WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

eco Position Paper on the Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) COM (2022) 68 final

Berlin, 01.06.2023

With the Data Act, the European Commission aims to create a legal framework to improve the use of non-personal data and make it easier for businesses and citizens to access different types of data, covered by the proposal. To this end, data silos are to be broken down by obliging data holders to share their data. Users of connected products are to be granted a right to data portability, comparable to Article 20 of the GDPR. Users should be able to share data with third parties so that they are able to use their services. The Data Act also provides for public sector bodies to have access rights to corporate data under certain conditions – for example, in order to be able to respond to public emergencies. New rules are also planned for providers of data processing services. The Commission's aim here is to make it easier for users to switch between different providers and to prevent log-in effects.

In principle, eco supports the Commission in its goal of creating an innovation-friendly and uniform legal framework for the handling of non-personal data. However, in a position paper which we published on the Commission's draft, we included a number of comments.

Both the European Parliament and the Council of the European Union have now set their negotiating mandates for the trilogue negotiations. eco would like to take this opportunity to point out relevant points that, from the perspective of the Internet industry, should be further taken into account in the negotiations.

1. The scope

The report of the European Parliament and the general approach of the Council of the European Union both advocate changes to the scope of the Data Act. In its report, the Parliament proposes a broader definition of "connected products". The definition in Article 2 (2) now also includes products that are not tangible or movable. The Council approach maintains the definition of tangible products but deletes the requirement that the product must be movable in order to fall under the rules of the Data Act. Both approaches constitute an expansion of the scope that the Data Act provisions are set out to cover.

Overall, we are not in favour of the scope's expansion proposed by both the Parliament and the Council. Both definitions lack clarity as to which products are considered as part of the Data Act's scope. The proposed definitions could therefore create legal uncertainty for manufacturers and operators. What therefore needs to be clearly defined is to whom the rules of the Data Act apply.

The Parliament, like the Council, also imposes limitations on the types of data that fall under the sharing obligation. The Commission's draft proposed that all data generated by the use of a connected product would fall under the sharing obligations and the scope of the Data Act, i.e. not only raw data but also data and data sets generated from it. In contrast, the Parliament's report creates exceptions for aggregated data generated by algorithms in Article 3 (1), for example. The Council clarifies in Article 2 (1af) of its general approach that data modified by the processing shall not be part of the scope of the chapters II and III. In addition, the Parliament does exclude personal data from the scope of chapter V, which regulates the access rights of public sector bodies.

From the perspective of the Internet industry, the decision to exempt algorithm-based data from the sharing obligation is understandable. It can help protect trade secrets and ensure that investments in algorithms or data-driven business models as a whole continue to be rewarding for companies. Nevertheless, in order to achieve the goals of the Data Act, it should be carefully considered as to whether a general exclusion of algorithm-generated data makes sense. In general, the introduction of different data categories – some of which fall under the sharing obligation and some of which do not – could result in legal uncertainty; for example, if companies are not able to clearly distinguish between these categories. In particular, SMEs – which usually do not have large legal departments – could find the implementation of the Data Act even more difficult. For this reason, the Data Act should provide definitions that can be the clearest and most easily understandable.

2. On the interplay with the GDPR

To ensure a smooth application of the Data Act and to create legal certainty for the companies concerned, eco regards it as important to create clarity with regard to the interaction with the GDPR. This is particularly important with regard to mixed data sets that contain both personal data and non-personal data.

Both the Parliament and the Council have recognised this problem and are addressing it in their positions. To this end, various clarifications have been made compared to the original version. Even if the proposal is moving in the right direction, we would like to point out that the rules must be suitable for everyday use, which we believe is still not the case.

In principle, the Data Act follows the logic of the GDPR in parts, as far as the handling of non-personal data is concerned. Both the Council and the Parliament leave this approach largely intact. From the perspective of the Internet industry, it is still important to emphasise that non-personal data should be treated differently than personal data in regulatory terms. No fundamental rights are affected by the processing of non-personal data, such as the right to privacy or informational self-determination. From eco's point of view, when it comes to the processing of non-personal data generated from the use of a connected product or one of its services, it makes no sense that it should only be processed with the explicit permission of the user. The penalties provided for in the event of non-compliance are also based

on the GDPR. The Data Act must take greater regulatory account of the different sensitivities with regard to processing and not create new hurdles for data use. Given that the GDPR allows for personal data to be processed for a “legitimate interest”, it makes no sense that data holders are not granted the right to process non-personal data for a “legitimate interest”. The Internet industry therefore calls for improvements in this context.

3. Protection of trade secrets

The Data Act also potentially affects trade secrets of data holders through the intended obligation to share data. It cannot be ruled out that trade secrets, even if they are subject to protective measures, are used by a third party to develop competing products or services. Both the Parliament and the Council have supplemented the Commission’s draft in this field.

