Ref. Ares(2021)3527151 - 28/05/2021

European Commission

INCEPTION IMPACT ASSESSMENT

Inception Impact Assessments aim to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders are in particular invited to provide views on the Commission's understanding of the problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options.

TITLE OF THE INITIATIVE	Data Act (including the review of the Directive 96/9/EC on the legal protection of databases)
LEAD DG (RESPONSIBLE UNIT)	CNECT/G1
LIKELY TYPE OF INITIATIVE	Legislative proposal
INDICATIVE PLANNING	Q3-Q4/2021
ADDITIONAL INFORMATION	

A. Context, Problem definition and Subsidiarity Check

Context

The Covid-19 crisis has shown the essential role of data use for crisis management and for informed decision-making by governments. Data has a key role in achieving the objectives of the European Green Deal and in the EU Recovery Plan, given its potential for innovation and job creation, as well as its contribution to the efficiency and international competitiveness of industries across all sectors. The European Council has underlined this potential on several occasions.

With its European strategy for data, published on 19 February 2020, the Commission has formulated a vision for the data economy. It will work towards the creation of a Single Market for data, where data flows between countries and sectors, where data is available for use in full respect of European values and rules, and where there are fair, practical and clear rules for access and use of the data. The Data Strategy also underlined that the EU should ensure an open, but assertive approach towards international data flows, based on European values.

The strategy announces the adoption of a horizontal legislative initiative, which would complement the proposal for a Regulation on European Data Governance, already adopted by the Commission. The aim would be to create fairness in the data economy by addressing the difficulties of access to and use of data in specific situations, including in a B2B context. It may be complemented by initiatives for the individual sectoral data spaces or for data access and use in specific sectors or markets, such as regarding access to vehicle data.

Processing of personal data is regulated under the GDPR and Directive 2002/58/EC ("ePrivacy Directive", to be replaced by the ePrivacy Regulation which is currently in legislative negotiations) which additionally protects private life and the confidentiality of communications, including any (personal and non-personal) data stored in and accessed from terminal equipment. Any proposal that specifies the conditions of processing of such data must comply with these requirements.

Further to the European strategy for data, the European Commission's Work Programme 2021 and the Intellectual Property Action Plan also announced a revision of the Directive 96/9/EC of 11 March 1996 on the legal protection of databases (hereinafter "the Database Directive") and a clarification of Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (hereinafter "the Trade Secrets Directive") as part of the broader Data Package.

Problem the initiative aims to tackle

This initiative will aim to increase access to and further use of data, so that more public and private actors can benefit from techniques such as Big Data and machine learning. The conditions of access and further usage in B2B relationships are often regulated by private contracts. The initiative would look both at data usage rights in industrial value chains and particularly at a fair distribution of usage rights that allow all parties to benefit from data-driven innovation. It would also seek to ensure positive effects for the use of data in the public interest. In short, it is about ensuring fairness in the allocation of economic value among actors of the data economy. This is particularly important in the context of the digital transformation of all sectors and ecosystems of industry. This requires clarity on the rules with respect to B2B access to and sharing of data, both non-personal and personal, by ensuring in particular data can be shared safely and not misappropriated, and in line with the applicable EU legislation. As

increasing fairness of the data economy starts with ensuring fairness the underpinning data processing services and infrastructures, the proposal aims for fairer and more competitive markets for data processing services, such as cloud computing services. Finally, clear and efficient rules on protection may be necessary for confidential business data that enjoy protection according to Union and Member State law, including but not limited to situations where such data are transferred outside the Union. This is particularly true in the context of cloud computing services.
The initiative in this respect seeks to provide a coordinated response that takes into account existing legal instruments such as the General Data Protection Regulation, the ePrivacy Directive and the Trade Secrets Directive, as well as the Database Directive which could be amended so that it supports the objectives of this initiative. The potential will also be explored for smart contracts to support a competitive and fair data economy by technical protection measures that ensure respect for data rights and contractual conditions for data sharing.

