PUBLIC CONSULTATION ON DATA ACT AND AMENDED RULES ON THE LEGAL PROTECTION OF DATABASES

Summary report on the public consultation

Disclaimer: the views presented in this factual summary report are not the views of the European Commission but of the stakeholders that participated in this open public consultation. It cannot under any circumstances be regarded as the official position of the Commission or its services.

The Data Act aims to ensure fairness in the allocation of data value among actors in the data economy and to foster access to and use of data. The Act will not alter data protection legislation and will seek to preserve incentives in data generation. In the context of this Act, a review of Directive 96/9/EC on the legal protection of databases is being undertaken in order to ensure its continued relevance for the data economy.

I. Objectives of the consultation

The objective of the public consultation, which took place from 3 June to 3 September 2021, was to gather stakeholders' views and experience on various topics in order to help shape the proposal for a Data Act.

This summary report on the results of the consultation provides an overview of the contributions and presents some preliminary conclusions, in particular of a quantitative nature.

The public consultation targeted all types of stakeholders, including citizens and businesses. The questionnaire gathered feedback on the different measures considered in preparing the Data Act. It was divided into the following sections:

I. Business-to-government data sharing for the public interest
II. Business-to-business data sharing
III. Tools for data sharing: smart contracts
IV. Clarifying rights on non-personal Internet-of-Things data stemming from professional use
V. Improving portability for business users of cloud services
VI. Complementing the portability right under Article 20 GDPR
VII. Intellectual Property Rights – Protection of Databases
VIII. Safeguards for non-personal data in international contexts

II. Who replied to the consultation?

449 stakeholders responded to the questionnaire from 32 countries (25 EU Member States, Argentina, Brazil, Canada, Japan, Switzerland, United Kingdom, United States). Businesses constituted the largest share, with 122 business associations and 105 companies/ business organisations. 100 respondents were public authorities and 58 were citizens (56 from the EU and 2 non-EU).

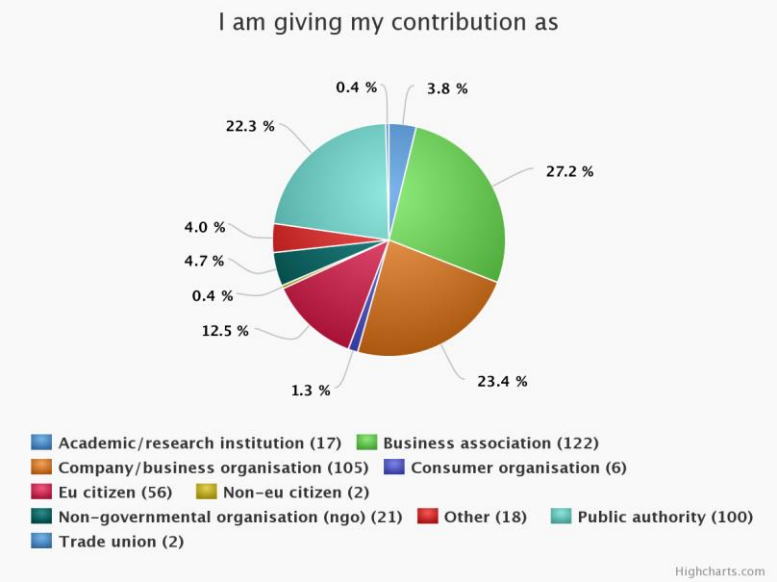

Fig. 1: Distribution of responses to the public consultation by type of respondent

