Amendments proposed by COCIR on the General Data Protection Regulation[1]

Please find below amendments proposed by COCIR on the General Data Protection Regulation.

Article 4: Definitions

(12) 'data concerning health' means any ~~***information***~~ ***personal data*** which relates to the physical or mental health of ~~***an individual***~~ ***a data subject***–, or to the provision of health services to the ~~***individual***~~ ***data subject***.
Data not directly associated with the data subject, data associated to a medical equipment (e.g. serial number of a medical device), is not 'data concerning health'. Anonymised and pseudonymised data are not 'data concerning health'.

(13) 'anonymised data' means 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 anonymized information back to a specific data subject.

(14) 'pseudonymised data' means previously identifiable data where Personally Identifiable Information (PII) – such as name, date of birth, address or account number – has been replaced with a code (pseudonyms or symbol). The link between the code and the PII is kept separately. An investigator would not be able to link anonymized information back to a specific data subject.

+ new recital: 'technical data' or any data associated to a piece of equipment used to process data (e.g. serial number, etc) but which is not directly associated with the data subject, and does not allow the identification of the data subject, should not be considered 'personal data'.

Justification:
The Regulation should recognise that data that do not relate to a data subject or cannot be linked to a data subject through various data protection mechanisms (e.g. anonymisation or pseudonymisation) are not 'personal data', nor 'data concerning health'.

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

Article 14: Information to the data subject

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria ~~***for categories of recipients referred to in point (f) of paragraph 1***~~, for the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.

Justification:
In a healthcare environment, categories of recipients of data vary on healthcare providers' or eHealth service provider practices, organizations, and workflows. It should remain under the power of these actors considering the case reference as required. The European Commission adopting prescriptive delegated acts (Art. 14(7)) is not the right approach as it will delay the process and reduce flexibility in healthcare settings.

Article 17: Right to be forgotten and to erasure

(3) The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
(a) for exercising the right of freedom of expression in accordance with Article 80;
(b) for reasons of public interest in the area of public health in accordance with Article 81;
(c) for maintaining medical records for prevention, medical diagnosis, treatment, palliative care, clinical trials, patient registries, and other health research and medical innovation purposes.
(***c*** ~~***d***~~) for historical, statistical and scientific research purposes in accordance with Article 83;
(~~***d***~~ ***e***) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(~~***e f***~~) in the cases referred to in paragraph 4.

Justification:
Implementing the right to be forgotten and to erasure in healthcare requires careful consideration of the consequences. Deleting data from electronic health records does not effectively protect individual privacy, and can run counter to patient safety, public interest, health research, and eHealth deployment. For instance, deleting all or parts of the information contained in an electronic health record would undermine the ability of medical professionals to treat the patient effectively. Statistical analyses will be "depowered" if data is deleted, particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as pediatric.

Article 20: Measures based on profiling[2]

Delete

Justification:
Profiling techniques per se do not need special regulatory treatment given the many safeguards introduced in the draft Regulation especially when incentives are provided for companies to anonymize and/or pseudonymize data. The current text of Article 20 might render legitimate use of data for health research impossible with great consequences for the social benefits in this area.

Article 23: Data protection by design and by default

Delete

Alternatively:

(1) Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.
~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~
~~4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~

Recital (61)

Delete

Justification:
The concepts of 'Privacy by Design' and 'Privacy by Default' are subject to interpretation and lack clear definition. These ideas are probably more effective as reflecting organisational policy or for use as marketing concepts, rather than as a framework for compliance with legal requirements. In addition, the underlying elements of PBD and PBD are already reflected in the Regulation through new requirements: data protection impact assessment, data minimisation, etc. These concepts are therefore superfluous at best, and would introduce legal uncertainty at worse.

