Statement on the Digital Services Package and Data Strategy

Adopted on 18 November 2021

The European Data Protection Board has adopted the following statement:

Since November 2020, the European Commission has presented several legislative proposals as part of its digital and data strategies, most notably the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA) and the Regulation on a European approach for Artificial Intelligence (AIR). A fifth proposal for a "Data Act" is expected to be presented very soon, as one of several initiatives announced in the European strategy for Data[1].

The proposals aim to facilitate the further use and sharing of (personal) data between more public and private parties inside 'the data economy', to support the use of specific technologies such as Big Data and AI and to regulate online platforms and gatekeepers. Processing of personal data already is or will be a core activity of the entities, business models and technologies regulated by the proposals. The combined effect of the adoption and implementation of the proposals will therefore significantly impact the protection of the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the EU Charter') and in Article 16 of the Treaty on the Functioning of the European Union ('TFEU').

The EDPB and EDPS have already issued joint opinions on the DGA[2] and the AIR and the EDPS has issued opinions on the European strategy for Data, on the DMA and on the DSA[3]. These Opinions highlight a number of concerns and make recommendations to bring the proposals more in line with existing Union legislation on data protection. The EDPB regrets that several recommendations have so far not been fully addressed by the co-legislature[4].

[1] Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final.
[2] The EDPB has also issued Statement 05/2021 on Data Governance Act in light of the legislative developments.
[3] The EDPS has also issued a Preliminary Opinion on the European Health Data Space. An overview all opinions and statements issues by the EDPB and the EDPS is provided as an annex to this statement.
[4] The concerns highlighted in this Statement concern the initial text of the proposals made by the Commission and do not refer to any subsequent position of the European Parliament or Council of the European Union unless explicitly indicated otherwise.

With this statement, the EDPB draws attention to a number of overarching concerns and urges the co-legislature to take decisive action. Our concerns consist of three categories: (1) lack of protection of individuals' fundamental rights and freedoms; (2) fragmented supervision; and (3) risks of inconsistencies.

The EDPB considers that, without further amendments, the proposals will negatively impact the fundamental rights and freedoms of individuals and lead to significant legal uncertainty that would undermine both the existing and future legal framework. As such, the proposals may fail to create the conditions for innovation and economic growth envisaged by the proposals themselves.

1. LACK OF PROTECTION OF INDIVIDUALS' FUNDAMENTAL RIGHTS AND FREEDOMS

In the proposals, certain choices have been made that are likely to have a long-lasting impact on the fundamental rights and freedoms of individuals and society as a whole. While the proposals seek overall to mitigate a variety of risks, the EDPB holds serious concerns about a number of choices made and considers the fundamental rights and freedoms of individuals require additional protection. Specific examples include:

- The proposal for the AIR would allow for the use of **AI systems categorizing individuals** from biometrics (such as facial recognition) according to **ethnicity, gender, as well as political or sexual orientation**, or other prohibited grounds of discrimination, or AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU[5]. The EDPB considers that such systems should be prohibited in the EU and calls on the co-legislators to include such a ban in the AIR. Furthermore, the EDPB considers that the use of AI to **infer emotions of a natural person** is highly undesirable and should be prohibited, except for certain well-specified use-cases, namely for health or research purposes, subject to appropriate safeguards, conditions and limits[6].

- In the same vein, given the significant adverse effect for individuals' fundamental rights and freedoms, the EDPB reiterates that the AIR **should include a ban on any use of AI for an automated recognition of human features in publicly accessible spaces** - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context.[7] The proposed AIR currently allows for the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement in certain cases[8]. The EDPB welcomes the recently adopted EP Resolution where the significant risks are highlighted[9].

- The EDPB also considers that **online targeted advertising should be regulated more strictly** in the DSA in favour of less intrusive forms of advertising that do not require any tracking of

[5] E.g., polygraph, Annex III, 6. (b) and 7. (a)) of the AIR. EDPB-EDPS Joint Opinion on the AIR, paragraph 32.
[6] EDPB-EDPS Joint Opinion on the AIR, paragraph 35.
[7] EDPB-EDPS Joint-Opinion on the AIR, paragraph 32.
[8] Specified under Article 5(1)(d)(i)-(iii) AIR.
[9] European Parliament resolution of 6 October 2021 on Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

user interaction with content and urges the co-legislature to consider a phase-out leading to a **prohibition of targeted advertising on the basis of pervasive tracking**[10] while the profiling of children should overall be prohibited.