The Council’s general approach creates a mechanism whereby data holders can refuse to hand over data to a third party under certain conditions. However, according to Article 4 (3a), this should only be possible in “exceptional circumstances” if it is very likely that the data holder could suffer great harm, in spite of technical protection measures. The mechanism envisaged in the Parliament’s report would allow data holders to suspend the disclosure of data to third parties if the third party is not able to ensure the protection of trade secrets or undermines the agreements to protect them.

From the perspective of the Internet industry, the inclusion of such mechanisms for the protection of trade secrets is welcome. However, adjustments should still be made to these mechanisms to enable effective protection. For example, the path proposed by the Council is still tied to very high requirements for data holders, with these being difficult to fulfil. It is questionable whether these can ensure an adequate level of protection, since even damage that is not existentially threatening to a business model ultimately harms the data holder and can nevertheless be significant in the long run due to the potential use by a large number of third parties. The report of the European Parliament offers a mechanism to limit – but not to prevent – damage already caused by the leakage of trade secrets. For some companies, such misuse can threaten their existence, which is why we believe it is important to be able to refuse the disclosure of trade secrets from the outset. In addition, in order to avoid an extra burden for data holders, they should not have to assume liability for the data they provide, especially with regard to damages caused by the use of third parties. We therefore positively assess the Council’s initiative in this direction. Even with the present amendments, there is nonetheless still a question regarding the enforceability of confidentiality agreements, especially between data holders and third parties. The data holder must therefore be in a position to see to whom the shared data has been passed on.

4. On the prohibition of “unfair” contract clauses

The Data Act also regulates business-to-business (B2B) contracts in the area of data sharing. The aim is to prohibit practices and contract clauses that are classified as “unfair”. The Commission’s original aim was to protect and prevent SMEs, in particular from the market dominance of large providers. In the Council and Parliament versions, this prohibition of practices which are deemed to be unfair is now extended to all companies, regardless of their size. The Parliament’s report would like to grant the affected companies a 3-year transition period, whereas the Council proposes not to provide for a transition period after the entry into force deadline.

eco has already critically assessed Article 13 in our statement on the Commission’s draft. It is understandable that the Commission has decided to support SMEs and to protect small businesses from unfair practices, but we do not consider the means chosen here to be suitable. On the one hand, it interferes with the freedom of contract and, on the other hand, the proposed rules are not practicable. Especially in the case of mass contracts, it is not possible to negotiate each Article individually. This would lead to considerable additional work and make the sharing of data between companies more difficult and less attractive. What is also particularly critical to note is that there is to be interference in already existing contracts. Businesses need to be given the necessary time to adapt to the new legislation. The fact that Article 13 has been extended to all companies instead of providing tailored support for micro-enterprises or start-ups is viewed negatively by eco.

5. On compensation possibilities for data holders

The generation and collection of data is often associated with an enormous use of resources by the providers of data-driven business models. Theoretically, the Data Act offers the possibility for the data holder to demand compensation for data access. However, at the same time, the Data Act also sets limits on the possibility for compensation. In principle, access for users of a connected product to the data created during use should be free of charge. In the context of data use by third parties, “reasonable” compensation should be possible in some cases.

From the perspective of eco, even though the existing provisions represent an improvement over the Commission’s draft, the included regulations on compensation levels and possibilities are still insufficient. Also, the additions of the Council which set out investment costs as provision costs make it unlikely that the costs listed here cover the actual costs of provision. It must be ruled out that the obligation to disclose to third parties causes economic damage to data holders. In this context, we are not in favour of the Commission’s guidelines on the costs of providing different types of data, as requested by Parliament in Article 9 (2a). The actual costs can differ between different companies, situations, sectors and scopes to such a degree that an all-encompassing approach by the Commission can be considered unlikely. The exemptions for SMEs should be critically challenged – particularly in view of the fact that the vast majority of companies in Europe belong to this group, and it will therefore not be possible in many cases for data holders to

earn money from the data covered by the Data Act. This would deprive companies of an important incentive to invest in data-driven business models in the first place. We would therefore propose to limit the exceptions to micro and small businesses. Nevertheless, we welcome the fact that access by public authorities in some cases of "exceptional need" would lead to the receipt of compensation that can also exceed the pure provision costs.

6. On the access rights of public sector bodies

The Data Act not only provides for user access and sharing of data from connected products, but also for public sector bodies to access data from private companies. Access by public bodies should be necessary in the event of "exceptional needs" on the part of the authorities. In comparison to the Commission's draft, the Parliament and the Council set out to partially restrict the access possibilities of public authorities. Article 14(1) of the Parliament's report and Article 15 of the Council's general approach, for example, stipulate that these requests should be limited in time and scope and should also exclude personal data from the obligation. The definition of public authorities also includes research institutions, which may also process data used by public authorities for statistical purposes.