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

Article 26: Processor

1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:
(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
(c) take all required measures pursuant to Article 30;
(d) ***~~enlist another processor only with the prior permission of the controller;~~***
(***d~~–e~~***) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(***e ~~f~~***) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;
(***f ~~g~~***) ***~~hand over all results to the controller after the end of the processing and~~*** not process the personal data further ***after the end of the agreed processing ~~otherwise~~***;
(***g ~~h~~***) ***upon request*** make available to the controller ***~~and the supervisory authority~~*** all ***relevant and permissible*** information necessary to control compliance with the obligations laid down in this Article.
3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2.
4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.
~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.~~

Justification:
The proposed text introduces a host of new requirements for data processors and states how these should be included in the contractual arrangements. Some of these additions are unworkable in practice. For example, a controller may want to ensure that additional sub-processors - which may be numerous – apply effective data protection but this does not mean they are able or willing, to assess each in turn prior to their employment. As the processor has the closer relationship, they are better placed to make such a judgment. In relation to handing over results at the end of processing, there may be no results as such to hand over if the data minimisation principle has been effectively applied. Making data available to the supervisory authority should be handled by the controller. Certain information may be subject to a confidentiality obligation under law

or contract and hence a processor may not be at liberty to disclose such information to a supervisory authority. Moreover, such data should not be required to be transmitted on a regular basis as this would overburden authorities and further increase the administrative burden.

Requiring each Data Controller (e.g. hospital) to agree, individually, to each sub-processor enlisted by a Data Processor would introduce excessive administrative burden and increase costs to both the data controller and data processor.

Article 28: Documentation

1. Each controller ~~***and processor***~~ and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.
2. The documentation shall contain at least the following information:
   (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;
   (b) the name and contact details of the data protection officer, if any;
   (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);
   (d) a description of categories of data subjects and of the categories of personal data relating to them;
   (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;
   (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;
   (g) a general indication of the time limits for erasure of the different categories of data;
   (h) the description of the mechanisms referred to in Article 22(3).
3. The controller ~~***and the processor***~~ and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers ~~***and processors***~~:
   (a) a natural person processing personal data without a commercial interest; or
   (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.
5. ~~***The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.***~~
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification:
Requiring both controllers and processors to maintain the same documentation for the same processing operation in an unnecessary burden that does not enhance the protection of data subjects or facilitate enforcement by the authorities. Controllers are in the best position to determine the purposes of processing and provide associated documentation that supports the basis and details of processing. Furthermore, given the

required level of detail already demanded in the documentation, it does not make sense for the Commission to have powers to adopt even more requirements or criteria.

Recital (65)

In order to demonstrate compliance with this Regulation, the controller ~~***or processor***~~ should document each processing operation. Each controller ~~***and processor***~~ should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

Justification:
In line with proposed amendments to Article 28.

Article 30: Security of Processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

~~***(3) The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies.***~~

~~***(4)The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:***~~

~~***(a) prevent any unauthorised access to personal data;***~~

~~***(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;***~~

~~***(c) ensure the verification of the lawfulness of processing operations.***~~

~~***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Justification:
Any specifications pertaining the security requirements for processing personal data should be technologically neutral, flexible, scalable and applicable to the type of data being processed, the context for the data processing, and the potential implications to the processing activities. In the healthcare context, highly secure transmission and storage of data is desirable, however, access controls must be respectful of the need to access data in the provision of care, serviceability of medical devices and healthcare technology, etc.

Article 33: Data protection impact assessment

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller ~~***or the processor acting on the controller's behalf***~~ shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
2. The following processing operations in particular present specific risks referred to in paragraph 1:
   (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which *decisions* are based that produce legal effects *that gravely and adversely affect the individual's fundamental rights*
   (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;
   (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;
   (d) personal data in large scale filing systems on children, genetic data or biometric data;
   ~~***(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).***~~
   (e) Impact assessment should be carried out if the processing differs significantly from existing practices of the controller and the new approach in itself presents specific risks and this creates doubts with the compliance of this Regulation.
~~***3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.***~~
~~***4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.***~~
3.~~5~~. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
~~***4. 6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium sized enterprises.***~~
~~***5. 7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).***~~

Justification:
With the view to ensure legal certainty and enable better enforcement by supervisory authorities and in accordance with Recital 62 which requires "a clear attribution of the responsibilities under this Regulation", privacy impact assessments should be carried out by the controller. Notably, the controller is in the best position to assess the impact of any processing. The controller, and not the processor, has ready access to all relevant information, including risks and benefits of processing the personal data. Furthermore, the requirement to seek the views of data subjects is impractical.