More specifically, the initiative seeks to address the following issues:

- **Use of privately-held data by the public sector:**
  When seeking to use privately-held data whose use are necessary to serve the public interest, the public sector is currently limited in making use of full potential of these data for the common good. There are several reasons for this deficiency recognised by the B2G expert group in its report[1]. B2G data sharing lacks structures and dedicated functions. There is a lack of rules governing reliable data sharing functions and transparent production of information from privately held data. Data sharing rules are fragmented across sectors and between Member States. This also includes data use only on an occasional basis, in particular unpredictable emergencies such as natural disasters or pandemics. In such situations, regular reporting obligations would be too burdensome and market-based procurement too slow. The economic barriers in sharing the data are very high. Use of such data requires high initial investment costs while the ex-post risks in terms of breach of personal data protection and privacy legislation or public perception are very high. As a result, companies would normally not make available actual data but prefer commercialising data services to the public sector. That would limit the public sector's capacity to develop data models of its own. The initiative would include personal data as well as non-personal data. It will examine the role of the Database Directive. It would build on existing applicable rules including the GDPR and ePrivacy and will assess the appropriate legal bases for business-to-government data sharing. It will be designed in full respect of the Trade Secrets Directive.
- **Data access and use in business-to-business situations**:
  Access to data in particular for start-ups and SMEs to develop new products/services in the digital economy is essential. The initiative will examine in a coordinated manner issues around data access and use in B2B situations, considering existing instruments such as the Database Directive and the Trade Secrets Directive, potentially additional measures in terms of rules promoting contractual fairness or specific data access and usage rights as well as the use of smart technologies. More specifically in this respect, the assessment will consider the following problems:
  i. B2B data sharing works best where the data holder has an incentive to share data and the parties' negotiating power is comparable. A data holder with a stronger negotiating power may, however, unilaterally impose unfair terms and conditions to the detriment of a company seeking data access which could have the effect of making data sharing disproportionately difficult or economically prohibitive or refuse access to data altogether. This may prevent data-driven businesses from developing/running their business models and could push existing market players out of the market and prevent new players from entering the market.
  ii. Non-personal data co-generated through industrial use constitute a specific class of data that will grow at exponential scale over the years to come (factory robots, agricultural machinery, etc.). The attribution of the rights to access and use such data is left to private contract. This can raise questions of fair competition in terms of the different markets (supplier, OEM-buyer relations, aftermarkets). Also, there is untapped innovative potential in secondary and tertiary uses made of the data through the development of novel services that rely on access to such data. The assessment will be conducted within the framework set by ePrivacy rules on access to information stored in a user's terminal equipment, currently under revision.)
  iii. The role of the Database Directive needs to be examined in this context. This directive provides for a two-tier structure of intellectual property protection: for original databases through copyright and a specific *sui generis* right for databases (including 'non-original' ones) if the qualitative or quantitative investment in obtaining, verifying and presenting the data was substantial. The copyright part of the directive harmonised rules governing databases, in compliance with the EU international copyright obligations whereas the *sui generis* regime is specific to EU law, limited territorially to the EU and does not derive from any international convention. Since the adoption of the directive in 1996, database businesses and technology have evolved and investments into data have gained

[1] See: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954

prominence. Important questions have arisen as regards the interaction of the directive with the current data economy, notably in view of the potential legal uncertainties as to the possible application of the *sui generis* right to databases with machine-generated data. At the same time, broadening access to and use of data have become a policy priority so as to maximise economic welfare. The initiative will therefore include a review of the Database Directive. Such review should address related uncertainties, with the overall objective of increasing legal certainty for access to and sharing data, in the context of B2B and B2G. The review needs to ensure in particular that the application of the directive does not pose an obstacle to the access and use of machine generated data and data generated in the context of Internet of Things. Moreover, additional amendments can also be considered and proposed.

