children. These devices may also contain a SIM-card, allowing children to connect to the Internet through mobile-networks or a Wi-Fi connection. In its most basic form, the smartwatch functions as a mobile phone or a tablet attached to the wrist, which connects to the parents' phones through an app. The use of a combination of GNSS and Internet data can also allow real-time location tracking and direct communication. They can also store names, photos and geolocation data.

Problem the initiative aims to tackle

Through a few simple steps, as shown in the report of the Norwegian Consumer Council, a stranger can take control of the watch without having physical access to it, and eavesdrop on and communicate with the child. They might be able to track the child as it moves or fake the location of the child. The report also shows that some of these toys can also advertise products when interacting with the child, which may not be in line with the expected transparency of this kind of products. For this reason, its outcome has become part of a call for action from the European Consumer Associations[2].

However, connected toys and smartwatches are just a part of a broader sector, which may present similar risks.

[1] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

[2] http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

Baby monitors, smart appliances, smart cameras and a number of other radio equipment are also example of equipment at risk of hacking and of privacy issues. In 2016 in EU28, there were nearly 125 mobile phone subscriptions per 100 inhabitants[3]. Mobile phones and other devices connect to the Internet via a mobile network using a SIM card. The later include certain laptops, dongles, alarm systems, home automation systems. Many other smart products connect to the Internet using Wi-Fi (e.g. home automation centrals, web cameras, TV sets, etc.).

Consumers, experts and international organizations are concerned about the ways in which personal information and data are collected and shared[4] and how these data may be used for illicit practices. Also EU Member States have highlighted to the Commission that given the increasing risks in the area of cyber security due to the increase of connected products, it would be beneficial to apply a minimum level of security to all radio equipment directly or indirectly connected to the internet[5]. This would imply requirements that such radio equipment supports the protection of personal data and privacy and prevents loading incompatible or malicious software.

Manufacturers of internet-connected devices, most of which are expected to be part of the Internet of Things (IoT) are being requested to minimize data collection, perform privacy assessments, and implement privacy and security standards and/or certify them, on top of the traditional product safety. In fact, the IoT development brings the need for improved digital security not only for individual users but also for society as a whole. This initiative will consequently focus on (1) wearable radio equipment and (2) internet-connected radio equipment, i.e. *radio equipment intended to be*

(i) connected (directly or indirectly) to or

(ii) controlled through

the internet.

Numerous Member States and Consumer Associations raised the attention to these issues to the EU Institutions and also to the members of Telecommunications Conformity Assessment and Market Surveillance (TCAM) Committee as well as the TCAM Working Group.

Basis for EU intervention (legal basis and subsidiarity check)

The Radio Equipment Directive (RED), which is based on Article 114 of the TFEU, establishes a regulatory framework for placing radio equipment on the market, ensuring a Single Market for radio equipment. The scope of the RED covers devices that use the radio spectrum for communication and/or radio determination purposes. All internet-connected wireless devices (e.g. that are part of the Internet of Things) fall under this Directive.

Articles 3(1) and (2) of the RED set out the essential requirements that radio equipment shall respect. Those relate to health and safety, electromagnetic compatibility and radio spectrum. Article 3(3) provides the basis for further delegated regulation governing additional aspects, empowering the Commission to adopt delegated acts in order to specify which categories or classes of radio equipment are concerned by each of the requirements set out in its points (a) to (i). The requirements referred to in points (a) to (i) relate to interoperability, emergency services, software, fraud, accessibility, privacy, personal data and misuse.

Certain RED requirements could be made applicable via delegated acts to improve the digital safety/security/privacy at equipment level for certain categories of radio devices. More specifically, Article 3(3)(e) and (f) refer to the features of safeguards for privacy and against fraud, respectively.

The Commission is establishing the Expert Group on Radio Equipment E03587 in order to provide expertise with respect to any possible initiative pursuant Articles 3(3)(e) and (f) of the RED.

The objectives can be better achieved at EU level, rather than by the Member States alone, due to:

[3] The EU in the world — 2018 edition, p. 116, Figure 10.5 https://ec.europa.eu/eurostat/documents/3217494/9066251/KS-EX-18-001-EN-N.pdf/64b85130-5de2-4c9b-aa5a-8881bf6ca59b

[4] https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826 and specifically https://www.oecd-ilibrary.org/docserver/7c45fa66-en.pdf?expires=1537876141&id=id&accname=guest&checksum=9B6F059A453E382BCD1C3A08A03EFB24

[5] E.g. TCAM WG (12)08 and TCAM WG (14)07

- The delegated powers conferred to the Commission by the RED;
- The need for harmonised standards and interoperable solutions;
- The global nature of industrial value chains, as well as the activity of global competitors working across the markets.

