Vodafone Position Paper on EU Data Act

General Remarks

Vodafone welcomes the publication of the EU Data Act and the overarching aim of the legislation to facilitate increased sharing and reuse of data in the digital economy. The legislation chimes with the findings of our recent report with Capgemini on Cloud-edge Sovereignty that with the right policy framework, increased interoperability and portability could generate up to 576 billion euros in extra value for EU organisations from industrial data exchange and collaboration within and across sectors. In particular we focus on the need for a harmonised approach to data sovereignty that is strategically open and backed up by fit for purpose regulatory oversight to realise this potential.

The EU Data Act goes a long way towards achieving this, helping to clarify the rights and obligations of different parties involved in generating and processing data and introducing strong new regulatory obligations for cloud service providers to facilitate switching and interoperability. We harbour some concerns about the proposed regulation however, in particular on the scope and modalities of Business to Government (B2G) data sharing and the potentially prescriptive and overly burdensome nature of some of the new rules on B2B data sharing and international data transfer. We are confident that with these issues addressed the Data Act can form a solid foundation for the EU to realise it's ambitions for enhanced data sharing and reuse across the single market, in the interests of both businesses and citizens.

Detailed views

I. Business to Business Data Sharing

As a leading IoT provider, Vodafone has a strong interest in the provisions under Chapter II of this regulation to stimulate sharing and reuse of data stemming from connected objects and associated services. We have for some time argued in favour of the introduction of FRAND conditions to underpin data sharing between providers in the IoT value chain, recognising that at present a lack of clarity around the respective rights and obligations of different parties can prevent data from flowing as freely as it should. Vodafone wishes to play a more active role in digital services space and facilitate the emergence of European digital champions via its added value services in the field of agriculture, health and mobility.

We are therefore supportive of the obligations under Article 3 for designers and manufacturers to make the data generated by IoT products accessible to users, and to provide additional transparency as to how and when that data can be used and shared with third parties. We would suggest the introduction of some mitigating language in the text however to recognise that this may not always be feasible in the context of IoT products that either lack a direct user interface or are designed and manufactured for the enterprise rather than consumer market.

With reference to Article 4, we underline that the regulation needs to strike a careful balance between the overlapping interests of various parties, and while welcoming the new right for users to access data they have contributed to generating, we note this must be weighed carefully against the legitimate

right of data holders to invest in and market proprietary solutions and to be able to obtain a fair return on those investments. In this sense we would prefer the regulation afforded greater room for the fundamental principles of the market economy to develop, particularly in still nascent markets such as for the sharing of data.

We propose two concrete changes to the text to achieve this: firstly, qualifying the obligations on data holders here to alleviate the potential compliance burden, by clarifying that only the data that users have immediately contributed to generating should be accessible (and that ancillary data should therefore be out of scope). Secondly that to remove the obligation to provide data "continuously and in real time" as we believe this requirement would be unworkable and overly burdensome in practice.

Furthermore, we underline the need for the regulation to adequately respect the integrity of trade secrets and intellectual property rights for data holders and would suggest that the text be altered to ensure that these intangible assets should not be disclosed as a result of the obligations under this regulation.

The Data Act interacts with and complements current and planned legislation in several important ways. It is our view that the Commission has taken the correct approach in stipulating that none of the provisions in this legislation are prejudicial to the data protection and confidentiality rights provided under the General Data Protection Regulation (GDPR) and ePrivacy Directive. Furthermore, we support the view that the EU Data Act should not result in the creation of any new grounds for data processing under GDPR. Lastly the regulation foresees an interaction with the forthcoming Digital Markets Act: we strongly agree with the Commission's proposal that companies designated as Digital Gatekeepers under the DMA should not be direct beneficiaries of the new data access rights enshrined under this legislation.

Commission proposed text	Proposed Amendments
Article 3	**Article 3**
1.Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user	1.Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, ~~by default~~, **where possible and feasible** , ~~easily, securely and, where relevant and appropriate~~, directly accessible to the user
Article 4	**Article 4**
1.Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.	1.Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data **immediate** generated by its use of a product or related service without undue delay, **and** free of charge ~~and, where applicable, continuously and in real-time.~~ This shall be done on the basis of a simple request through electronic means where technically feasible.

3. Trade secrets shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.	3. Trade secrets shall **not be** ~~only be~~ disclosed **as a result of the obligations under this regulation** ~~provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties.~~ The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.

II. Business to Government Data Sharing

Vodafone has long advocated for a sustainable regulatory framework for B2G data sharing that allows the emergence innovative new business models, innovative public-private partnerships. In our experience cooperation between MNOs and the public sector is broadly well-functioning, with operators able to supply governments and public bodies with timely data insights to help them improve their decision making and delivery of public services. Vodafone sharing partnerships include mobility, out-of-home advertising, footfall and smart retail for 'clients' such as European Space Agency, Ferrovial, Lisbon City Council, Istat, Banca D'Italia, Andalucia region, INE Tourism in Spain.

