Council of the European Union
General Secretariat

Interinstitutional files:
2020/0340(COD)

Brussels, 01 February 2021

WK 1360/2021 INIT

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Data Governance Act : ES comments Articles 2, 5 and Chapter III

Delegations will find in annex ES comments Articles 2, 5 and Chapter III of Data Governance Act.

ES COMMENTS - ARTS 2, 5 AND CHAPTER III

Article 2 – Definitions

2(5)

- What happens with data holders that has a de facto right but not a right in accordance with applicable unión or national law? Is this also a data holder?

2 (7)

- We would eliminate the word "shared" in this line and change the order of the complement "of data" as this "data sharing means the provision **of data** by a data holder to a data user …. use of **such** ~~shared~~ data". Minimal comment.

2 (10)

- Add "evidence-based policy making" at the end as in "such as scientific research purposes, **evidence-based policy making** or improving public services".

2(14)

- We think that it would be good to add that the secure processing environment needs to include a reference that it is to process data "in a privacy-preserving way and to ensure compliance with applicable legislation".

Recital 11

This recital is much clearer than the article it refers to. We would propose to bring some of the elements of this recital into the article so as to highlight some conditions that should be absolutely included in the list of conditions that the MS impose. This would bring certain harmonisation to the process.

Article 5

General comment: either in the recital or in the article, as the legal basis for processing is consent in some exceptional cases, the legal basis of public interest should be set as an example as the most appropriate legal basis for processing personal data in this settings as used by Finland or France.

5 (3)

- There might be a need to define what pre-processed data means
- You can protect commercially confidential information not only by deleting it but also aggregating it. We propose to add the word modify or aggregate. It would read " pre-processing aims to… delete, **modify or aggregate** commercially confidential information, including trade secrets".

5 (4)

- in letter (a) it is only clear that it refers to remote access to the secure processing because letter (b) talks about "within physical premises". This is why, we would add the word remote in letter (a). It would read " to access and re-use the data **remotely** within a secure processing environment…".

5 (5)

- impose conditions should be imposed also for the process, not only for the functioning and the results. This would mean that there might be the capacity for the public sector to verify the algorithm that is sent remotely or similar actions to make sure the rights are fully protected. It would read "the public sector body should be able to verify the **process, means** and any results of processing of data undertaken by the data re-user **to preserve the integrity of the protected data**…".

5 (6)

- We would change the word **cost** by **burden**. It is not only about how much money it costs, but how much burden is put on the public sector to collect consent.

5 (9)

- We would eliminate letter (b) and include it as text in the recital on how the Commission may assess that a third country provides equivalent protection on intellectual property rights. It should be enough to say that it provides equivalent protection and provides effective judicial redress. If the protection ensured is not effectively applied and enforced, it would not be equivalent.

5 (10)

- We would not use the word "confidential data" as this may be too broad and not useful. It should refer to "**non-personal data protected on grounds set out in Article 3**".

5(11)

- This para might need redrafting as it is confusing.
- In line 9, which reads "necessary to achieve the public policy objectives identified in tech Union law act, such as safety and public heath". It is not clear why safety and public health are highlighted here and not other public policy objectives. It seems out of context, we recommend to delete it from here and add in recital further examples of what public policy objectives these can be.

General comment: is there a possibility for non-personal data not to be transferred at all to third countries? Is that article 5(4)b?

Chapter III –

Article 11 - Conditions for providing data sharing services

The conditions set out for providers, e.g. in subparagraphs (5) and (8), require competent authorities to have sufficient means and resources, including advanced cybersecurity expertise, to exercise their functions of monitoring data exchange service providers.

It would be appropriate to consider requiring certification by a conformity assessment body, as provided for in the supervision regime for qualified trust service providers in the eIDAS Regulation. This would also prevent providers from choosing the Member State with the weakest supervision (forum shopping). The COM ensures that the same requirements of Art.11 will apply to all providers, however, as they are defined at such a high level, their degree of application will depend on the competent authority of the country where they are established. It would therefore be appropriate to refer to the application of common standards or the development of future guidance by COM.

Article 13 - Monitoring compliance

Sub-paragraph 6 mentions the procedure for intra-Community cooperation between competent authorities, but does not detail it. As the Regulation on the free movement of non-personal data (FFoD) provides in Article 7, the content of the request and the obligation to respond without undue delay and within a proportionate period should be laid down**.**