In this context, the provisions of the Trade Secrets Directive, adopted in 2016 and formally implemented in all Member States, will be assessed. Companies need clear rules when providing access to and sharing of their data. This is even more important when companies share business sensitive data and trade secrets. The Trade Secrets Directive is an instrument that ensures protection against (un)lawful acquisition, use and disclosure of certain business sensitive information. This directive can apply to (business sensitive) data. The assessment of the application of the directive in the context of the data economy is ongoing, and it includes the launch of a study focusing on four key sectors (automotive, health, energy and financial services). Based on this assessment, clarifying guidance may be issued at a later date.

- The proliferation of IoT in personal use and increased overall connectivity are creating more personal data. The General Data Protection Regulation (GDPR) gives the data subjects important control rights over such data, not least the right to port data to other service providers (Article 20 GDPR), when such personal data is processed based on data subjects consent or it is necessary for performance of contract. The GDPR has left it up to industry to develop interoperability formats that enable personal data portability. In particular with IoT in personal use, the absence of an obligation to put in place technical interfaces for automated data exchanges, including in real time, can make it hard to offer certain services that require real time data flows, e.g. predictive maintenance of a household appliance, leading to lock-in situations for data subjects. This may hamper the development of innovative based on access to such data that data subjects would be interested in.
- In the context of B2G and B2B data access and use as well as in the portability of personal data by data subjects, **smart contracts** have an untapped potential to facilitate automated data sharing and pooling at scale while enforcing of usage restrictions. There has been a steady and significant increase in the number of smart contracts deployed since 2017. The absence of harmonized standards for smart contracts, however, undermines interoperability and consequently hampers scaling across sectors and across borders. A legal requirement at EU level setting essential requirements for smart contracts could designate the voluntary standards developed by the European Standardisation Organisations as harmonised standards, and thereby support interoperability of smart contracts across sectors and across borders, while also providing an important technical support for the pooling and sharing of data within and between data spaces.
- **Establishing more competitive markets for cloud computing services**: European organisations depend increasingly on cloud services for the processing of their data (which include highly distributed services known as 'edge computing' where computing resources are not centralised but processed closer to the user, eg in mobile communication base stations or even in connected end-user devices). In order to prevent vendor lock-in and ensure an open and competitive cloud market, it is necessary that business users can easily switch their data and applications between different cloud computing service providers or port their data back to on-premise IT systems without encountering contractual, technical and/or economic barriers. Service providers and users have jointly developed codes of conduct to address this issue, as mandated by the Regulation on the Free Flow of Non-personal Data. The adherence to these codes of conduct by market players could be invigorated by the recently published proposal for a Digital Markets Act, which contains a broad and high level portability provision that covers 'gatekeeper' service providers. While this provision does not provide any description of what 'enabling portability' means in this context, nor which terms should apply while enabling portability, the codes of conduct could offer a suitable tool for providers to show their compliance. The Commission is currently investigating whether the codes themselves offer sufficient guarantees for portability, with preliminary findings expected soon. While the codes of conduct offer solid information requirements and pre-contractual transparency obligations, they contain less provisions on technical requirements and the costs/timeframes associated with cloud service portability for cloud switching, which are also key preconditions for the effective portability of different services, including infrastructure and platform and software cloud services. Moreover, they cover data portability exclusively, but may omit the aspects of interoperability and application portability, which are key for cloud switching. On the basis of the outcomes of the evaluation of the codes of conduct, the Commission could decide it is necessary to establish a binding right on cloud service portability.
- **Safeguards for non-personal data in international contexts**: Non-personal data generated by EU companies may be subject to access requests pursuant to provisions of laws of third countries. This would

be specifically relevant when processing of such data occurs in a cloud computing service the provider of which is subject to the laws of third countries. The recent proposal for a Data Governance Act does not cover such services. Data access requests can be of legitimate nature, in particular for certain cross-border criminal law investigations or in the context of judicial or administrative procedures. Whereas the GDPR provides for rules and safeguards in this respect, for non-personal data there are currently no statutory law rules that would oblige the cloud computing service providers to give precedence to EU law on the protection of IP and trade secrets. There can be differences in approach between the EU and third countries with essential guarantees against disproportionate government access to non-personal data for law enforcement and other legitimate purposes. This can put confidential business data held within the EU at risk, exposing it to conflicting obligations.

