COCIR
SUSTAINABLE COMPETENCE IN ADVANCING HEALTHCARE
European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

COCIR Position Paper
on the General Data Protection Regulation[1]

COCIR represents the European Medical Diagnostic Imaging, Electromedical and Healthcare ICT Industry. Our industry offers many technologies that support the safe, fast and seamless transfer of medical data to support quality healthcare.

COCIR supports an effective, clear and reliable data protection framework and welcomes the intent to harmonies the legal framework at European level through the adoption of an EU regulation. COCIR also recognises considerable improvements in the provisions for data concerning health. However COCIR recalls that quality healthcare depends on the availability of comprehensive health data at the point of care and throughout the healthcare cycle. COCIR feels some provisions could restrict the availability of health data, delay innovation, create legal uncertainty and increase compliance costs. We therefore recommend that the following aspects of the regulation be considered:

COCIR's main recommendations to improve the General Data Protection Regulation:

1. **Clarify definitions** (Art. 4): The use of anonymised, pseudonymised or key–coded data by the healthcare and research sectors should be facilitated by the Regulation. Article 4 should recognise that data which cannot identify the data subject (e.g. anonymised data); data which are not directly associated to the data subject (e.g. technical data) or data which require unreasonable time and effort to identify the data subject (e.g. pseudonymised data) are not personal data and are not subject to the Regulation.

2. **Maintain clear and separate responsibilities between the healthcare provider and the medical technology provider**, as per the current regime (Art. 28- 33- 34- 77). The relationship between the healthcare provider and the medical technology provider should be managed by contract, not by law.

3. **Reduce administrative burden** (Art. 26): In an environment where outsourcing is part of the business model and care delivery, seeking approval of the healthcare provider before enlisting other medical technology providers generates administrative burden on both sides, without bringing benefits to privacy.

4. **Allow processing of data concerning health by medical technology manufacturers for maintenance and equipment performance evaluation purposes** (Art. 81 - 83): Professionals employed by medical technology manufacturers (technicians, engineers, medical professionals), should be able to access data concerning health for technical maintenance and equipment performance evaluation.

[1] *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

DETAILED BRIEFING

COCIR believes the following provisions could be improved to add legal clarity, legal certainty and ensure feasibility in a healthcare environment.

The following detailed briefing includes additional information substantiating the four critical recommendations (Part A) articulated above as well as secondary recommendations (part B).

A - COCIR main recommendations

1. **Clarify definitions** (Art. 4)

The proposed definitions for '*Personal Data'* and '*Data Concerning Health'* are too broad. The Regulation should cover only data that can lead to the identification of a data subject. For instance the serial number of a medical device may be considered 'data concerning health' although it is associated to a medical equipment and not to a data subject.

- ***Anonymised*** data cannot be linked to the data subject and should be explicitly excluded from the scope of the Regulation.
- Other data that are not directly associated to the data subject, and that cannot identify the data subject without unreasonable time and effort should also be explicitly excluded from the scope of the Regulation:
    - ***Pseudonymised*** data are data where personally identifiable information (PII) - such as name, date of birth, address or account number – has been replaced with a code. An investigator would not be able to link anonymised information back to a specific data subject provided the link between the code and the PII is kept separately.
    - ***Technical data*** are data directly associated to medical equipment (e.g. serial number of a medical device) but are not directly associated to a data subject. An investigator would not be able to link technical information back to a specific data subject without unreasonable time and effort.

2. **Maintain clear and separate responsibilities between the healthcare provider (data controller) and the medical technology provider (data processor)** (Art. 24-26-77)

The new obligations on processors create confusion around responsibility between healthcare provider (data controllers) and medical technology provider (data processors).
Responsibilities and liabilities between the controller and the processor need to be handled through contractual arrangements, not through law.
COCIR recommends keeping the approach of the existing legal framework in Directive 95/46/EC. This would promote clarity as well as better enforcement from the point of view of the relationship with supervisory authorities.

3. **Reduce administrative burden when enlisting a sub-processor** (Art. 26)

Requiring each Data Controller (e.g. a hospital) to agree to each sub-processor enlisted by a Data Processor (e.g. eHealth service provider) introduces an excessive administrative burden and increases costs for both the Data Controller and Data Processor. COCIR recommends keeping the existing legal framework in Directive 95/46/EC. Responsibilities and liabilities between the controller and the processor should be handled through contractual arrangements, not through law.

4. **Allow processing of Data Concerning Health by technicians for technical maintenance and equipment performance evaluation** (Art. 81-83)

Article 81 provides that data concerning health may by processed by a healthcare professional or a professional with an equivalent obligation of professional secrecy.
It is not clear whether this provision covers technicians and engineers employed by manufacturers, who may have access to Data Concerning Health when maintaining medical systems, either onsite or remotely. The regulation should clarify that professionals who have signed a commitment of secrecy by contract with their employer qualify as *'professionals with an equivalent obligation of professional secrecy'*.

The proposed exemption for processing data concerning health in article 83 does not seem to take into account registry studies for the improvement of medical devices or medical services effectively making it impossible for companies to meet regulatory requirements under the medical devices Regulation. The regulation should clarify that the processing "*for historical, statistical or scientific research purposes*" in the meaning of Article 83 includes processing for the purposes of the manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of a medical device, by clear guidance[2].