Specific risks should be clarified. The notion of harm or 'grave or adverse impact' on the individual's rights could be an element to determine 'specific risks'.
The obligation to carry out impact assessment should not apply to every single existing routine processing, but only to new processings which differ significantly to the current practices of the Data Controller.Given the fact that according to Art. 14 data subjects need to be informed of the data processing, an obligation to consult data subjects as part of the assessment appears misplaced and unnecessary.

Furthermore, impact assessments should not be standardised. Different types of organisations may have equally effective means of performing such assessments, and unnecessary constraints may hinder improvements in the process, as technologies emerge, and contexts change.

Article 34: Prior authorisation and prior consultation

Delete

Alternatively

1. The controller ~~***or the processor as the case may be***~~ shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.
2. The authorisation process by the supervisory authority should be limited in time, with a maximum timeline of 15 days to respond, or request additional information, where deemed necessary.
~~***2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:***~~
~~***(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or***~~
~~***(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.***~~
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified

or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.

~~***4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.***~~

~~***5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.***~~

~~***6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.***~~

4. ~~***7.***~~ Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.

~~***8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.***~~

5. ~~***9.***~~ The Commission may set out standard forms and procedures for prior authorisations ~~***and consultations***~~ referred to in paragraphs 1 ~~***and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6***~~. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Justification:

Requiring prior consultation in the case of the wide range of processing operations that may qualify for a 'high degree of specific risks', in accordance with the long list in Article 33, is likely to be a serious impediment to innovation in Europe. DPAs could face a deluge of cases that quickly back-up. Even if the DPAs had the resources to handle the case-load, conducting a thorough investigation is likely to be a case of months, not days. An ex-post system is far more fitting to a regime of effective and accountable data protection which does not impede growth and innovation.

In addition, it is essential to set a time limit for the assessment by the supervisory authority in order to avoid unreasonable delays.

Recital (74)

~~***Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure***~~

~~***based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.***~~

Justification:
In line with changes to Article 34.

Article 39: Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms ***shall be voluntary, capable of global application and affordable. These mechanisms shall also be technology neutral and shall*** contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

~~***2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.***~~

~~***3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).***~~

Justification:
The amendment proposed to Article 39(1) would introduce important conditions on certification schemes that would ensure they are widely usable by controllers and processors large and small. Specifically, certification schemes would need to: be voluntary, affordable, be capable of being rolled-out and recognised globally, be neutral as to system, service or technology.

The adoption of delegated and implementing acts for the purposes of data protection certification would create regulatory uncertainty (Article 39 (2) and (3)). Moreover, the express provision regarding the possibility for the Commission to lay down technical standards in this area is too broad and risks endangering the principle of technology neutrality.

By contrast, the view supported by Directive 2002/58/EC, that "no mandatory requirements for specific technical features [should be] imposed on products and services, including terminal or other electronic communications equipment, which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States", should be maintained.

Article 41: Transfers with an adequacy decision

1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defense, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation in question has entered into.

(3) The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

(4)Transfers to the United States of America under HIPAA rules are deemed adequate safeguards.

Justification:
Many global or European companies have a strong presence in third countries (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 establish adequate safeguards for privacy. In addition the transfer of anonymized / 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.

Article 44: Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) The personal data has been anonymised or pseudonymised, and the key is kept separately from the data.