Basis for EU intervention (legal basis and subsidiarity check)

Article 114 TFEU:

This initiative intends to further complete a single market for data, i.e. an area in which data from the public sector, businesses and citizens can be accessed and used in the best possible manner while respecting rights in relation to such data and investments made into their collection. Protection of confidential business data and trade secrets should also be safeguarded. Safeguarding the balanced outcome of the intervention will also be the objective for the review of the Database Directive. The initiative will allow the EU to benefit from the scale of the internal market, since data-driven products and services are often developed using data from different Member States, and later commercialised across the EU. Moreover, some Member States have taken legislative action to address the problems described above, in particular on the use of data by governments, whereas others have not. This can lead to legislative fragmentation in the internal market and different rules and practices across the EU and related costs by companies that would have to comply with different regimes.

Subsidiarity check:

The cross-border nature of industrial data value chains, of cloud computing service offers as well as the production and sale of smart objects by individuals makes it very difficult to address problems of fairness of contractual rules on B2B data sharing, access and use at Member State level. In a Single Market, potential obligations on manufacturers of smart objects connected to the IoT (both for personal and industrial use) can only be set at Union level. Similarly, cloud computing services are rarely offered within one Member State only. Fairness of business-to-business contracts would also be hard to achieve by different national rules that would lead to undesirable forum shopping.

In the area of business-to-government data sharing, many data providers that have relevant data are multinational companies. Such data providers should not be confronted with a fragmented legal regime. The initiative should leave, however, room for national implementation in particular in terms of the structures to be put in place.

Fragmentation resulting from adoption of national rules should be avoided, as they will lead to increased transactional costs, lack of transparency and legal certainty. This is particularly important in all situations concerning B2B data sharing, where it is essential that the framework is homogeneous throughout the EU. Cross-border aspects of B2G data flows and the need to act at EU level will be assessed.

B. Objectives and Policy options

Objectives concern the following, in full compliance with existing applicable rules including GDPR and ePrivacy rules and the Trade Secrets Directive:

- Business-to-government data sharing: Promote fair reliable and transparent, access to and use of (big) data sources held by private companies that can be valuable for innovative uses and the digital transformation of delivery of public services and better policymaking in a more flexible manner.
- Business-to-business data sharing:
  - Promote fairness in B2B data sharing contracts to further facilitate access to data and data sharing, which will benefit in particular start-ups and SMEs while ensuring compliance with EU competition rules as regards the data sharing.
  - Provide for a harmonious application of the conditions applicable in case sector-specific legislation mandates data access for the benefit of certain parties.
  - Improve legal certainty on access and use of co-generated non-personal data, including data generated from the Internet of Things (IoT): The objective is to open up more opportunities to generate value from data and to allow innovation through improved product design, to design additional services, but also to avoid lock-in effects.
  - Review of the Database Directive, with the overall objective of increasing legal certainty for access to and trading in data. The review will aim to ensure that the application of the Directive, in particular the *sui generis right* does not pose an obstacle to the access and use of machine-generated data and facilitate the sharing of such data.
  - These actions should be in full observance of the Trade Secrets Directive.

- Improve data and application portability between cloud computing services in the whole data economy. This could include addressing contractual, technical and/or economic barriers, faced by business users, to portability between cloud services, resulting in a stronger position of business users and a more competitive and open European cloud market.
- Improve technical standards for portability of data generated by individuals. The objective is to allow consumers to have more choice with respect to services around such objects, services that would depend on having access to certain data generated by these objects.
- Jurisdictional conflicts: The objective is to reduce the risk of conflicts of laws and the legal uncertainty they generate for service providers, notably providers of cloud computing services, and establish clear safeguards and transparency for non-personal data of EU companies that may be subject to disproportionate foreign access requests. The objective is to clarify the position of data processing services subject to conflicting jurisdictional requirements for disclosure of data while respecting the EU's international obligations in the WTO and bilateral trade agreements including in the areas of services, investment and intellectual property rights.