Therefore, the EU can adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, the proposed measures will not go beyond what is necessary in order to achieve those objectives.

The following provisions would be the legal basis for one or more Commission acts related to this initiative:

Article 3 (3)

Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements: […]

(e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
(f): radio equipment supports certain features ensuring protection from fraud. […]

The Commission shall be empowered to adopt delegated acts […] ***specifying which categories or classes of radio equipment are concerned*** *by each of the requirements set out in points (a) to (i) of the first subparagraph of this paragraph.*

Any delegated act under Article 3(3)(e) will activate the application of the essential requirements set out in Article 3(3)(()(e) for these categories of radio equipment. As a result, such a delegated act will not affect the coherence with

(i) the General Data Protection Regulation (EU) 2016/679 (GDPR) and
(ii) the Directive on privacy and electronic communications (Directive 2002/58/EC, "ePD"), notably Article 5(3) on the storing of information or accessing of information already stored on terminal equipment, and other provisions where relevant.

The **GDPR** and the **ePD** set forth rules on data protection and privacy protection. Unlike RED, they do not concern market access of products. Currently, Member States can only rely on possible national acts to withdraw products that may negatively impact data protection and privacy from the market and therefore there is a need for specific action to have a solid harmonised legal basis for this purpose. A delegated act pursuant Article 3(3)(e) of the RED would allow the essential requirement of safeguards to ensure that the personal data and privacy are protected to be demonstrated a product in question can be placed on the market.

The EU law already provides that any information addressed specifically to a child will need to be adapted to be easily accessible, using clear and plain language (Art. 12 of the GDPR). In addition, other rules of the GDPR are also relevant in this context, such as Article 25, which mandates data protection by default and by design and Article 32, which mandates security of processing.

Another piece of relevant legislation is the proposed **Cybersecurity Act**[6], which is expected to establish, when adopted by the co-legislators, voluntary certification scheme for showing cybersecurity resilience. Subject to future stakeholder consultations, a relevant certification scheme may be established with cybersecurity requirements related to the objectives of the delegated act i.e. safeguarding data protection, privacy and ensuring protection from fraud.

The activation of one or more delegated acts pursuant Article 3(3)(e) and/or (f) of the RED, will also entail that, if Member States identify a radio-connected product presenting a serious risk related to personal data, privacy or fraud, a notification should be submitted through the Rapid Alert System for dangerous non-food products (RAPEX)[7]. As it is established in articles 1, 16, 20 and 22 of Regulation 765/2008[8], market surveillance

[6] Proposal for a Regulation Of The European Parliament And Of The Council On Enisa, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM/2017/0477 final - 2017/0225 (COD)

[7] https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm

[8] Regulation 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products

authorities should ensure that products fulfil the specific requirements established in EU legislation relating to technology, health and safety, environment or any other aspect of public interest protection (which in this case would be the protection of personal data, privacy and fraud).

In addition to protecting consumers, the notification through the Rapid Alert System of radio-connected products not respecting the essential requirements established on the delegate act((s) will also ensure that the free movement of these products in the Single Market is not restricted to any extent greater than what is allowed under EU legislation.

Also the revision of the **Goods Package**, when adopted by the co-legislators, is expected to strengthen controls by national authorities to ensure that products are safe and comply with the rules. Equipment failing to meet the requirements for safety or the quality expectations not only risks to endanger consumers, but also puts compliant businesses at a competitive disadvantage. The draft Regulation on **Compliance and Enforcement** will help create a fairer internal market for goods, through fostering more cooperation among national market surveillance authorities. This will include sharing information about illegal products and ongoing investigations so that authorities can take effective action against non-compliant products. The Regulation will also help national authorities to improve checks on products entering the EU market.

Consequently, possible delegated acts pursuant Article 3(3)(e) and/or (f) of the RED would fit in the implementation of the Digital Single Market and in providing legal certainty for both manufacturers and consumers (including children), addressing some of the technological challenges of new technological development. In particular, they would allow to (i) cover *ex-ante* the protection of the personal data and privacy of the user and of the subscriber and the protection from fraud, (ii) keep the current framework and conformity assessment procedures for placing radio equipment on the market and (iii) provide a benchmarks for any additional voluntary scheme that may be put in place (e.g. by the Cybersecurity Act). These delegated acts would consequently complement the legal framework, preserving its coherency and strengthening its effectiveness.