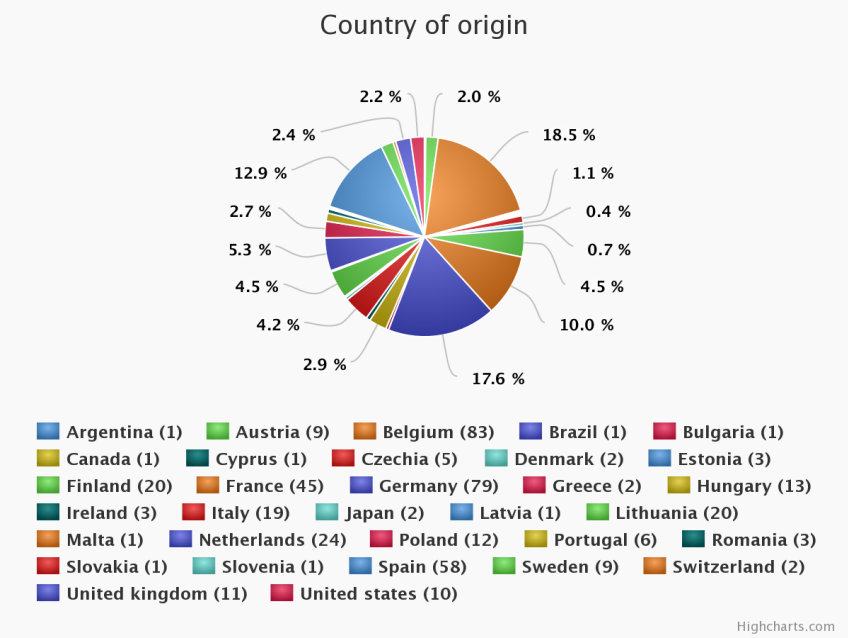

Fig. 2. Distribution of responses by country

Although a variety of sectors was available in the questionnaire for respondents to choose from, 34% identified themselves as 'others'. Amongst the sectors available, the largest share of respondents selected IT (11%), followed jointly by automotive (6%) and finance and insurance (also 6%), then media, publishing and broadcasting (4%). All other sectors were below 3%.

III. Main findings of the consultation

Business-to-government data sharing for the public interest

The majority of respondents (405 out of 449) contributed to section I. Some 40% of stakeholders responding to this section have experienced difficulties when requesting access to data in the context of business-to-government (B2G) data sharing for the public interest. This figure reaches 68% when looking at the responses from public authorities alone, and 30% as regards responses from companies and business organisations/ associations.

Most (62%) of the respondents consider that action (EU or national) on B2G data sharing for the public interest is needed. More specifically, this is the opinion of 91% of public authorities, 80% of academic/ research institutions and 38% of companies and business organisations/ associations.

Respondents identified the following main factors impeding B2G data sharing:

- legal uncertainty due to different rules in Member States (68% strongly or somewhat agree);
- legal barriers to the use of business data for the public interest, including competition rules (67%);
- commercial disincentives/ lack of incentives (67%);
- lack of appropriate infrastructure and cost of providing or processing such data (e.g. interoperability issues) (67%);
- lack of awareness (benefits, datasets available) (66%);
- lack of safeguards ensuring that the data will only be used for the public interest purpose for which it was requested (63%).

Respondents that replied to the question consider the following to be key areas where B2G data sharing should be compulsory: protecting the environment (59%), emergencies and crisis management, prevention and resilience (57%), and a healthier society (50%). When looking at public authority respondents only, the key areas identified are somewhat different: data for official statistics (90%), for protecting the environment (90%) and for emergencies and crisis management, prevention and resilience (86%).

55% of the stakeholders that replied to the question consider that the level of compensation for a business sharing data with public bodies should depend on the specific use-case. 23% of respondents consider that B2G data sharing should be free of charge, 8% that public bodies should pay the market price and 7% that a preferential rate/ below market price (marginal cost or other) should apply.

According to respondents, the most appropriate safeguards are data security measures including protection of commercially sensitive data (85% of the respondents to this section) and transparent reporting on how the authority has used the data (79%).

Business-to-business data sharing

Among the 336 respondents to section II, most stakeholders (68% of those that replied to the question), in particular companies (91%), confirmed that they share data with other companies (i.e. provide data to or access data from other companies), and they do this ‘many times’ (86% of respondents overall and 91% of companies). This data sharing happens either on a voluntary basis (44% of respondents) or both on a mandatory and voluntary basis (48%). The figures are similar when looking at companies only.

Some 44% of respondents to this section use data to design innovative products and services, 31% to optimise the supply chain, 29% for training algorithms for Artificial Intelligence, and 26% for predictive maintenance.

However, of those that indicated that they experienced difficulties in relation to B2B data sharing over the last 5 years, respondents described an array of obstacles, including of a technical nature (formats, lack of standards) (69%), of a legal nature (i.e. refusal to grant access not linked to competition concerns) (55%), the lack of a legal basis for the data holder to give access to data (48%), abuse of contractual imbalance (44%) and unreasonable prices (42%).

On contractual issues, 60% of the respondents to the question agree that *model contract terms* could contribute to increased data sharing, while 14% did not agree. SMEs and micro companies in particular (78%) support model contract terms. 46% of respondents across various sectors, (e.g. agriculture, construction, aftermarket, gaming, crafts, digital) agree that a *contractual fairness test* to avoid unilaterally imposed unfair conditions could contribute to increased data sharing, whereas 21% disagree. SMEs and micro companies show strong support (50%) and a significant number of large companies (41%) are in favour of a fairness test (22% disagree). Finally, 46% of respondents from various sectors (e.g. aftermarket, digital, industry, gaming, financial, as well as representatives with cross-sectoral membership) support the *horizontal data access modalities* applicable to data access rights established in specific sectors, while 19% disagree. More than half of the responding micro companies and SMEs (52%) are in favour of this measure, as are more than a third of the representatives of large companies (41%).