The following policy options - which are not mutually exclusive - could be considered, again in full compliance with existing applicable rules:

- Improved access to private sector data for the public sector:
  A more flexible framework for access and use of such data sources, including data-sharing requirements, transparency requirements and safeguards, could be designed. It could cover both ad-hoc and more regular access to and use of such data sources that due to their size and volume could not be subject to a reporting obligation (big data) and that could be better exploited for specific use-cases only. Legislation will clarify and bring certainty to B2G data sharing, facilitating decisions on the use of private sector data by government while complying with the existing legislation concerning protection of personal data, should such data be involved. Intermediation structures or bodies could aggregate demand, support professionalization, convene public sector bodies interested in certain data as well as private sector data holders, including at sectoral level. Their mandate could be to facilitate agreement on the conditions of use of such data, including remuneration. They could provide for a dispute settlement mechanism. In a high intensity option, legislation would lay down a right of public sector to access privately-held data for a range of defined public interest purposes. It would be examined what legal basis would be necessary in accordance with applicable rules including the GDPR. When designing the options, the proposed technical solutions should minimise the need for transmission of personal data, including confidential business information to the public sector, or offer appropriate safeguards.
- Ensuring fairness of data access and use in B2B situations:
  The following options would be studied:
  (1) Specific transparency obligations for manufacturers of connected objects on rights to access and use of non-personal data in professional use for the benefit of users of such objects.
  (2) A B2B fairness test to avoid unilaterally imposed unfair conditions for access to and use of data. Such test could be complemented by model contract terms recommended by the Commission. It could apply to specific data, such as non-personal data generated by objects connected to the IoT in professional use, or to a wider set of data sharing situations.
  (3) Laying down data access and use rights, potentially on the basis of fair, reasonable, proportionate, transparent and non-discriminatory terms for non-personal data. It could apply to specific data, such as non-personal data generated by objects connected to the IoT in professional use, or to a wider set of data sharing situations.

  (4) Providing a harmonisation of horizontal modalities for access to data, which could apply to data access rights established in specific sectoral rules. The horizontal modalities would address the question of how parties agree to access data, while potential sector specific data access rights could be established by sector specific rules, where justified. Such access to data could be based on fair, reasonable, proportionate, transparent and non-discriminatory terms, to be agreed between the parties. The approach would leave room to take into account specific characteristics of the relevant market and allow for the modalities to be further specified in sector specific legislation (e.g rules on in-vehicle data are being assessed as part of the review of the Type Approval Regulation). The principles could reconcile the interests of both, data-driven businesses interested in getting access to data, as well as those of data holders interested to receive a satisfactory yield on their investments, and thereby potentially create a win-win situation. Any ensuing mechanism should be in compliance with competition rules on information sharing. A horizontal dispute settlement mechanism could provide a solution in cases where parties are not able to find an agreement.

  (5) Examination of the role of the current rights and exceptions under Directive 96/9/EC on the legal protection of databases in this context and potential adaptations to that instrument with the overall objective to facilitate data access and use, with special attention given to the role of the *sui generis* right and clarification of its relationship with machine generated data. In this context, it needs to be ensured in particular that the application of the Directive does not pose an obstacle to the access and use of data, in particular machine generated data and data generated in the context of IoT. Related potential policy options

could include a clarification of the scope of application of the *sui generis* right to increase legal certainty as regards, in particular, machine generated data; the definition of a specific access regime to facilitate trading in and access to databases in a balanced manner; other additional elements to modernise the Directive, particularly the *sui generis* right, e.g. by aligning the exceptions to more recent EU copyright instruments.