- The EDPB recommends introducing in both the DSA and DMA **interoperability requirements** to promote a digital environment more open to competition, making it easier for individuals to choose among services that offer better privacy and data protection[11].

2. FRAGMENTED SUPERVISION

The proposals all provide for the establishment of supervisory authorities and new European cooperation structures between these authorities ('European Boards')[12]. While the processing of personal data is central to the activities regulated by the proposals, data protection supervisory authorities are not designated as the main competent authorities. The EDPB recalls that, as far as the protection and free flow of personal data is concerned, Article 16(2) TFEU and Article 8(3) of the EU Charter require that the supervision of the processing of personal data be entrusted to independent data protection authorities[13].

Moreover, the EDPB is very concerned that the proposals do not clearly set out how new the supervisory bodies (and the accompanying European Boards) should cooperate with data protection supervisory authorities (and the EDPB). In particular, the proposals fail to adequately address situations of potential overlap in competences or consult each other in matters of mutual concern. This creates a **risk of parallel supervision structures** where different competent authorities supervise the same entities having regard to the same (processing) activities **without structured cooperation** between them.

Specific examples include:

- The proposed DSA requires competent authorities to supervise the **recommender systems**[14] of very large online platforms (which often involve profiling data subjects within the meaning of the GDPR); as well as measures taken to **assess and mitigate systemic risks, including the risk to the right to privacy**[15]. The same proposal also contains provisions on **codes of conduct** that may concern processing of personal data[16]. Yet it does not require competent authorities

[10] See also the EDPS Opinion on the DSA, paragraphs 69-70, as well as the European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), paragraph 15.
[11] See also EDPS Opinion on the DSA, paragraphs 84-85 and EDPS Opinion on the DMA, paragraphs 37-38.
[12] Digital Markets Advisory Committee (DMAC) in the DMA; European Board for Digital Services (EBDS) in the DSA; European Artificial Intelligence Board (EAIB) in the AIR; European Data Innovation Board (EDIB) in the DGA.
[13] See EDPB statement 05/2021 on the DGA in light of legislative developments, at page 3; the EDPB-EDPS Joint Opinion on the AIR, at page 14.
[14] Article 29 of the DSA.
[15] In particular in the context of Article 27 (identification and assessment of the most prominent and recurrent systemic risks, as well as best practices to mitigate such risks), which refers to Article 26, including 26(1)(b), and Articles 35 and 36 of the DSA (codes of conduct).
[16] See articles 35-36 DSA.

to formally consult or to cooperate with the EDPB or its members. This poses a risk for conflicting guidance or even different outcomes in enforcement actions by supervisory authorities.

- The proposed DGA defines **new types of service providers and organisations** that would process large amounts of potentially sensitive data, notably, data intermediary services and data altruism organisations. However, **the 'vetting' regime for these entities is almost declarative and as such does not provide sufficient protection for data subjects**[17], since it is limited to the verification by the competent authority of (mainly formal) requirements[18] which shall occur within a very short time-limit[19].

- The proposed AIR sets out a **certification scheme and codes of conduct** for high-risk AI systems, but it is unclear if and how these certificates and codes may interface with requirements under the GDPR[20]. This could lead to situations in which AI systems, despite being certified (CE-marked) under the AIR to be placed on the market or put into service, would not be compliant with the rules and principles of data protection (notably, DPbDD)[21]. Furthermore, the proposed AIR lacks any reference to (mandatory) monitoring mechanisms for the codes of conduct designed to verify that providers of non-high-risk AI systems comply with their provisions[22].

- The proposed DMA requires gatekeepers to facilitate the exercise of **data portability** in line with the GDPR and to provide under certain conditions, **access to data**, including personal data, under Article 6(1)(h) and (i) and to anonymised data under Article 6(1)(j), without providing a clear legal basis for the processing of personal data or a duty of consultation and cooperation between any competent authority designated under the DMA with the competent data protection authority when supervising compliance with these provisions of the DMA.