This regulation can emphasise further that voluntary data sharing arrangements, based on the principle of fair remuneration provide the most sustainable long-term footing for B2G data sharing.

We do recognise however that in certain, limited circumstances, business may waive their rights to compensation and provide governments with access to data either for free or at cost. Article 14 of the regulation describes how business would need to make data available to public authorities in situations of exceptional need; we would suggest to amend the text here to clarify that any such request for access to privately held data must be specific, duly substantiated and time limited.

To clarify the matter further, Vodafone would propose to include within the regulation an exhaustive list of all the situations that are deemed to constitute a public emergency, whereby compensation rights may be waived. In our view these circumstances should be limited to the following situations: public health emergencies, emergencies resulting from environmental degradation and major natural disasters including those aggravated by climate change, as well as human-induced major disasters.

For other, non-emergency situations, public authorities may request access to privately held data based on the existence of an exceptional need. These circumstances are understood to be less serious and more frequent and should therefore be subject to fair remuneration. We support the inclusion of a market failure test within the regulation, with the burden of proof sitting with the public authority to demonstrate that they have been unable to obtain data on the open market, before invoking the data access rights under this regulation We also underline here the importance of strong safeguards for data holders within the regulation, for example those that ensure security and confidentiality of data, and that personal data of EU citizen's is not unnecessarily disclosed in complying with a data access

request. We also support the "once only" principle that companies should be protected from multiple and repeat requests to access the same data. Lastly, we underline the need to ensure better training and availability of skills necessary to effectively structure, analyse and action data within public agencies as we have found in the past these skills to be sorely lacking. This is often one of the greatest inhibitors to effective and timely supply of data from private companies to the public sector.

Commission proposed text	Proposed Amendments
Article 14	**Article 14**
1. Upon request, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested	1.Upon receipts of a specific**, duly substantiated and time limited request**, a data holder shall make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested.
Article 15	**Article 15**
An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances: (a) where the data requested is necessary to respond to a public emergency;	An exceptional need to use data within the meaning of this Chapter shall be deemed to exist in any of the following circumstances: (a) where the data requested is necessary to respond to a public emergency; **including the following situations: public health emergencies, emergencies resulting from environmental degradation and major natural disasters including those aggravated by climate change, as well as human-induced major disasters** **For other, non-emergency situations, public authorities may request access to privately held data based on the existence of an exceptional need. These circumstances are understood to be less serious and more frequent, and should therefore be subject to fair remuneration:**
Article 20	**Article 20**
1. Data made available to respond to a public emergency pursuant to Article 15, point (a), shall be provided free of charge.	1.Data made available to respond to a public emergency pursuant to Article 15, point (a), **may be provided free of charge with the data holder choosing to waive their right to compensation in recognition of the existence of a public emergency**

III. Cloud switching and interoperability

Vodafone is a strong supporter of the new regulatory obligations for providers of data processing services to facilitate switching and interoperability between cloud and edge services. These measures are well aligned with the findings of our recent support on cloud-edge sovereignty, which found that the EU cloud market today is insufficiently regulated, and therefore binding new rules are required to drive competition in the market and deliver the outcomes around, security, data portability and service interoperability that consumers are looking for.

Measuring the trade-off EU organisations are willing to make between trust and price, our report shows that EU organisations are willing to pay extra for trust. This is especially true if the price difference can be contained below a 10% surplus relative to global market average – at which price point the number of EU organisations willing to choose cloud-based solutions increases compared to today's situation.

One important clarification that should be made within the regulation is that the obligations under Chapter VI apply exclusively to providers of data processing services, and not to companies that re-sale, bundle or aggregate different cloud services within a multi-cloud portfolio. Indeed, providers of such multi-cloud offerings are looking to achieve the exact aims of the EU Data Act; reducing vendor lock in, driving innovation and creating additional value for the cloud customer, and should therefore be the primary beneficiaries and not the intended targets of this regulation.

IV. International Data Transfer

Vodafone is concerned that new transfer restrictions beyond personal data could entail significant unnecessary administrative burden and disruption on how companies innovate, collaborate with subsidiaries and commercial partners outside the EU.

In particular the requirements under Article 27 that providers take "all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union" is insufficiently clear on the precise obligations incumbent on businesses and when they would apply.

We suggest the text is amended to stipulate exactly what constitutes *all reasonable measures* for this purpose, and to provide indicative examples of when such a conflict of law would (and would not arise). We also request further clarity on what impact a country holding an Adequacy agreement with the European Union has on the application of Article 27 for service providers based in that country.

Therefore, we encourage legislators to clarify the intended objective of this provision, as it is currently unclear how this advances the objectives of the Data Act and to state explicitly that any new requirements should be proportionate to the actual risk of unlawful data access and should not constitute an unfair or arbitrary barrier to transfer of non-personal data to third countries.

Commission proposed text	Proposed Amendments
Article 27	**Article 3**
1. Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3	1. Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union**. Such measures should only apply in situations** where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3 and **should not constitute an unfair or arbitrary barrier to transfer of non-personal data to third countries.**