- Contribute to portability of data generated by individuals: The legal instrument would, consistent with Article 20 GDPR, provide for technical specifications to help individuals take advantage of the portability right. It could mandate companies selling smart home appliances, wearables and home assistants to have in place technical interfaces that allow real-time portability of the data these devices collect during their use.
- Safeguarding a competitive cloud market by ensuring easy cloud service portability:
  On the basis of the soon to be expected results of the evaluation of the industry codes of conduct on data portability, the Data Act could introduce a binding obligation for cloud computing service providers to offer data and application portability.
  The sub-options available for this scenario would be:
  1) limiting intervention to mandating Standard Contractual Clauses, developed on the basis of elements of the Codes of Conduct already provided by the industry.
  2) formulating high-level legal requirements in the Data Act, to all cloud computing service providers on the market;
  3) developing more specific legal requirements defining distinct conditions of contractual, technical and economic nature.
  As it regards the latter, more far reaching sub-option, the obligatory provision should stipulate that, on request of the user organisation, its data must be exported in a structured, widely used and machine-readable format, for free or against an additional, but modest specified maximum fee, or fee structure, depending on the different use cases, in full compliance with the EU data protection legislation.
  The conditions should also include the maximum allowed timeframes within which cloud computing service providers should complete effective portability and a strong guarantee for ensuring business continuity during the porting process. In relation to the aforementioned conditions, standard APIs, open standards and allowable data formats could be specified further by means of implementing acts under the Data Act.
  Regardless the option chosen, it should be referenced in the future EU Cloud Rulebook, foreseen for Q2 2022, which will create a comprehensive overview of binding and non-binding EU rules, policies and standards applicable to cloud services operating on the EU market. This will ensure coherence with other important elements associated with cloud use, such as data protection, cloud security or unfair contractual practices already addressed by existing legislation (e.g. the GDPR) or self-regulatory initiatives, and will also facilitate proper compliance monitoring..
- Explore the possibility to define essential requirements for smart contracts' interoperability that could accompany a potential mandate for the European Standardisation Organisations for setting technical standards for smart contracts. The Data Act could define such essential requirements and foresee the possibility to designate the European standards ensuing from the aforementioned mandate as European harmonised standards. The latter would mitigate the risk of market fragmentation while also providing technical support for the creation of data spaces.
- To mitigate the risks resulting from government access to non-personal data of companies established in the Union, held by cloud computing service providers and to ensure trust in the use of cloud computing services, the following two options will be considered, consistent with the framework proposed for the Data Governance Act and for law enforcement obtaining e-evidence proposal, as well as the Commission's trade policy and international commitments:
  - the first option would entail creating an obligation for cloud computing service providers to notify, to the extent possible under the foreign law in question, the user every time they receive a request for access to data by foreign authorities, as well as to notify the Commission of all different laws of non-EU jurisdictions with extraterritorial effect to which they are subject. This information will then be published on an EU Transparency Portal.
  - A second option would entail the obligations from the first option and, in addition, mandate cloud computing service providers to ensure that they have all reasonable legal, technical and organisational measures in place, in order to prevent the transfer of or access to non-personal data of companies established in the Union and held by cloud computing service providers to third countries' governmental authorities, where such transfer or access would be in conflict with EU or national laws. The cloud service provider would not have to apply these legal, technical and organisational measures to deny access to the non-personal data in specific cases where such transfer or access would be based on an international agreement or a mutual legal assistance treaty, or where the legal system of the third country from which the data access requests emanates would contain the same legal safeguards and possibility for judicial redress as it is proposed by EU legislation on international access to electronic evidence. This option would extend the provisions included in the proposal for the Data Governance Act on this issue to cloud computing service providers.