It is also finally noted that the radio equipment in the scope of this initiative may fall in the scope of a parallel initiative on the upload of new software into radio equipment[9] pursuant Articles 3(3)(i) and 4 of the RED[10]. This aims to ensure that the level of protection of privacy and against fraud at the moment of placing radio equipment on the market would be maintained at the upload of new software also after the initial placing on the market, i.e. throughout its lifecycle. The certainty of the preservation of the compliance of radio equipment throughout its life-cycle is a key feature to ensure that new technologies, whose safety and security might be impacted by the upload of new software, can be used by consumers with trust.

B. Objectives and policy options

The overall objective of this initiative is to ensure an adequate level of security for internet-connected radio equipment and wearable radio equipment at the moment of placing on the market.

The following policy options and their effects for potentially affected parties (e.g. manufacturers, consumers, National Authorities) will be analysed:

- **Option 0,** baseline scenario: a situation in which manufacturers are not obliged to implement any specific measures as it is currently the case.
- **Option 1,** a situation whereby the industry self-regulates to implement the existing legislation which protects personal data, the confidentiality of telecommunications, security and protection against fraud.
- **Option 2,** adoption of a delegated act pursuant Article 3(3)(e). This will require that radio equipment incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected, also as a tool to enhance the cybersecurity of these products, and this requirement will have to be demonstrated for the purposes of market access.
- **Option 3,** adoption of a delegated act pursuant Article 3(3)(f).This will require that radio equipment incorporates certain features ensuring protection from fraud, also as a tool to enhance the cybersecurity of these products, and this requirement will have to be demonstrated for the purposes of market access.

[9] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-6621038_en

[10]

- **Option 4,** adoption of a delegated act pursuant both Articles 3(3)(e) and (f). In this case, both requirements in Options 2 and 3 will have to be demonstrated for the purposes of market access.

C. Preliminary assessment of expected impacts

As radio equipment and technologies are a key part of the forthcoming deployment of new technological developments and/or environments[11], this initiative will take into due account all the possible related aspects, such as the impacts for the society (e.g. consumers and economic operators), the national Authorities, the common market access conditions and the implementation of, or synergies with, additional pieces of EU legislation, in particular those relating to (cyber)security, data protection and privacy.

Likely economic impacts

The following economic impacts will be analysed:

- Operating costs of and administrative burden on manufacturers of specific categories of radio equipment when/if new requirements are made mandatory;
- Competitiveness of EU industry also in terms of fair competition. Industrial stakeholders potentially affected by this initiative are manufacturers of (1) internet-connected and (2) wearable radio equipment. Since some manufacturers could be SMEs, the initiative will include SMEs in their analysis. In any case, manufacturers respecting the highest privacy and anti-fraud expectations are predicted not to be affected by this initiative, which will mostly impact those manufacturers with a reduced attention to the security of their products;
- Functioning and harmonisation of the Internal Market, also with respect to the prevention of National Regulations to be put in place, hence facilitating economic operators to presume conformity of their products with the law;
- Stimulation of the development of the Digital Single Market and improvements in the data protection and privacy field;
- Increased resilience against frauds.

Likely social impacts

The following social impacts will be analysed:

- Increased security and safety for EU citizens (or some kind of users, e.g. children) in the digital society and economy.
- Increased protection of personal data.
- Increased capacity of producers in the European Union to make their products secure.
- Increased consumer trust in the Digital Single Market and the digitization of traditional goods;
- Resilience against illicit practices (e.g. increased cybersecurity of the concerned products, prevention of frauds);

Likely environmental impacts

No specific or major impact on the environment is expected at this stage of the analysis.

Likely impacts on fundamental rights

Increased capacity of the European Union to autonomously secure its products and services is also likely to help the citizens to better protect their information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life.

Likely impacts on simplification and/or administrative burden

[11] E.g. Artificial Intelligence or IoT

The RED is a new approach legislation, where only essential requirements are defined. Manufacturers are requested to demonstrate how the technical solutions in their products comply with the law.

On the one hand, one or more delegated acts pursuant this initiative will create some additional burden for the manufacturers, who will have to demonstrate compliance with the newly adopted essential requirements.

