SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

Stockholm, September 2 2021

Comments on the forthcoming Data Act from the Confederation of Swedish Enterprise

Ahead of the announced Data Act the EU Commission published an impact assessment ("the Report"). Our comments in summary are the following:

- The Data Act must not undermine the competitiveness of companies and European industry.
- Relevant existing and planned international regulation and agreements on data access must be taken into consideration in the legislative work.
- We emphasize the importance of achieving rules that are proportionate and - as far as possible - principle-based and technology-neutral. This is crucial for ensuring predictability, encouraging innovative power and creating a positive investment climate.
- The Data Act must not overlap or conflict with existing or planned sectoral and horizontal legislation with the same or similar purposes.
- We oppose rules on mandatory data sharing to be included in the Data Act.
- Companies' willingness and ability to share data is determined by legal, technical, and commercial considerations. It is therefore important that data sharing continues to protect freedom of contract and be conducted on a voluntary basis. Companies must be able to decide whether and how data sharing should take place on a case-by-case basis and consider which underlying technical solutions are used, which business models parties have, and the legal regulations that are applied.
- It is not the role of public policy to manage how and on what terms market actors choose to co-operate.
- It must be legally easier to assess how data can be shared, in particular with regards to intellectual property rights, integrity, and competition law. In Sweden, it must also be ensured that information shared by companies is covered by confidentiality and thus cannot be passed on to other actors due to the principle of public access.
- The revision of the Database Directive must ensure that the protection of databases and the protection of business secrets is fully respected, although this does not necessarily imply an exclusive right to such content per se.

Below are our more detailed comments on the issues raised by the Report.

Business to Government Data Sharing (B2G)

Business to Government (B2G) data sharing refers to the practice of companies making their data of general interest available to public bodies. Initiatives aimed at increasing B2G data

Confederation of Swedish Enterprise
Address: SE-114 82 Stockholm Visitors: Storgatan 19 Phone: +46 (0)8 553 430 00
swedishenterprise.se

sharing must not undermine the competitiveness of companies and European industry. Rules that force companies to share their data with the public are extremely intrusive. In many cases, data that companies generate are vital to their operations, and the business advantage of producing information can be lost if companies are forced to share data with the public sector through expropriation-like rules.

B2G data sharing already takes place in several different ways.[1] There is no specific data sharing model that is suitable for all situations, and circumstances of specific cases should always be considered.

Sweden has rules on mandatory data sharing that require companies to fill in millions of forms every year with information requested by Swedish authorities. The same or similar information is often requested by different authorities, entailing duplication of work for companies. Instead of imposing additional requirements on data sharing for companies, authorities should work to reduce, simplify and facilitate current requirements so that resources can be freed up to develop their own operations and contribute to growth and societal benefits.

Principle of proportionality and subsidiarity

Companies need proportionate, principle-based and technology-neutral legislation that provides sufficient predictability, innovation incentives, and a favourable investment climate. The Data Act must not introduce additional regulation where there are already initiated or existing sector-specific and horizontal legislation with the same or similar purposes.

For example, the Directive on open data and re-use of public sector information (the Open Data Directive, 2019/1024) was adopted in 2019. The directive has been supplemented by proposals for the Data Governance Act (DGA), which aims at making certain types of public data available that are not already covered by the Open Data Directive.

The Open Data Directive and the DGA seeks to, among other things, increase the amount of public data. Data generated by public bodies on, for example, statistics, demographics, public transport, meteorology and geographical data may lead to further development of existing activities and for producing new solutions to societal problems. This can also contribute to a more transparent society and increase trust in the public sector, thereby contributing to a stronger culture of data sharing.

The Open Data Directive is just now being implemented in all member states and the DGA has not yet been adopted. Furthermore, many companies anticipate the introduction of additional sector-specific data sharing legislation. The effects of these initiatives must be taken info force and be evaluated before any further regulation is considered.

---

[1] Companies are legally required to provide comprehensive information to authorities. For example, there are requirements for incident reporting in the General Data Protection Regulation (GDPR) and the Directive on network and information systems security (NIS). Companies and authorities may enter into data sharing agreements for specific amounts of data and enter into partnerships for more long-term and continuous data sharing. Companies may also choose to make available data of general interest to the public sector as part of social responsibility efforts by donating data. Third parties may be hired to process data and ensure that data that is of general interest is shared without the responsible authority having full access. Another model involves the public sector offering rewards to encourage private actors that specialise in data analysis to identify solutions to specific problems of public interest.

The concept of “public interest”

Most companies agree that for specific use-cases with a clear public interest B2G data sharing are necessary with appropriate safeguards.

B2G data sharing must however be limited to data *necessary* to satisfy such specific public interests. A clear definition of the term “public interest” is needed to counteract uncertainty over which data is subject to B2G data sharing.

Legal obstacles

Existing legislation relating to B2G (and B2B) data sharing needs to be reviewed so that it becomes legally easier to assess how data can be shared, in particular with regards to intellectual property rights, integrity, and competition. In this respect, Sweden and Finland face particularly severe challenges with data sharing to the public sector due to the principle of public access, a principle that makes companies often hesitant to provide sensitive information to authorities. It must therefore be a legal requirement that information shared by companies is covered by confidentiality and thus cannot be passed on to other actors.

Compensation for B2G data

Possible remuneration for B2G data could, where applicable, be made as one-off payments for each shared amount of data, or possibly under a licensing agreement. Compensation should also cover, for example, companies’ costs relating to the development of secure systems for sharing data as well as costs associated with encryption and anonymisation.