C. Preliminary Assessment of Expected Impacts

Likely economic impacts

Overall, the economic impact of the measure is expected to materialise in more data-driven services and products that will be designed with the help of the use of digital data as well as efficiency gains in production and business processes. This would result from facilitating data sharing among businesses and a broader distribution of rights to use data. Moreover, efficiency gains are also expected from a more competitive and open cloud market, resulting in lower costs for data processing across the EU. More competitive markets are expected in markets offering complementary services for IoT objects in business and in personal use. This could particularly benefit start-ups and SMEs that are active in repair and maintenance of household appliances, but more generally allow for more data-driven innovation. In this respect, the fact that to a large extent not only personal data will be at stake will need to be considered. The conditions for sharing personal data are regulated in the GDPR and the processing of data in the electronic communication sector, including rules on access to terminal equipment, are regulated in the ePrivacy Directive. The measure may take away certain privileged positions of some companies, in particular OEMs of IoT objects, and could thus lead to limits in investments into data-generating objects. In this respect, the measure should be designed so as not to discourage investments into data generation and/or collection. The economic impact of third-country operators will also be assessed.

For cloud service providers and potential additional obligations to protect confidential business data, a broader assessment will be made of the likely impacts of the proposal on the Union's trade relations with third countries. Insofar that it sets additional requirements with related costs on cloud service providers, such costs may be set off by increased use of cloud services, as more (industrial) users trust cloud services.

In the context of business-to-government data sharing, the initiative will designed in a manner to take account of the costs that additional data sharing will have on companies.

Likely social impacts

The initiative is expected to improve policy implementation and government services, including at the local level, based on better data availability (e.g. as a result of easier access to privately held data by the public sector), as well as in public areas with high societal impact. It will lead to faster and more targeted responses to societal challenges due to anticipating risks using more available information, and it will also contribute to better decision-making in the public sector through better analysis of information. This was demonstrated during the Covid-19 pandemic: in the Exscalate4COV initiative, an ad hoc consortium of 18 partner organisations tested available molecules with drug-like properties in order to identify new treatments for COVID-19. This was only possible because pharmaceutical companies 'donated' information on molecules to European research centres. In the absence of an established data-sharing process it took 3 months to start processing the data. With a more structural and flexible approach on sharing of business data with the public sector, similar types of collaborations in the context of policy design or delivery of public services could be achieved.

Improved legal certainty regarding co-generated data that is within the scope of this initiative would lead to the development of better and new services and products for users, and through this, to a higher level of employment in this field, while the enhanced usability of data generated by individuals would provide data subjects with a broader range of choice and augmented authority and control over the use of such data.

Likely environmental impacts

The environmental impacts of increased data use are largely conditional on the progress made in reducing the energy consumption of data processing facilities and technologies. Cloud services in general can bring efficiency gains compared to local data centres. Furthermore, the initiative will seek to stimulate re-use of existing data so as to avoid environmental impacts of additional data collection (environmental impact of additional sensors and data storage costs).

This initiative is likely to produce positive impacts on the environment, through the public sector's better access to privately held big data that could enhance research as well as policymaking concerning climate change, more efficient use of natural resources, or reducing waste. Supporting data access in the context of predictive maintenance services carried out by independent repairers could also increase reparability and could therefore be a strengthening measure for the Circular Economy Action Plan and the Green Deal.

Likely impacts on fundamental rights

Since personal data and data stored in terminal equipment such as connected devices would fall into the scope of some elements of this initiative (e.g. improving usability of data linked to natural persons), the measure will be designed in a way that fully complies with the existing rules on personal data protection and ePrivacy. Further promoting the use of personal data in a B2G relation could bear risks that need to be addressed in the institutional design, in line with personal data protection by design and by default, such as promoting privacy-preserving data processing technologies and tools.

The revision of the Database Directive may have an impact on the fundamental right to property (as with any IPR). Any potential impact will be analysed in the context of the preparatory work for a possible legislative proposal.

Likely impacts on simplification and/or administrative burden

Although the setting up of a dispute settlement mechanism might incur administrative costs on the part of the public sector, a more flexible framework for on-demand access and use of private sector data by the public sector would provide a simpler and less burdensome way for public sector entities to acquire private data.

