Council of the European Union
General Secretariat

Brussels, 09 July 2021

WK 9209/2021 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.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Data Governance Act : Informal non-paper supported by AT, DK, FI and NL on the 4th compromise text (doc. 9642/21)

Delegations will find in annex an informal non-paper supported by AT, DK, FI and NL on the fourth compromise text on Data Governance Act (doc. 9642/21)

Informal non-paper with suggestions on DGA

Dear SI Presidency,

We welcome the fourth compromise proposal and look forward to working with you on the DGA. We are a group of MS who support the ambition and intention with the DGA to contribute to a flourishing and responsible data economy. And yet we see substantial challenges in the text that need to be addressed going forward. Therefore, we have formulated common proposals to improve the text which we hope you will take into account when drafting the fifth compromise proposal. We would be happy to elaborate on these suggestions on a WP or bilaterally and we warmly invite other Member States to join us.

Kind regards,

The Friends of the Data Economy,
Austria, Denmark, Finland, the Netherlands

Suggestions are marked with tracked changes as compared to the 4th Presidency compromise text.

DGA chapter 2 – articles to be revised

Article 5: Conditions for re-use

(5) **In the case of re-use allowed according to paragraph 3 points (b) and (c) t~~T~~he** public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body ~~shall~~ may **reserve the right** ~~be able~~ to verify **the process, the means and** any results of processing of data undertaken by the re-user **to preserve the integrity of the protection of the data** and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties.

(5a)

Unless national law includes provisions on applicable confidentiality obligations, t~~T~~he public sector body ~~shall~~ may make the use of data provided in accordance with paragraph 3 ~~Article 5(3)~~ ~~such secure processing environment~~ conditional on the ~~signature~~ adherence by the re-user to ~~of~~ a confidentiality ~~agreement~~ obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place. ~~Public sector bodies shall prohibit the re-users~~ Re-users shall be prohibited from re-identifying any data subject to whom the data relates ~~and~~ unless strictly necessary for research purposes in the public interest according to Article 89 of Regulation (EU) 2016/679. This data shall under no circumstances be made publicly available without informed consent of the data subjects. ~~Re-users~~ shall be ~~oblige~~ required ~~the re-users~~ ~~to assess on an on-going basis the risks of re-identification and to notify any data breach resulting in the re-identification of the individuals concerned to the public sector body concerned.~~

Justification:

It is up to Member States to decide on the necessary requirements for accessing data. National laws on access to documents may already prohibit the disclosure of confidential information. In these cases, there is no need to have a confidentiality obligation. Additionally, we would like to open up the possibilities for research under the conditions of the GDPR.

Also, we consider the requirement for re-users to assess the risk of re-identification on an ongoing basis as quite burdensome. Re-users should be able to utilize data for research purposes once permission has been given. Concerning the prevention of risks the general provisions of the GDPR apply to both re-users and public sector bodies. Also, in accordance with the GDPR, a re-user as a data controller must inform the data protection supervisory authorities in accordance with the GDPR. Therefore, there is no need to introduce this requirement in the DGA.

(6)
Justification:
The wording of "**may provide assistance** to potential re-users in seeking consent of the data subjects" needs to be kept under art. 5(6).

(8a) Where a re-user intends to transfer non-personal data protected on the grounds set out in Article 3(1) to a third country, it shall inform the public sector body of its intention as well as of the purpose of the transfer. In the case of re-use in accordance with paragraph 6, ~~the public sector body shall inform the legal person whose rights and interests may be affected of that intention and purpose and shall not allow the re-use in case the legal person refuses to give the permission for the transfer.~~ the public sector body may allow or refuse the permission for the transfer.

Justification:
We prefer not introducing more requirements to public sector bodies in this regard, except for the possibility of the public sector body to allow or refuse the permission for transfers. If applied, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR. Furthermore, we consider that data protection authorities would need to be included in the standard-setting of these decisions.

(11)
Justification:
We see parallels to the Open Data Directive 2019/1024 regarding the definition of high value datasets. Unlike provided in the previously mentioned Directive, the criteria for determining in specific Union acts certain non-personal data categories held by public sector bodies to be highly sensitive are lacking (except for mentioning safety and public health and the risk of re-identification of anonymised data). It is essential that further possible action happens in accordance with a legislative procedure and is discussed at expert level, where necessary by the WP DAPIX.

As recommended by the EDPB/EDPS, the concept of "highly sensitive non-personal data" has to be clarified in this Article and explained by providing concrete examples instead of leaving this to future legislation. Generally, we consider that the terminology of the Regulation should be streamlined. The Regulation currently refers to several seemingly different categories of data which are not defined in Article 2 such as "sensitive data" (Recital 14, 18a) "commercially

sensitive data" (Recital 16, 17), "highly sensitive data" (Recital 19), "highly sensitive health data" (Recital 19), "highly sensitive non-personal data" (Recital 19), "competitively sensitive information" (Recital 29, 44).

Furthermore, it is unclear to us, what is meant by "risks of re-identification of anonymized data." If such risks exist, the data is considered personal data regulated by the GDPR and relevant national regulation. This notion should thus be clarified or omitted.

Article 7: Competent bodies

(1a) Member States shall ensure that procedures are in place to grant access to the re-use of the categories of data referred to in Article 3 (1) that fulfil the conditions set out by this Regulation.

Justification:

We strongly encourage a way forward where requirements to the access to data is clearly defined in the DGA, but it is not described in detail *how* member states fulfill requirements in the DGA e.g. in terms of organizational and procedural matters.

(~~1~~2) **For the tasks mentioned in this Article,** Member States shall designate one or more competent bodies to support re-users and grant access to the re-use of the categories of data referred to in Article 3 (1). Member States may designate competent bodies, which may be sectoral, to support the public sector bodies which grant access to the re-use of the categories of data referred to in Article 3 (1) in the exercise of that task. **Member States ~~shall be allowed~~ may either ~~to~~ establish one or more new competent bodies or ~~to~~ rely on existing public sector bodies ~~ones~~ or** on internal services of public sector bodies **that fulfil the conditions set out by this Regulation.**

Justification:

It is essential to clarify that Member States are obliged to define (existing) competent bodies, but they may optionally define new sectoral competent bodies (possibly at a higher organisational level) supporting other public sector bodies. The link to provisions in paragraph 2 related to the "support" (from a technical viewpoint) are upheld.

Member States should maintain flexibility regarding their internal administrative setups for granting access to data. If Member States choose to make data available for reuse, they should decide how to internally organise this data access. It does not make sense to define a one-size-fits-all model regarding internal administration of Member States in the DGA. In any case, it has to be clarified that non-competent public sector bodies are not affected.

Public sector bodies specialised in e.g. health data would and should have the technical and legislative knowledge themselves to support and give access to their own data. On the contrary it would be very difficult for a general public sector body to have sufficient knowledge about very different sectoral data held by different authorities.

(2) The support provided for in paragraph 1 ~~shall~~ may include, where necessary:

(a) providing technical support by making available a secure processing environment for providing access for the re-use of data;

(b) providing technical support **for** ~~in the application of tested techniques~~ ensuring data processing in a manner that preserves privacy **and confidentiality** of the information contained in the data for which re-use is allowed~~, including techniques for pseudonymisation, anonymisation, generalisation, suppression and randomisation of personal data~~;

~~(c) **where relevant,** assisting the public sector bodies **to support provide assistance to re users**, where relevant, in obtaining consent **for re use from data subjects** or permission **from data holders** by re users for re use for altruistic and other purposes in line with **their** specific decisions of data holders, including on the jurisdiction or jurisdictions in which the data processing is intended to take place;~~

Justification:
There is no need to oblige Member States to organise support functions within their public sectors. Member States can perfectly decide for themselves what kind of support different public sector bodies should have.

The decision to provide assistance to re-users is at the discretion of the Member States. The public sector should not be involved in seeking consent on behalf of third parties. In any case, standard-setting decisions would require the inclusion of the data protection authorities. The legal basis for this requirement has still not been clarified and therefore, paragraph c should be deleted.

~~(d) providing public sector bodies with assistance on the adequacy of undertakings made by a re user, pursuant to Article 5 (10).~~

Justification:
This assistance to public sector bodies concerning the adequacy of international data transfers should be provided by the data protection authorities.

Article 8a: Processing of requests for re-use

(1) ~~(3)~~ Requests for the re-use of the categories of data referred to in Article 3 (1) shall be ~~granted or refused~~received by ~~the competent public sector bodies or~~ the competent bodies referred to in Article 7 (1) ~~within a reasonable time, and in any case within two months from the date of the **receipt of the** request~~. Requests shall be granted or refused within a reasonable time.

~~**(2) In the case of exceptionally extensive and complex requests this period may be extended by 30 working days. In such cases the applicant shall be notified as soon as possible that more time is needed to process the request and the reasons why.**~~

Justification:
It is vital to clarify that requests for the re-use of protected data cannot be made to any public sector bodies, but only to competent bodies as designated by the Member States. The term "competent public sector bodies" should be avoided without a proper definition.. It is important that the competence to grant access to data belongs to the competent public sector body determined by the national law.

It is essential to avoid any setting of time periods, as this would be in conflict with national procedures and with national laws on access to data. Furthermore, the setting of time limits irrespective of the type of data and the complexity of the application in relation to the data sources applied for and relevant approval procedures is inappropriate. In practice, re-users and public sectors bodies engage in a dialogue to identify the needs of the re-user and the necessary data to be accessed.

~~**(3)** (4) Any natural or legal person affected by a decision of a public sector body or of a competent body, as the case may be, shall have **an effective right of redress** the right to an effective judicial remedy against such decision before the courts **in** of the Member State where the relevant body is located. **Such right of redress shall be laid down in national law and shall include the possibility of review by an impartial review body with the appropriate expertise, such as the national competition authority, the relevant access to documents authority, the supervisory authority established in accordance with Regulation (EU) 2016/679 or a national judicial authority, whose decisions are binding upon the public sector body concerned.**~~

Justification:
There is no need to introduce a right to judicial remedy against decisions regarding data access. This is an unnecessary layer of bureaucracy that will not result in enhanced access to data. The amount of administrative measures proposed in the DGA could have the exact opposite effect: It will be less attractive for Member States to grant access to data because of the amount of administrative procedures required by the DGA.

Article 8a (3) imposes a potentially difficult and comprehensive task. It will require the establishment of a new organization, new workflows, a new regulatory basis, etc. It will be difficult to ensure the right expertise to perform in practice, since the data regulation differs across sectors and is in some sectors very complex (e.g. health data).

DGA chapter III - articles to be revised

Article 2.2a

The definition is an essential tool to set the scope of this chapter of the Regulation. Further optimisation will ensure that the legal effect of the text will be clear to authorities as well as companies that might be affected by the Regulation.

Neutral data intermediaries have the potential to give data subjects and data holders a better choice on how to give access to their data, without compromising on the confidentiality of that data. At the same time, services that aggregate data and offer added value services, such as real-time mapping, are vital for innovation in the data economy. We therefore think it would be best to have both kind of services present in the internal market: neutral intermediaries that

only offer intermediation services and integrated data-services that do not have intermediation as a core part of their service. The intermediation services should be recognised as such.

The Data Governance Act can achieve this by further finetuning the following elements in the definition:

1. The meaning of a 'direct link': this should involve reference to a contractual relationship to be established between the data holder or data subject and the data user.
2. Exclusion of (existing) added value services aiming at pooling data or extracting value from data (offered by the same operator; closed arrangements; exclusion of existing data ecosystems).
3. The intermediary should have a contract with the data holder or data subject.
4. The intermediary should allow for an active involvement of data holders to make informed decisions, i.e. make explicit efforts to facilitate data sharing between contractual parties. This distinguishes them from services that simply transfer content, such as cloud services, communications services etc.

Once these elements will be brought into the scope, a number of points may follow:

- As there is a contractual relationship between the intermediary and the data subject/holder and the data user, the intermediary has a responsibility in the value chain. Therefore, liability should be addressed.
- The data economy would benefit from a clear distinction of reliable, neutral intermediaries. A title or label for providers that notify their services according to art. 10 would help data holders and subjects identify such intermediaries and add to the trustworthiness of these agents. Parliament has similar thoughts.

Article 14: Exceptions

This Chapter shall not apply to**:**

(a) public sector bodies that offer data sharing intermediation facilities on a non-commercial basis;

Justification:
Lit. a needs to be maintained and should preferably be moved to art. 2(2a)(e). Services of the public sector of a non-commercial character have to be exempted from the DGA in order to better distinguish e-Government services according to the European Digital Identity proposal from data intermediation services. This needs to be stipulated in the normative part of the proposal.

DGA chapter IV - articles to be revised

Art. 14a
National arrangements for data altruism

(1) Member States ~~shall define national polices for data altruism and shall~~ may ~~put~~ have in place organisational and/or technical arrangements to facilitate data

altruism in the public interest. In support of this Member States may define national policies and ethical guidelines for data altruism. These national policies ~~shall~~ may in particular support the freedom of choice for data subjects in making personal data related to them held by public sector bodies available voluntarily for data altruism and refer to necessary information requirements to data subjects concerning the re-use of data in the public interest. If a Member State develops such national policies, it shall inform the Commission.

Justification:
We understand that legally speaking, an active obligation is required in a Regulation. However, an obligation to develop or execute national policies goes beyond the objectives of this Regulation and the subsidiarity for Member States to develop such policies. We therefore suggest a compromise that leaves Member States the choice to develop such policies. If they do so, they shall inform the Commission. This will enable the Commission to monitor the development of data altruism policies throughout the Union.

It is vital that "Member States may define national policies" is kept. Furthermore, we suggest referring to allow for the definition of national ethical guidelines for data altruism, as many decisions on the re-use of sensitive data are based on essential ethical decisions. Incentives of the public sector may not influence the individuals' freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it. It is vital that data subjects are informed about the benefits of their data donations in the public interest. Member States could support data altruism through additional quality assurance measures. These may include: independently awarded seals of approval, random checks by authorities and the introduction of a national reporting office for abuse warnings.

Article 16

(d) comply with a code of conduct referred to in article 19a, at the latest by [date of implementation of this Regulation + 18 months].

Article 32

~~The Commission shall, by [two years after the date of application of this Regulation], assess the effectiveness of the provisions set out in Article 19a, and whether adherence to self regulatory codes of conduct should become a requirement for the registration of recognised data altruism organisations in accordance with Article 16.~~

Justification:
We support the use of codes of conduct as suggested by the EDPB/EDPS, as a means to ensure data altruism organisations comply with standards to ensure transparant and ethical use of the data they receive for a general interest. Compliance with a code of conduct for all users of the label, both early adopters and newly developed ones, is essential to ensure a level playing field and a transparent situation for (potential) data donors. This makes the addition to art. 32 obsolete.

* * * * * * * * * *