(~~b~~ ***c***) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(~~c~~ ***d***) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(~~d~~ ***e***) the transfer is necessary for important grounds of public interest; or

(***e f***) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(~~f~~ ***g)*** the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(~~g~~ ***h***) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(~~h~~ ***i)*** the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.
4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.

Justification:
As per article 44

Article 64: European Data Protection Board

1. A European Data Protection Board is hereby set up.
2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.
3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.
4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.
5. ***The Industry shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. Industry should provide technologically neutral guidance regarding safeguards for personal data processing.***

Justification:
Industry participation in the Board will provide guidance to develop scalable, technologically neutral guidance regarding safeguards for personal data processing.

Article 77: Right to compensation and liability

1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller ~~***or the processor***~~ for the damage suffered.
2. Where more than one controller ~~***or processor***~~ is involved in the processing, each controller ~~***or processor***~~ shall be jointly and severally liable for the entire amount of the damage***, to the extent that liability has not already been established in the determination of responsibilities envisaged in Article 24.***
3. ***If a processor processes personal data other than as instructed by the controller, they may be held liable should any person suffer damage as a result of such processing.***
4. ***In case of joint controllers***, one controller ~~***or the processor***~~ may be exempted from this liability, in whole or in part, if the controller ~~***or the processor***~~ proves that they are not responsible for the event giving rise to the damage.

Justification:
Under the current Directive, liability is correctly attributed to the data controller. Essentially, they direct the data processor and if the processor does not act on those orders then contractual arrangements apply to address the circumstances. Introducing a vague liability clause does not clarify the current situation but creates confusion for controllers, processors and data subjects alike.

Article 81: Processing of personal data concerning health

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law ~~***or Member State law***~~ which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or 'or another person who has committed to confidentiality by contract with his employer'.
(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or
(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system ***and the provision of health services.***

2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.

+ new recital:

The principles of data protection should take context into consideration and should recognise the need for medical equipment manufacturers to maintain medical systems and devices with the support of technicians or engineers, provided they have been trained on the confidentiality of 'data concerning health', have signed a commitment of confidentiality by contract with their employer and third parties and remote maintenance security rules are in place. Manufacturers are also consulted by healthcare providers to advice on radiation dose for medical images on the basis of the patient age, weight, medical condition, etc. The Regulation should facilitate such scenarios.
The principles of data protection should also take obligations under other legal frameworks into consideration and should recognize the obligation for medical equipment manufacturers to collect clinical data to evaluate the performance of said medical equipment/devices[3].

Justification:

Processing of personal data should be based on Union law only. The reference to Member States in 81.1 laws undermines the harmonisation brought by the Regulation and could impose additional or conflicting requirements in the context of "safeguarding the data subject's legitimate interests".
The proposed exemption for processing data concerning health of Article 81 does not take into account registry studies for the improvement of medical devices or medical services, like eHealth services, effectively making it impossible for companies to meet regulatory requirements under the medical devices regulation. The analysis of health data should be authorized for professionals who are not healthcare professionals, but have been trained to privacy and have a signed a commitment to secrecy (e.g. laboratory agents, workers in a telemedicine service, etc). The same logic applies for the

[3] *This last statement falls is anonymised data are not covered by the Regulation.*

technical maintenance (remote or onsite) of medical devices, which is carried out by technicians (not by healthcare professionals).

Article 83: Processing for historical, statistical and scientific research purposes

1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:
   (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
   (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.

2. Within the limits of this Regulation, personal data may be processed for the purposes of manufacturer's regulatory pre- and post-market obligations with respect to clinical evaluation of medical devices[4].

3. ~~***2.***~~ Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:
   (a) the data subject has given consent, subject to the conditions laid down in Article 7;
   (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or
   (c) the data subject has made the data public.

4. ~~***3.***~~ The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and ~~***2***~~ ***3*** as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.

Justification:
The regulation should take into account the obligations for manufacturers under the medical devices Regulation to perform registry studies and post-marketing follow-up studies with respect to medical devices.

[4] *This amendment falls is anonymised data are not subject to the Regulation.*