Measures on mitigating the exposure of EU citizens' data to foreign jurisdictions would generate some administrative and financial burden for cloud computing service providers in the form of notifications and the costs of the measures they would be obliged to take.

D. Evidence Base, Data collection and Better Regulation Instruments

Impact assessment

An Impact Assessment will help prepare the policy initiative, supported by an evidence collection exercise and a stakeholder consultation process. The support study (SMART 2019/0024) is currently ongoing. The final results are expected in Q2 2021. Furthermore, the Commission will launch a study on fairness in data sharing and data access to inform the IA, with results to be expected in Q2/Q3 2021. The Impact Assessment will also benefit from substantial consultation actions that have already taken place in 2017-2019.

Evidence base and data collection

Extensive work has been done during the past mandate, identifying the problems that are currently preventing Europe from realising the full potential of the data-driven innovation in the economy. This work includes earlier Commission policy documents (Commission Communications on "Building a European data economy [COM(2017)9] and on "Towards a common European data space" [COM(2018)232]), and extensive exploratory study work. The analyses have identified difficulties linked to the access to and the (legal and technical) ability to use data as key barriers to data-driven innovation using techniques of Big Data analytics and Artificial Intelligence in the EU.

The Report of the High Level Expert Group on B2G data sharing also provides an analysis of the problems on B2G data sharing in the EU and offers a set of policy, legal and funding recommendations. Data portability under GDPR has also been interpreted by the Guidelines on the right to data portability of the Article 29 Working Party (WP 242 rev.01).

A number of obstacles were identified. They concern technical barriers (interoperability, safety and security requirements), legal ones (uncertainty about rights on the data, the costs of compliance with existing legal obligations as well as costs of licensing), organisational challenges, the difficulty to control downstream use, the fear of misappropriation and non-availability of skilled labour.

The Impact Assessment can thus build on earlier and upcoming study work, namely:

- Study on data sharing among companies in Europe,
- Study on emerging issues of data ownership, reusability and access to data,
- Study on switching cloud providers,
- Impact assessment study on the Free flow of non-personal data Regulation,
- Results of a 2017 public online consultation,
- Targeted SME panel consultation,
- Impact assessment study supporting the review of the public sector information directive
- Study supporting the evaluation of the Database Directive
- Staff working document on the evaluation of the Database Directive.
- Study on Artificial Intelligence and challenges to the Intellectual Property Rights Framework
- The work of the Support Centre for Data Sharing
- Study on model contract terms, fairness control in data sharing and in cloud contracts and on data access rights
- Study on the legal protection of trade secrets in the context of the data economy (GRO/SME/20/F/206) launched in Q1 2021.

Additional evidence will be sought in terms of the specific costs and benefits of the concrete elements of the measures described above. These costs, benefits and burden reduction/simplification potential will be identified and quantified.

Consultation of citizens and stakeholders

The preparation of the Impact Assessment will rely on a consultation of the stakeholders.

A dedicated public online consultation to be launched in May 2021.

The initiative will also benefit from the findings of past consultations about data-related issues. These are

- the Commission online open consultation on the data strategy that ran from 19 February until 31 May 2020.
- the 2017 public consultation on building a European data economy,
- the 2018 public consultation on the revision of the Directive on the reuse of public sector information,
- the 2017 public consultation on the evaluation of the Database Directive and
- the 2018 SME panel consultation on the B2B data sharing principles and guidance given in Communication COM(2018)232.

Further consultation activities include workshops. Additionally, further targeted dialogues with SMEs will be organised in 2021, as well as sectoral events, allowing for interaction in specific areas, in particular health, industrial manufacturing, agriculture and law enforcement. Finally, the contractors of the support study will contribute to the consultation process, including through interviews with targeted stakeholders (deadlines subject to possible change in light of the COVID-19 crisis).

Will an Implementation plan be established?

Depending on the type of act, an implementation plan would be established. This would in particular suggest mechanisms for business-to-government data sharing where Member States could retain a degree of flexibility in the implementation.