Overall, the access rights for public sector bodies remain extensive. The definition of public sector bodies remains broad. In addition, the definition of "exceptional needs" is changed somewhat by the Council and the Parliament, but it remains unclear in both cases and, in our view, comes across as too broad. Furthermore, public authorities may also invoke "exceptional needs" to access data if they have to perform statutory duties in the public interest. In our view, the temporal limitation of these "needs" demanded by the Council and Parliament is not sufficient as a restriction. It is unclear whether the "single point to handle public sector bodies' request" envisaged by the Parliament can effectively contribute to a reduction of the administrative burden.

As we see it, access by public bodies to the data of private companies must remain the exception and should be limited to non-personal data. In particular, not only the protection of business secrets, but also the bureaucratic burden of processing such requests must be taken into account. eco is therefore of the opinion that a clear and limited definition of public emergencies is required.

7. On the regulation of data processing services

The Data Act will also regulate providers of data processing services. The aim of the Commission is to prevent lock-in effects and to simplify switching between different providers for users. To this end, the Data Act creates new rules regarding switching fees, notice periods and interoperability of the services regulated here.

As an association of the Internet industry, we support the goal of ensuring fair competition between different providers. However, we believe that the means chosen by the Commission should be reconsidered, especially as they interfere in part with the freedom of contract between a provider and a user. The complete abolition of switching fees is understandable from our point of view, but we regard

it critically. In addition to the encroachment on contractual freedom, it is not certain whether the intended regulations on charging for the technical costs of switching are sufficient to absorb the actual costs incurred by a provider as a result of switching. The definition of a maximum transition period, as is spelt out here, is also not appropriate in our view. Although the transition periods were increased by the Parliament and the Council in comparison to the original draft, they are still too rigid to take into account the actual complexity of a switching process in every case. A better alternative would be a formulation on which the provider would complete the switch "without any delay based on the provider's own disruption". The standards ordered here for the interoperability of individual services are also very far-reaching and, in some cases, deeply interfere with the business models of the individual providers. This could ultimately weaken competition, as providers of data processing services would have to align them strongly in order to achieve functional equivalence.

8. Summary

The Data Act is intended to kick-start the data economy in Europe and provides for deep interventions in this industry. In our estimation the practical implementation and the scope of the data sharing obligation are still unclear. We support the goal of increasing data sharing in Europe and breaking down data silos. We also see a need to create a uniform legal framework for the use of non-personal data in order to better leverage the potential for value creation in Europe. However, this requires that companies investing in data-driven business models are not overly exposed to bureaucracy and uncertainty. To this end, we propose the following points which, from the perspective of the Internet industry, should be taken into account in the trilogue negotiations:

- Create a clear scope of application
  In order to give companies and users in the EU legal certainty, it is necessary to clearly define the scope of the Data Act. To this end, it is important to precisely define for whom which rules apply and to what end, with this also to be defined in terms of simple applicability by SMEs. The current approaches of the Council and the Parliament do not manage to eliminate all ambiguities.

- Enabling data use
  The Data Act should enable the use of non-personal data through a uniform legal framework. Restrictions that are not justified by the protection of fundamental rights or trade secrets should therefore not be part of the Data Act. We therefore reject a ban on processing non-personal data without the user's consent.

- Consistently protect trade secrets
  The data sharing obligation provided for in the Data Act must not lead to a weakening of trade secrets. It is therefore necessary to empower data holders to determine which data they consider to fall into the category of trade secrets. In addition, strong rules against the development of competing products are needed. Data holders should also be able to prevent the disclosure of data if they have legitimate concerns about economic harm.

- Restrict data access for public sector bodies
  Public bodies should only be able to access data of private companies in narrowly defined emergencies. To this end, the group of authorised public bodies should be limited to those that are actually involved in the fight against an emergency. Data access by public bodies must remain the exception.

- Strengthen incentives for companies
  Companies should be encouraged to share data. We are of the strong opinion that this requires incentives above all. Data holders should be given the opportunity to share their non-sensitive data with other companies on data marketplaces under clear rules, in return for compensation. Above all, this requires incentives for common standards. However, this is barely addressed in the Data Act. Instead, as it presently stands, the Data Act would create more bureaucracy for data holders.

- Create fair rules for providers of data processing services
  We advocate fair competition between providers of data processing services. However, the regulations envisaged here go too far. Rigid deadlines for switching, notice periods that are too short, and a complete abolition of switching fees should be avoided. In our view, the obligation to establish functional equivalence interferes too deeply in the providers' product design.

About eco

With more than 1,000 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust and ethically oriented digitalisation. That is why eco advocates for a free, technology-neutral and high-performance Internet.