B- COCIR secondary recommendations

1. **Extend the exemption to the right to be forgotten to healthcare** (Art. 17)

Implementing the right to be forgotten in healthcare requires careful consideration of the consequences. Deleting data from an electronic health record can run counter to patient safety, public interest, healthcare research and eHealth deployment. Medical records, patient registries and other clinical databases should be exempted from the right to be forgotten.

2. **Allow the secondary use of anonymised and pseudonymised data for health purposes** (Art. 20)

The text of Article 20 might render legitimate use of data for health research impossible or extremely difficult, with great consequences for the social benefits in this area. COCIR

[2] *This concern falls if anonymised data are not subject to the Regulation.*

recommends deleting Article 20 or reverting to the language currently used in Article 15 of Directive 95/46/EC.[3]

3. Delete '*privacy by design*' and '*privacy by default*' obligations (Art. 23)

Although COCIR supports imbedding privacy and data protection features in products and services from the onset, we are concerned that 'Privacy by Design' and 'Privacy by Default' mean different things for different people. The intent of both is already reflected in the Regulation through new requirements: data protection impact assessment, data minimisation, etc. COCIR feels these concepts are superfluous and should be deleted.

4. Consider context and feasibility for Data Breach Notifications (Art. 31 - 32)

The definition of 'breach' and associated notification requirements, especially the concepts of 'reasonable timeframe' and 'mitigating effects of safeguards' and 'potential for harm/adverse impact' pose issues of practicability in a real world environment. Industry would greatly benefit from a more pragmatic and proportional approach. A two-step approach could be considered for the notification of the breach, and the submission of the requested documentation within a longer time frame. This would allow more time for a qualitative impact assessment, and efficient corrective and mitigation actions.

5. Ensure data protection impact assessments and pre-authorisation obligations take account the context and are not 'one size fits all' (Art. 33-34)

Data Protection Impact Assessment should not be mandatory, and should be relative to the scope and types of processing activities, and based on a well-defined category of "high-risk" activity. Organisations should be able to construct their own assessment, based on their specific type of organisation, legal requirements, contractual obligations, and, where appropriate, internal policies.

Prior consultation should not be needed when processing is based on consent or contract. Where approval is required (Article 34), a clear time line for the approval should be clarified prior to effective dates.

6. Keep certification industry led and voluntary for more efficiency (Art. 39)

Certification mechanisms and data protection seals and marks developed and managed by industry should be favoured. They should remain voluntary rather than mandatory and COCIR recommends the adoption of existing internationally recognised standards (e.g. ISO/IEC 27001) rather than developing new certification mechanisms. COCIR also recommends removing paragraphs 2 and 3 on delegated and implementing acts in Article 39.

[3] *This concern falls if anonymised data are not subject to the Regulation.*

7. **Recognise compliance with non-EU frameworks, e.g. HIPAA Privacy and Security Rules in the U.S., as adequate safeguard for transferring data beyond EU borders** (Art. 42)

Many COCIR members have a strong presence outside of Europe (e.g. in the USA), and have invested in processing capabilities there. Transfer of health data to the USA should be allowed under the HIPAA rules which provide safeguards for privacy. The transfer of anonymised /pseudonymised data should not require further authorization or consultation where the recipient does not reasonably have access to the key, and contractual or legal restrictions prohibit re-identification of the data subjects.

8. **Allow the transfer of anonymised, pseudonymised and encrypted data to a third country, without further regulatory authorisation, where re-identification is not possible** (Chapter V)

The transfer of anonymised data should not require any further authorisation or consultation where the recipient does not reasonably have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects. Anonymised[4] and pseudonymised[5] data which do not reasonably permit re-identification of a data subject, and encrypted data[6] which do not permit understanding of the information, are central to many data processing operations. Responsible data controllers and processors have invested heavily in a raft of data processing techniques to prevent the identification of data subjects and protect user privacy. These efforts should be recognised and encouraged.

9. **To introduce proportionality to Administrative Sanctions** (Art. 79)

COCIR recognises the need for credible enforcement mechanisms, specifically sanctions and fines, but notes that the current proposal lacks proportionality. This may result in making the EU less competitive in attracting investment in facilities or services. Furthermore some terms would need a clear definition to be implementable, e.g. '*incomplete information'*, '*insufficiently transparent'*, etc.

---

[4] *Previously identifiable data that have been de-identified and for which a code or other link no longer exists. An investigator would not be able to link anonymised information back to a specific data subject.*

[5] *Pseudonymisation, a Privacy Enhancing Technology (PET), is the replacement of Personally Identifiable Information (PII) – such as name, address or account number – with pseudonyms. Key-coded data are a classical example of pseudonymisation. Personally Identifiable Information (PII) is earmarked by codes, while the link between the code and the PII (like name, date of birth, address, etc.) is kept separately.*

[6] *Encrypted data are information that has been transformed and made unreadable by the use of algorithms. Only those with the key can decrypt the data.*

10. Limit the number and scope of delegated acts for more legal certainty

The number and scope of delegated acts undermines the legal certainty of the Regulation. The number should be reduced and clear timelines introduced for those remaining.

- The categories of recipients of health data should not be determined by delegated acts, but by healthcare organisations (Art. 14.7).
- The legal framework should be fully harmonised to avoid conflicting provisions between the Regulation, delegated acts and national law (Art. 81.1).
- Measures, criteria, requirements, etc., provided for by delegated acts (Art.81.3) should be technology, service and business model neutral and industry-based.