Business to Business Data Sharing (B2B)

The concept of Business to Business (B2B) data sharing refers to companies sharing data with other companies. Except for certain mandatory sector-specific regulations, B2B data sharing is mainly governed by freedom of contract between parties present on markets.

Companies’ data sharing policies reflect, among other things, customer integrity protection, compliance with data protection rules, commercial considerations, and interoperability issues. Being forced to share data in combination with strict personal data protection requirements gives rise to many complex issues and jurisdictional challenges. In cases where the information to be shared contains personal data, the GDPR may prevent sharing. In such situations, anonymisation may be a solution, but these measures are both time-consuming, risky, and costly. Copyright must also be considered when data is or must be shared, primarily in terms of who must grant consent for a possible transfer of data.

As freedom of contract prevails, data is now shared between companies in many different ways. How the breakdown of sharing looks in specific cases may depend on which underlying technical solution is used, which business models parties have, and the specific legal regulations that are applied.

Swedish Enterprise believes that data sharing from companies should continue to safeguard freedom of contract and be conducted on a voluntary basis. This view is also reflected in the European Commission’s consultation from 2018, which states that the starting point should be to ensure that data markets have the best possible conditions to develop independently, based on the freedom of contract.[2]

[2] EU Commission, *Towards a common European data space*, 2018.

The starting point should therefore continue to be that companies are free to decide, for example, who and on what conditions data – that does not constitute personal data – are shared with other companies. However, other measures are welcome to help facilitate voluntary B2B data sharing, such as promoting the use of APIs, the development of standardised contract terms, and EU guidance.

A special type of B2B data sharing involves P2B (platform to business) data sharing. The proposed Digital Markets Act (DMA) includes requirement for certain platforms, so-called gatekeepers, to be forced to share data with its business customers in certain cases.

Swedish Enterprise argues that it is justified to deviate from the principle of freedom of contract and voluntary P2B data sharing in the DMA. However, this is not straightforward and presupposes that any data sharing is preceded by a dedicated regulatory dialogue to ensure that sharing is compatible with applicable legislation (data protection rules, copyright, competition law, and other legal frameworks covered by respective gatekeepers). The DMA is now for consideration in the Council and the European Parliament, and at this stage there should be no additional requirements for mandatory B2B data sharing in the Data Act.

Smart contracts

The Report states that smart contracts have an untapped potential to facilitate B2G and B2B data sharing and established rights to data portability. According to the report, what is missing are harmonized standards for smart contracts, which undermines interoperability and limits the use of such contracts.

Smart contracts may be an option for some companies, but decisions to use smart contracts must be based on freedom of contract and on a voluntary basis. The need for standards must be market-driven. It is not public policy's role to drive forward how and on what terms market participants choose to co-operate in the Data Act.

Clarifying rights on non-personal Internet of Things data stemming from professional use

To maximise the benefits of generated data, market participants may need to access and use data from other companies. For example, in terms of data generated from the Internet of Things (IoT). According to the Report, some manufacturers have carved out very powerful positions, which allows them to decide who gets access to and who can use data generated from their services. However, this is an issue that should not be further regulated in the Data Act. This approach is also supported by a consultation previously initiated by the European Commission which states that actors consider it premature to introduce comprehensive legislative measures regarding data sharing between companies, and that the existing legal framework is sufficient.[3]

Cloud Data Portability

It should be possible for users to easily choose between cloud services, software, and platform services that meet requirements for, among other things, security, data protection,

[3] EU Commission, *Summary of the public consultation on Building a European Data Economy*, 2017.

and data portability. The technological development of these services is rapid, and it is not appropriate to complete or build on existing codes of conduct and certifications in the Data Act.

Article 20 GDPR Portability

It follows from the EU's Data Strategy that opportunities to expand individuals' rights to data portability under the GDPR must be reviewed. The right to data portability means that those who have submitted their personal data to a personal data controller in certain situations have the right to obtain such data themselves and demand direct transfer of such data from the personal data controller to another controller *where technically feasible*. In other words, the right to data portability presupposes interoperability.

For particularly mature technology markets, the development of market-driven standards that support interoperability and technology transfer may be a solution. However, in new technology markets, standards risk restricting innovation, especially among start-ups. Work on standardisation is strategically important, but it must not hinder innovation or market-driven, consensus-based processes.

IP Protection in relation to Databases (Database Directive)

The revision of the 1996 database directive to adapt to current conditions is most welcome. It will be especially relevant for the review to clarify the legal conditions regarding data access in B2B and B2G data sharing. In this context, it is important that the protection of databases and the protection of business secrets functions as intended. It will be important to ensure that protections are fully respected. However, this does not necessarily mean that protections must imply exclusive rights to the content of given information per se. The protection of business secrets does not confer an exclusive right to the information itself, as this would be contrary to the freedom of information, (for example Article 10 of the ECHR). Database protection does not give an exclusive right to data as such, but rather its compilation.

Safeguards for non-personal data in an international context

The Report states that there may be legitimate situations when authorities in third countries request access to information from private actors. The GDPR prescribes rules and safeguards in this regard. However, for non-personal data there are currently no rules which mean that the person who has been requested to disclose such non-personal data is subject to EU legislation on the protection of intellectual property and business secrets. When considering such rules, it is also important to consider relevant existing and planned international agreements on data access, in particular in negotiations with the WTO, the UN, the OECD, the ILO and UNESCO.