Some 79% of respondents to the question consider that *smart contracts* (section III) could be an effective tool to technically implement data access and use in the context of co-generated IoT data, in particular where the transfer is not only one-off but would involve some form of continuous data sharing. Companies and business associations (78%) show strong support for smart contracts (21% disagree). This is consistent with the support expressed by responding public authorities (85% in favour) as well as of other responding other stakeholders (76% in favour). Similarly, 71% of respondents consider that, when individuals request data portability from businesses, smart contracts could be an effective tool to implement data transfers. 66% of the responding companies and business associations agree, whereas 34% disagree. Here, again, public authorities (82%) and other stakeholders (72%) also expressed overwhelming support for smart contracts. In sum, the business community, public authorities and stakeholders share a common favourable view of the role of smart contracts for data access and data transfers as a function of data portability rights.

As regards *Internet-of-Things (IoT) data stemming from professional use* (section IV), 55% of respondents to the question use or plan to use such IoT objects. Of these, 70% consider that data coming from such objects may represent new challenges for market fairness, especially when access to relevant information about the functioning and performance is held by the manufacturer of such objects. Business organisations in particular see many problems with IoT contracts, such as lack of clarity in terms of data access rights.

As regards the *portability right under Article 20 GDPR* (section VI), 70% of the respondents to the question consider that manufacturers of connected objects should not be able to decide unilaterally what happens to the data generated by such objects. Instead, the majority (68%)

considers that such decisions should be taken by the owners/ users of the objects. Respondents consider that the absence of standards ensuring data interoperability (38%), of clearer rules on data types in scope (33%) and of universally used identification/ authentication methods to secure the request (31%) are the most important issues preventing the portability right from being fully effective.

In the context of B2B data sharing, the survey also covered questions about *intellectual property rights* (section VII). The largest group of respondents (54%) represent the business sector (of which 30% business associations and 24% companies or business organisations), followed by respondents from the public sector (18%). The majority (54%) agree that the 'sui generis' right should be reviewed, in particular in relation to the status of machine-generated data. Of all stakeholders responding to the question, 45% are unsure of the relation between this type of data and the Database Directive. The main difficulty reported in relation to the access and use of data was the lack of clarity regarding the application of the 'sui generis' right (11% of respondents to the section), but the most frequent reply was that stakeholders did not know or had no opinion (36%) or experienced no difficulties (20%).

As regards trade secrets, the majority of respondents (58%) rely on trade secrets protection when sharing data with other businesses. This figure is higher for business representatives (74%) than for public authorities (24%). Divergences exist between sectors. Some sectors rely heavily on trade secrets protection when sharing data with other businesses (financial: 90%, agricultural: 85%, telecom: 77%). Figures are lower for other sectors, such as the automotive (54%) and the health (57%) sectors. To ensure control over the use of confidential business information, respondents rely on different measures, including contractual arrangements (45%), trade secrets protection (38%), intellectual property rights (31%) and technical means (31%).

Cloud services and non-personal data in international contexts

311 stakeholders responded to the questions on improving *portability for business users of cloud services* (section V). A minority (39%) of these are aware of the SWIPO Codes of Conduct. This figure is much higher when considering IT providers only (69% are aware). In general, public authorities (17% awareness) are much less aware of the Codes of Conduct than businesses (57%).

As regards an appropriate legislative approach, 52% of respondents consider that there is a need to establish a right to portability for business users of cloud computing services in EU legislation, while 27% have no opinion and 19% are against establishing such a right. A binding legislative approach is mostly supported by businesses (58%), but less so by public authorities (41%) and academics (35%). A majority of IT providers believe there is a need to establish a right to portability (52%). Almost half of the respondents (46%) indicate that high-level legal principles should be used to flesh out the data portability right, while 29% consider that more specific conditions of a contractual, technical, commercial and economic nature are needed.

As regards standardisation, 51% deem that it would be suitable to develop, as part of a legislative approach to cloud service portability, standard APIs, open standards and

interoperable data formats, timeframes and potentially other technical elements. 16% believe this approach would not be suitable.

Finally, on the topic of *safeguards for non-personal data in international contexts* (section VIII), 76% of the respondents to the question (only business organisations and associations) perceive potential access to data by foreign authorities on the basis of foreign legislation as a risk to their organisation, including 19% who consider this as a high risk. A very small share of respondents (0.7%) state that this is not a risk at all to their company. When asked whether this potential access to data may lead to the disclosure of trade secrets or confidential business information, 74% answered that this is a risk to their company, while 4% indicated that this is not a risk at all.

IV. Next steps

This online consultation is part of a broader stakeholder consultation process that will contribute to the preparation of an impact assessment accompanying the forthcoming Data Act and the review of Directive 96/9/EC on the legal protection of databases. In this context, the Commission will carry out a more in-depth analysis of the replies. The outcome of this analysis will be presented as a full synopsis report in the Impact Assessment (Annex 2).