On the other hand, however, the European Standard Organizations (ESOs) will be asked to prepare harmonised standards in support of the legislation. This will allow manufacturers using the technical specifications therein contained to presume conformity of their products with the law. It is relevant that the European Standardization Organizations have started the production of reports and specifications for complex systems[12]. As some of them relate to the IoT, these products can already benefit from the flourishing production of standards and technical specifications in this field. The more available technical solutions, the easier the production of harmonised standards. As a consequence, it is expected that this industry-driven process will reduce the burden on manufacturers and ease the fulfilment of the conformity assessment procedures.

In any case the impact on simplification can be high, compared to the scenario of MS adopting provisions at a National level.

Also for this reason, this initiative could improve the consistent implementation and application of the existing legislation in all Member States increasing predictability and legal certainty for all parties concerned.

D. Evidence base, data collection and better regulation instruments

Impact assessment

An impact assessment is being prepared to support the preparation of this initiative and to inform the Commission's decision. The Impact Assessment is likely to be finalized in the 3rd quarter of 2019.

Evidence base and data collection

The Impact Assessment will be based on in-house data of the Commission[13] and other relevant data such as compliance costs or market information. Further evidence will be gathered by a service contract to support the impact assessment.

The Commission will also take into account other relevant studies[14] conducted by Member States and consumer organisations.

Consultation of citizens and stakeholders

In line with the Better Regulation Guidelines, the Commission will consult stakeholders as widely as possible. The aim of this consultation is to gather external information on the possible gaps in the legislative framework and investigate which policy options would allow to increase legal certainty, facilitate the implementation of the Internal and Digital Single Markets and reinforce the consumers' trust in new technological developments. A broad set of stakeholders will be consulted including national authorities, competence centres and research community across the EU, industry, EU institutions and bodies, consumer and consumer organisation and others. Depending on the stakeholder group identified, different tools and methods will be used to conduct the consultation.

During a 4-week period, all interested stakeholders will be able to provide feedback on this Inception Impact Assessment.

[12] TR 103 421 V1.1.1 (2017-04), TR 103 306 V1.3.1 (2018-08), TR 103 305-4 V1.1.1 (2016-08), TR 103 305-3 V1.1.1 (2016-08), TR 103 305-2 V1.1.1 (2016-08), TR 103 305-1 V2.1.1 (2016-08), TR 103 570 V1.1.1 (2017-10), TS 103 532 V1.1.1 (2018-03), TS 103 487 V1.1.1 (2016-04), TR 103 369 V1.1.1 (2016-07), TR 103 331 V1.1.1 (2016-08), EG 203 310 V1.1.1 (2016-06), TR 103 309 V1.1.1 (2015-08), TR 103 308 V1.1.1 (2016-01), TS 103 307 V1.3.1 (2018-04), TR 103 304 V1.1.1 (2016-07), TR 103 303 V1.1.1 (2016-04), TS 102 165-1 V5.2.3 (2017-10), TS 103 458 V1.1.1 (2018-06)

[13] e.g, the study of the JRC in http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105061/jrc105061_final_online.pdf

[14] As for instance those in http://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf and https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

The Expert Group of the RED, which is being established under the call for expert in the Commission's website, will provide support during the IA.

The impact assessment process will include both public and targeted consultations. The public consultation will be open to the general public. The more specific, targeted consultations will take place by means of interviews and surveys with:

- Representatives of competent authorities in Member States responsible for the implementation of the RED (Directive 2014/53/EU) (including respective market surveillance authorities), the GDPR (Regulation 2016/679) and/or the ePD (Directive 2002/58/EC);
- Representatives of stakeholder's associations (Industry and SMEs, consumers, European Standardization Organisations, etc.);
- Representatives of selected enterprises;
- Representatives of NGOs (in particular those involved with privacy, fraud or children) and civil society.

The different tools that will be used to reach stakeholders are:

- 12-week internet based open public consultation, in 6 languages, to be carried out through on-line consultation tools.
- Targeted consultations and interviews with the representatives of the stakeholders mentioned above (3 languages).
- Targeted consultation of EU SME umbrella organisations and contact points in Enterprise Europe Network (EEN)

The public and targeted consultations and the interviews are expected to take place in Q2 2019.
The results of the consultations will be made available by a synopsis report.

Will an implementation plan be established?

An implementation plan will not be established, as this initiative does not require adoption by the Member States of new transposition/implementation measures.