In order to ensure complementarity in oversight and enhance legal certainty, the EDPB strongly recommends that each of the proposals clearly mentions data protection supervisory authorities among the relevant competent authorities with whom cooperation shall take place. In addition, each proposal should **provide for an explicit legal basis for the exchange of information necessary for effective cooperation and identify the circumstances in which cooperation should take place**. Moreover, the proposals should enable the competent supervisory authorities under each proposal **to share information** obtained in the context of any audits and investigations that relate to the processing of personal data with the competent data protection authorities, either upon request or on their own initiative[23]. The EDPB would like to underline the need to ensure that data protection supervisory authorities are provided with **sufficient resources** to perform these additional tasks.

[17] See EDPB EDPS Joint Opinion on the DGA, at paragraphs 136, 140, 151, 155, 175, 180, 191.
[18] Set out, respectively, in Article 11 of the DGA, for data sharing service providers, and Articles 16-19, for data altruism organisations.
[19] One week from the date of notification, for data sharing service providers (Article 10(7) of the DGA); twelve weeks from the date of application for data altruism organizations (Article 17(5) of the DGA).
[20] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 74.
[21] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 76.
[22] See EDPB-EDPS Joint Opinion on the AIR, at paragraph 79.
[23] See also EDPS Opinion on the DSA, at paragraphs 87-89 and EDPS Opinion on the DMA, at paragraphs 39-41.

3. RISKS OF INCONSISTENCIES

The proposals all aim to regulate technologies or activities that involve the processing of personal data. As such, the existing data protection framework is fully applicable. The operative text of the proposals, however, may **create ambiguity** as to the applicability of the data protection framework in certain cases. The co-legislature should resolve any ambiguities **to ensure** legal certainty and enhance coherence with the existing data protection framework in order to ensure its effective application**.** In any case, the proposals **should clearly state that they shall not affect or undermine the application of existing data protection rules and ensure that data protection rules shall prevail** whenever personal data are being processed[24].

Moreover, some provisions use the same terminology as the GDPR or the ePrivacy Directive, without an explicit reference to the aforementioned legislation. This risks affecting the interpretation given to core concepts of the GDPR (such as the key notion of 'consent' or 'data subject')[25]. It also creates the risk that certain provisions could be read as deviating from the GDPR or the ePrivacy Directive. Consequently, certain provisions **could easily be interpreted in a manner that is inconsistent with the existing legal framework and subsequently lead to legal uncertainty**.

Specific examples include:

- The proposal for a DSA requires service providers to **offer users at least one option for receiving content recommendations that does not involve the use of profiling**.[26] However, the principle of data protection by design and default requires that the systems offering these recommendations should not be based on profiling *by default*[27].

- In many cases, the **legal basis** for processing personal data is not clear from the legal text of the proposals. An example from the proposed DGA is the lack of clarity on the re-use of personal data held by public sector bodies[28]. The proposed AIR indicates that it does not provide a general legal ground for processing of personal data, while at the same time states that the providers of high-risk AI systems ''*may process special categories of personal data"* for ensuring bias monitoring, detection and correction and requires additional safeguards for that processing[29].

- **Overlapping terminology** (partly) with clearly different meanings like "online intermediation services" in the proposed DMA and "data intermediation services" in the proposed DGA are confusing and impeding on clarity of the proposals.

- One of the main points of concern regarding the proposed DGA is that the provisions do not sufficiently specify **whether they refer to non-personal data, personal data or both**, nor

[24] In accordance with the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the EU Charter and in Article 16 of TFEU.
[25] The EDPB welcomes that in the Council Mandate on the DGA as adopted on 24th of September 2021, the notions of consent and data subject has been brought in line with the requirements for consent in the GDPR.
[26] Article 29 of the DSA.
[27] See EDPS Opinion on the DSA, at paragraph 73.
[28] Article 5(6) of the DGA.
[29] Article 10(5) of the AIR.

specify sufficiently that in case of 'mixed data sets' the GDPR applies. As such, it is not clear that the data protection framework would remain applicable whenever personal data processing takes place, and when specific risks for re-identification of anonymised personal data need to be taken into account.[30] This lack of distinction may lead to confusion, for example, as to whether a legal basis under the GDPR is required (which is the case for all processing of personal data falling within its scope of application)[31].

Looking ahead:

The EDPB is conscious that one of the key initiatives of the European strategy for data is to create **Common European data spaces** in strategic sectors and domains of public interest, including in the area of health ("European Health Data Space"). In the Joint Opinion on the DGA, the EDPB and the EDPS already emphasised that any upcoming initiatives, such as **the Data Act**, that may have an impact on the processing of personal data, must ensure and uphold the respect and application of the EU acquis in the field of personal data protection[32].

At the time of drafting this Statement, the aim and content of the proposals for a Data Act, or for the European Health Data Space are not yet available. However, it is clear that both initiatives will aim to increase access and re-use of (personal) data for the purposes of data sharing between private and public parties.

In a similar vein, the EDPB therefore calls upon the Commission to avoid ambiguities in the new proposals to ensure legal certainty and coherence with the existing data protection framework to ensure its effective application. In any case, the proposals should clearly state that **they shall not affect or undermine the application of existing data protection rules and ensure that data protection rules shall prevail whenever personal data are being processed**[33].

Moreover, mindful of the particular challenges posed by increased data sharing, the EDPB calls for the forthcoming legislative proposals concerning European data spaces and the Data Act to define **specific data protection safeguards** at the outset, ensuring a high level of data protection, taking into account where relevant the processing of special categories of data such as health data. By explicitly defining these safeguards at the outset, we can ensure an adequate level of protection of personal data and avoid potential legal uncertainty.

In addition to the overarching concerns identified above, the EDPB wishes to stress:

(i) the **inalienable nature** of right to the protection of personal data as a right relating to **each natural person**, established under Article 16(1) TFEU and Article 8 of the EU Charter, which cannot be waived[34].

[30] See EDPB EDPS Joint Opinion on the DGA, at page 16.
[31] See further paragraphs 47-56 of the EDPB EDPS Joint Opinion on the DGA pointing out the legal uncertainty regarding the legal basis for the processing of personal data.
[32] EDPB EDPS Joint Opinion on the DGA, paragraph 19.
[33] In accordance with the fundamental rights to privacy and to the protection of personal data, enshrined in Articles 7 and 8 of the EU Charter and in Article 16 of TFEU.
[34] EDPB Statement on the DGA in the light of legislative developments, at page 4.

(ii) the need to incorporate **specific safeguards to ensure compliance with all data protection principles**, in particular **data minimisation, purpose limitation and transparency**. Relevant safeguards include, without being limited to: specifying the types of data which that may be processed, the purposes for which the data may be processed, the data subjects concerned, the parties the personal data may be shared with and storage periods. Particular attention should be paid to the safeguards for processing for the **purposes of scientific research**, ensuring **lawful, responsible and ethical data management**, such as **vetting requirements** for researchers who will have access to large amounts of potentially sensitive personal data[35].

(iii) the importance of the obligation of **data protection by design and by default**, which is particularly relevant in the context of **'connected objects'** (e.g. the Internet of Things and the Internet of Bodies[36]), due to the significant risks to the fundamental rights and freedoms of the persons concerned[37].

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[35] See for example the conditions set out in article 31(4) and 31(5) DSA.
[36] See Inception Impact Assessment to the Data Act, at page 6, referring to "*smart home appliances, wearables and home assistants*", available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.
[37] See Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Development on the Internet of things, p. 6-9, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

ANNEX: List of previous opinions and statements adopted by EDPB and EDPS

- EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), adopted on 11 March 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en

- EDPB Statement 05/2021 on the Data Governance Act in light of the legislative developments, adopted on 19 May 2021, available at: https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf

- EDPB-EDPS Joint Opinion 05/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), adopted on 18 June 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

- EDPS Opinion 01/2021 on the proposal for a Digital Services Act, adopted on 10 February 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en

- EDPS Opinion 02/2021 on the proposal for a Digital Markets Act, adopted on 10 February 2021, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en

- EDPS Opinion 03/2020 on the European strategy for data, adopted on 16 June 2020, available at: https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf

- EDPS Preliminary Opinion 8/2020 on the European Health Data Space, adopted on 17 November 2020, available at https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf.