Position Paper

Public consultation on the Data Act

2021 September 3

Summary

In context of the European strategy for data and after the proposal for a Data Governance Act, the European Commission (EC) recently published its roadmap for a Data Act & amended rules on the legal protection of databases (Data Act Roadmap) and subsequently launched a public consultation on the Data Act. Its main goal is to tackle barriers to data sharing. Among the key pillars of the Data Act are B2G and B2B data access and use, cloud services portability, and rights in the context of smart objects.

Bitkom is grateful for the opportunity to contribute to the consultation on the Data Act and welcomes future occasions to offer its expertise in open discussions.

In a nutshell, the EC's public consultation is an important step for the European data economy. We explicitly encourage the motion to increase B2G and B2B data sharing to foster an open, European data economy to bring together various actors in a fair and efficient manner and suggest more incentives to encourage it further. At the same time, applying the current legal framework and the SWIPO CoC are powerful tools to address most of the issues at hand. Generally, technical issues are best solved among subject matter experts and less via direct regulation, for example details on portability.

By means of this Position Paper, we would like to **supplement our replies** to the Data Act public consultation. For convenience, our comments are aligned with the structure of the questionnaire.

Annex

- Brief legal opinion on EC jurisdiction over cloud portability

This page of the document has been edited on 11 October 2021 after submission of this document to the EC's public consultation as the submitted version mistakenly referred to the (Data Act) Roadmap (questionnaire) instead of the Data Act public consultation at two occasions and mentioned a *proposed* Data Act.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Rebekka Weiss, LL.M.
Head of Trust & Security
P +49 30 27576-161
r.weiss@bitkom.org

David Schönwerth
Data Economy
P + 49 30 27576-179
d.schoenwerth@bitkom.org

David Adams
Manager EU Public Policy
P +32 471 92 78 90
d.adams@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Content Page

As a preliminary remark, we consider it crucial to fully align the Data Act with any other pieces of legislation, pending initiatives, and reviews. In particular, potential links or even contradictions with files such as Free Flow of Non-Personal Data Regulation, GDPR, Industrial Strategies, and pending initiatives such as E-Privacy, DGA, DMA must be kept in check. Legal uncertainty around data remains a key concern for many businesses and could weaken the effect of the proposed mechanism.

I. Business-to-Government data sharing

a. To what extent do you believe that the following factors impede B2G data sharing for the public interest in the EU?

i. Commercial disincentives or lack of incentives/interest/willingness.

The willingness of businesses to share data with public authorities for public interest purposes is sufficiently high as they are keen to contribute to the public good where they can. **However, there is a general lack of incentives to share data for public interest.** Data sharing can come with significant effort for businesses both upfront and over time for example to run such system as well as to ensure compliance. At the same time, it is often unclear what impact B2G data sharing will have in practise, which is suboptimal for business decision-making. Especially if B2G data sharing projects carry an abstract, future public benefit, and as they compete for resources against other (public interest) projects, they may not be the preferred option by all businesses.

ii. Lack of skilled professionals (public and/or private sector).

In particular, the public sector appears to experience difficulties in hiring, training, and maintaining qualified data professionals as well as in building necessary expertise in-house.

iii. Lack of appropriate infrastructures and cost of providing or processing such data.

As explained, the private sector may have difficulties in justifying B2G data sharing business cases (i.e., costs and benefits) but generally holds the required capabilities in terms of infrastructure and staff needed. Still, hiring and retaining staff with data-related skills is difficult as there is high demand.

At the same time, the public sector may lack appropriate infrastructure (on premise, cloud, hybrid) to handle state-of-the-art data sharing requests, for both ingoing and outgoing requests. Similarly, it may experience difficulties in hiring and retaining staff with data-related skills that go beyond the private sector's, due to different staffing priorities, formal requirements, career prospects, compensation grades, branding, among others.

iv. Lack of awareness.

Bitkom members are well-aware of the enormous potential of data for society and are keen to contribute to B2G initiatives where benefits are aligned with cost.

For different reasons, the public sector may not be aware of such data potential to the same degree. While this is obviously linked to technical capabilities, it is further linked to a lack of insight into which datasets exist. We expect fair incentives for B2G data sharing to improve insights given by the private sector vis-à-vis the public sector.

v. Insufficient quality of public authorities' privacy and data protection tools.

With respect to tools in general, many types of datasets risk losing their meaningfulness once taken outside of their concrete business context. This is because analysis and interpretation of data often depends on business frameworks and procedures and can be difficult to mirror without relevant expertise. In addition, the possibility of committing analytical errors or misinterpretations appears imminent once data is in second hands.

Simply sharing (personal) data with public authorities may carry strong non-incentives such as in the following cases.

- Public authorities are not necessarily aware which personal or sensitive data may be found in a dataset.
- By analysing a shared dataset, public authorities may obtain findings or correlations that may contain privacy-sensitive information.
- By combining a shared dataset with other sources of information, public authorities may generate formerly unknown privacy-sensitive information about individuals.

b. When sharing data with public bodies, businesses should provide it?

Like in virtually any other area of public procurement, paying fair market prices should be the default option to obtain business data as it leads to competition, innovation and a

level playing field. Additional rules in that area should, however, be coherent and include learnings from existing frameworks (eg the new German Competition Act) or regulation already in progress, such as the Digital Markets Act.

Firstly, paying a fair price for datasets can foster competition between businesses to share data with public bodies that, in turn, can encourage technological innovation, such as in the field of data quality, which is crucial for the success of data sharing.

Secondly, fair prices avoid tilting the playing field, for example towards businesses outside of the potential geographic scope of such a free-access regime to the detriment of European businesses.

Thirdly, public agencies who want to obtain data via B2G data sharing have a genuine interest to support the European data ecosystem by creating demand.

Finally, from a privacy and civil liberties perspective, doubts or lack of acceptance could arise if public authorities freely accessed and used countless datasets without oversight, including budget oversight.

At the same time, many businesses voluntarily decide to provide dedicated discounts or (even waivers) for defined purposes in areas such as education, social services, crisis management, or health care. Thus, in line with contractual freedom, we suggest including in the Data Act (i) an option for preferential rates including waivers for certain purposes in certain areas and (ii) to explicitly define such purposes and areas.

c. What safeguards for B2G data sharing would be appropriate?

While all the given categories of safeguards necessary and appropriate, they can typically be incorporated into data sharing agreements under contract law as of now.

With respect to combining different safeguards, attention should be drawn to possible conflicts between laws, frameworks, agreements, or other rules when it comes to data access and the question how such conflicts can be addressed.

If any, additional public sector transparency provisions should be coherent to existing transparency obligations under the GDPR.

d. Which of the following types of non-monetary compensation would incentivise you to engage in a B2G data-sharing collaboration for the public interest?

Building upon our general preference for fair market price compensation, other types of compensation that we selected in the questionnaire could provide additional benefits and thus complement a fair market price regime.

Tax incentives should not be used as compensation for the following reasons:

- Tax incentives would unnecessarily link the envisioned Data Act under EU competency with tax regimes under member states' competency.
- Implementing and managing tax incentives could cause considerable administrative efforts for member state governments, national tax authorities, and businesses with cross-border activities altogether, which could be disproportionate. If tax incentives are meant to complement a fair market price regime, this applies even more.
- If tax incentives and a fair market price regime both intend to compensate a data-sharing business with the same amount, the former seems indefinitely more complex than a bank transfer, and little aligned with usual procurement practise.

II. Business-to-Business data sharing

The scope of the term **data sharing** should be wide enough to mirror (i) current and future market reality and (ii) be inclusive of the diverse and growing European data economy. Hence, the term data sharing should not be synonymous with making data available for free to market participants. Similarly, the scope of data sharing should not be limited to obligatory data sharing. Instead, data sharing should also refer to data access and use between different entities via contractual means that may include compensation mechanisms and prices as this can create powerful incentives for data sharing.

a. Do you agree that the application of a 'fairness test', to prevent unilateral imposition by one party of unfair contractual terms on another, could contribute to increasing data sharing between businesses (including for example co-generated non-personal IoT data in professional use)?

We respectfully submit that the above question could merit further clarification. We are not certain about the suggested relationship between fairness of contractual clauses on

the one hand and data sharing per se on the other, because (un)fairness is inherent to any sort of interaction between entities.

With respect to a fairness test, requirements of such test do not appear sufficiently clear. In any event, such test is probably unnecessary as there exist sufficiently comprehensive B2B contractual clauses that may ensure fairness.

Furthermore, considering a situation where data intermediaries are involved, the mechanism of a fairness test appears rather unclear and complex.

With respect to unfair imposition of contractual terms, such would better be addressed with existing competition tools that allow a case-by-case assessment.

b. What, in your view, could be the benefits or risks of the options mentioned in the three previous questions, for example in relation to incentives for data collection, competitiveness and administrative burden?

We would like to submit our considerations vis-à-vis standard contractual clauses (SCCs) and their risks in terms of administrative burden in the present case.

Applicable law provides rights to protection with respect to data in two domains: the domain of data protection and the domain of confidentiality. In addition, data rights may emerge indirectly from other rights (such as property rights to storage devices and IP rights to devices that collect data). In sum, applicable law protects data from third-party access where such data falls within scope of primarily (i) privacy rights, (ii) neighbouring rights, (iii) copyrights and (iv) rights to the protection of storage devices.

However, all those protections are conditional. Copyright for example only provides legal protection for certain activities, such as personal intellectual creations, certain investments, or inventions. They exist to allow rightsholders to acquire exclusive usage rights of their investments/intellectual creations to be able to amortise their incurred effort for said activities. Vice-versa, if data is generated without any of such activities, it is generally in the public domain, which allows anyone to use it without infringing the IP rights of the data "creator".

The collection and use of data and information are legal activities under applicable law unless there are prevailing rights such as for exclusive allocation, free disposal, or against unauthorized reproduction that limit or prohibit them.

It emerges from these considerations that additional SCCs may equally be constructed in a comprehensive manner using existing legal tools and established contracts. While we see the chance of increasing regulatory coherence between member states, today's administrative burden caused by contract design is already very significant. If additional clauses were to be considered or complied with in today's contracts (even indirectly in case of non-binding clauses), businesses would face even additional hurdles.

III. Tools for data sharing

With respect to blockchain technology, a recent **representative study on companies in Germany** commissioned by Bitkom indicated the following:[1]

- Most consider blockchain an important future technology
- Only 2 percent are using it or have started pilot projects
- The biggest challenges around the use of blockchain applications are seen
  - in a lack of in-house know-how (87 percent)
  - a lack of qualified staff (81 percent)
  - no reliable use cases for blockchain applications (79 percent).

IV. Non-personal IoT data

a. To what extent are the following elements well addressed in contracts relating to the sale or long-term lease of IoT objects for professional use?

All elements suggested in the table may be sufficiently well addressed using existing contract law and do not require further regulation as a framework of existing private law clauses would be duplicated.

Instead, other legal norms can cause contractual issues, for example the GDPR with respect to data processors, joint controllership, or reliably compliant data anonymisation.

[1] Methodology: The data is based on a survey conducted by Bitkom Research on behalf of the digital association Bitkom. In the process, 652 companies with 50 or more employees in Germany were interviewed by telephone. The survey is representative of the German economy as a whole.
Survey results and further information available at: https://www.bitkom.org/Presse/Presseinformation/Deutsche-Wirtschaft-kommt-bei-der-Blockchain-nicht-voran (German).

V. Cloud services portability

a. In your opinion, do the self-regulatory SWIPO codes of conducts on data portability developed by the cloud stakeholders represent a suitable approach to address cloud service portability?

The SWIPO code of conduct (SWIPO) per se is a very useful, versatile, and promising ruleset and is supported by us. Given its recentness, waiting to see the effects of SWIPO instead of already supplementing it would merit consideration. In addition, a potential future discussion about cloud rules would profit from an evaluation of SWIPO in practice, which deserves more time.

More broadly, the SWIPO contains rather fundamental rules and – as it is non-binding per se – efforts to improve its immediate efficacy would merit consideration.

b. What legislative approach would be the most suitable in your opinion, if the data portability right for cloud users would be laid down in an EU legislation?

If the EC introduces the right to portability, it should only be introduced as a high-level principle. We strongly advocate for an approach that puts achieving data portability on a technical level into industry's hands. This is due to the following reasons:

Firstly, effective data portability requires a great effort when it comes to standardisation. Standardisation of the tagging and description of data in order to clearly define them in terms of content and semantics for further automatic processing and linking is the key to data portability. Additionally, standardised interfaces and data formats are of great importance. APIs, open Standards and interoperable data formats are, even today, already developed and implemented by the industry itself. The most recent example for companies coming together to explore new standards and agree on those is GAIA-X. This project should be given a fair amount of time in order to show that it can deliver. In a nutshell, the precise technical specifications of the data portability should be driven by cloud users and cloud providers, as they know best their needs and the technical feasibility.

Secondly, most cloud providers already offer processes for data portability in order to be competitive and to be compatible with relevant ecosystems. For most IT-companies the times where data was seen as an asset to be protected from other companies are over,

since it is business models, not the amount of data, that make companies successful. A right to data portability would thus be in line with recent developments in the market.

VI. Data portability under Article 20 GDPR

a. To what extent do you agree with the following statement: "Individual owners of a smart connected object (e.g. wearable or household appliance) should be able to permit whomever they choose to easily use the data generated by their use of that object."

In line with the European strategy for data, we support the creation of data spaces and the sharing of data to create economic and social benefit and are committed to an innovative and open European digital sector. We gladly support existing personal data protection regimes (e.g. GDPR, e-Privacy Directive) and believe that technology only works with trust.

Be it in the context of Article 20 GDPR or a potential new right to portability, self-regulatory approaches should be the preferred option as they can generate agreements that fit technology, markets, and consumers best. This holds even more for highly technical issues such as formatting, exchange standards, and interoperability, like in the present case.

Against back background, we respectfully submit that the question and its scope could be interpreted in different ways and thus would like to supplement our responses with the following.

i. Type of data

In light of the preamble of chapter VI, we would like to submit the following for completeness. If the scope was any type of data generated by an individual owner's use of smart objects, such provision would have severe implications in terms of e.g. IP protection and trade secrets because critical/technical/non-personal information could have to be disclosed to competitors or virtually anyone. Examples for such information include details on the very design, implementation, and performance of smart objects, such as data from sensors, interconnects, operating systems, backend databases, algorithms. Hence, data portability for non-personal, technical data should be disregarded as a regulatory option in any event.

ii. Type of supplier

If the scope of whomever they choose allows owners to exclude the very supplier of the device (OEM), several issues follow suit. Firstly, smart objects would be treated very differently from other personal devices. Such a distinction would create taxonomy issues, legal uncertainty, as well as confusion for consumers as rules would essentially depend on whether a device is wearable or not. Secondly, this could cause issues for owners in terms of security, maintenance, customer support, and functionality overall, if they try (more on that below) to port their smart object to another service provider. Thirdly, it would endanger the value chain of supplying smart objects and weaken feedback loops between smart objects and OEMs in many ways, such as security, maintenance, and product development. In addition, it would put ecosystems with European customers at a disadvantage vis-à-vis competitors who run ecosystems with customers in other jurisdictions and, finally, increase global regulatory fragmentation for a key technology.

Thus, the hypothetical formulation should be amended to explicitly refer to other actors and in turn exclude the OEM as subject to such principle.

iii. Real-time or continuous portability

It should be refrained from the principle of real-time or continuous portability as it stifles innovation in the field of smart objects, comes too early, and is overly complex.

One could argue that smart objects are inherently linked to an ecosystem to even qualify as smart since they input and output data to generate a benefit. The complex interaction between smart objects and their ecosystem is a key component as to why smart objects are useful and innovative.

Smart objects are designed with rules and procedures that can include different pieces of hardware and software, not necessarily compatible with each other today or over time. Within smart objects, the pieces of data that they collect, process, and store can exist in different levels of e.g. precision, accuracy, time frequency, granularity, format, or actuality. Around smart objects, they generally interact with an ecosystem that may include other devices and network resources with compatible rules and procedures. Such differences are a direct consequence of innovation and competition and need to be balanced carefully with a demand for standardisation by portability.

Real-time or continuous portability would require instantaneous alignment or translation of data and functionality via agreed-upon standards and routines spanning a plethora of versions, products, and ecosystems. Even if data **taxonomy and formatting issues** were solved, **data synchronisation and temporal alignment issues** would remain because data models and functionality would need to be coherent – not only at a snapshot moment but continuously. Such issues could occur within and around smart objects:

- Which data is collected and processed when and in what interval?
- Which protocols are used for an interaction with other devices or ecosystems?

That said, continuous or real-time portability would create significant technical as well as economic hurdles in terms of development, testing, deployment, and maintenance of such interfaces with respect to data synchronisation and temporal alignment. Due to the technical complexity of real-time or continuous portability, we are unsure if this is a feasible option, also considering that such level of portability between devices and ecosystems would be rare and early considering the recent emergence of smart objects. Also, it would be a significant burden to innovation as design changes would have to comply with portability standards.

VII. IP Protection of Databases

Any review of the Database Directive should be done in a cautious manner so as to ensure that trade secrets, confidential business information or IP rights and protections are not undermined. This would run contrary to the objectives envisaged by the Data Act. The EC should also stay connected with international entities, such as the World Intellectual Property Organization (WIPO), who are also reviewing similar data issues.

VIII. Trade secrets protection

From a trade association perspective, we regret to be unable to respond to this chapter‘s questions.

IX. Safeguards for non-personal data in international contexts

a. In your opinion, what would be the best solution at an EU regulatory level to mitigate the risks for European companies stemming from the request for access foreign jurisdiction authorities to their data?

First and foremost, we welcome the EC 's general effort to foster international alignment and compromise on data transfer and lawful access issues. These issues influence and often restrict businesses and users. They deserve rapid resolution in a collective global effort. We encourage the European Commission to purse an intergovernmental solution to these matters as soon as possible, with renewed effort and focus.

Against that background, the issue at hand cannot be isolated from the GDPR, the ePrivacy and e-evidence regulation initiative, and international negotiations or treaties (OECD process, Budapest Convention, post Schrems II EU-US negotiations, CLOUD Act negotiations). We suggest not to create another workstream that applies to data transfers and lawful access or interferes with past efforts or ongoing initiatives, neither via obligations to notify or to put in place safeguards.

With respect to notifications to business users, while the ability to notify business users appears desirable, there can be situations where an obligation for a data processing service provider to notify a business user could cause more harm than do good, such as if an account is hijacked.

Bitkom's suggestion not to act here stems from the above considerations and from our concern that much more than a simple obligation to notify could eventually be created. This would move non-personal closer to the umbrella of the GDPR, a regulation that we welcomed per se but that still causes high administrative effort and causes legal uncertainty in many areas. It also seems likely that the options proposed would generate more conflict of law with foreign jurisdictions rather than increase legal certainty for providers and customers.

telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

bitkom

Annex 1

Cloud Portability within the EU Data Act

What is this about?

The European Union plans to create Union-wide regulations for cloud services within the framework of the EU Data Act. The aim of the project is, among other things, to guarantee a right to cloud portability, comparable to the right to data portability introduced by Article 20 of the GDPR.

Bitkom's view

Bitkom considers the establishment of additional contract law regulations for cloud porting within the B2B area to be unnecessary, on the one hand, because a change of providers and the transfer of data between cloud providers does already work in practice without a set of regulations applicable throughout the Union. On the other hand, the EU lacks the necessary legislative competence to create such regulations.

Core points

The following report shows why the EU legislator lacks the necessary legislative competence for the present regulatory matter by illuminating the prerequisites of EU jurisdiction and applying it to the case of cloud portability.

In doing so, the following aspects will be addressed in detail:

- Explicit competence norms to be found in the TEU and TFEU
- Principles and doctrines from which competence can arise
- The subsidiarity and proportionality principles

I. The EU Data Act at a glance

The EU Commission published its roadmap for the planned Data Act on 03 June 2021 and launched the public consultation to prepare the new regulation. The consultation will run from June 3rd to September 3rd 2021 and is intended to shed light on/ provide input to the COM on the following topics:

- B2G Data Sharing in the Public Interest
- B2B data sharing
- Smart contracts as a means for data sharing
- Clarification of rights to non-personal business IoT data
- Improve portability for business users of cloud services
- Complementing the data portability right under Art. 20 DS GVO
- IP rights / protection of databases
- Safeguards for non-personal data in the international context

Bitkom is contributing to these important issues concerning data economy both in the consultation process and with a position paper. For detailed comments, we therefore refer to the other statements and consultation responses. However, the subject area of data portability for cloud services raises separate questions that will be addressed and examined in this paper, as they primarily concern the upstream question of legislative competence.

II. Proposals for the regulation of a data portability law in the B2B cloud sector

The Commission's proposals in the Data Act aim, among other things, to create a right of portability for business users of cloud services. In the area of data protection law, a right to data portability already exists in Art. 20 of the GDPR; the scope of application there refers to personal data and natural persons as entitled parties. However, the right envisaged in the EU Commission's consultation questionnaire on the Data Act would go beyond this and is apparently intended to establish a contractual right for business customers also for non-personal data. The new right would therefore go significantly beyond the current scope of application, cover more practical cases and, in addition to questions about the necessity of such a regulation, also bring with it renewed questions about interoperability requirements, which have not been sufficiently considered in the questionnaire to date.

From Bitkom's point of view, the European legislator lacks the legislative competence necessary for the introduction of a right to cloud portability. Such a competence does not result explicitly from the treaties of the European Union or from unwritten principles such as the flexibility clause or the implied powers doctrine.

Moreover, the creation of such a set of rules would not comply with the principle of proportionality to which the EU legislator is bound when deciding whether to adopt Union-wide rules.

III. EU competence to adopt cloud portability rules

Article 5 TEU gives rise to two fundamental principles that limit the legislative competence of the EU: On the one hand, the principle of conferral and, on the other, the principle of subsidiarity.

According to the principle of conferral under Article 5(2) TEU, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Through the legal bases contained in the Treaties (norms of competence), the Member States have transferred their own competences to the EU. All competences not transferred to the Union in the Treaties remain with the Member States.

The principle of subsidiarity in Article 5 (3) TEU states that the EU shall act only in areas which do not fall within its exclusive competence, if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central

level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

It follows from the two aforementioned principles that the EU is only competent to legislate if it has been expressly empowered to do so by the EU Treaties or if the subject matter of the regulation could not be regulated equally well at national level.

IV. Legislative competence by virtue of explicit authorisation

From Bitkom's point of view, the EU legislator is not likely to be explicitly authorised by the treaties to enact contract law requirements for cloud portability.

The areas in which the EU may legislate are derived from Art. 2 ff TFEU. According to Art. 2 (6) TFEU, the norm of competence results from the relevant provisions of the TFEU on the individual policy areas. Which competence standard is relevant is in turn determined by the objective focus of the measure. This depends in particular on the objective and content of the planned legal act. If several areas come into consideration, the legal act is to be based on the legal basis in whose area the substantive focus is to lie.

The decisive factor is therefore which objective the planned regulations on cloud portability as part of the EU Data Act are intended to focus on.

One area in which the EU has been assigned legislative competence by the Member States is **the establishment and functioning of the internal market within the Union.** This follows from Article 3 (1) TFEU. Article 114 (1) in conjunction with Article 26 TFEU could then be considered as the relevant norm of competence.

According to Art. 26 (2) TFEU, the internal market comprises an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties. This results, among other things, in the freedom of movement of goods and the freedom to provide services. These guarantee that goods can be traded without hindrance and services can be provided without restriction within the EU.

Goods in the sense of the free movement of goods are all tangible objects that can be the subject of cross-border trade and have a commercial value. Whether incorporeal objects, such as data, are covered by the free movement of goods at all is already questionable regarding the definition. Although gas and electricity are recognised as goods by the ECJ, this has not yet been decided for data.

Cloud services, however, could be subsumed under the (subsidiary) catch-all provision of the freedom to provide services. According to this, services are activities performed for remuneration, free of instructions and under one's own responsibility.

Since cloud portability offers the possibility to migrate cloud services or cloud products from one cloud provider to another without port or integration problems, one could argue that the right to cloud portability would ensure or promote the free movement of services.

However, the migration of data from one cloud provider to another cloud provider does not necessarily have to be against payment and free of instructions. Rather, it is conceivable that the right to cloud portability provides that a cloud provider may require another cloud provider to port its data at any time upon instruction, without owing a fee for doing so (comparable to the right to data portability). The concept of service would thus not be applicable to the porting of data as such.

Although the process of cloud portability as such - namely the mere migration of data from one cloud provider to another - is not to be subsumed under the concept of service, one could argue that it can nevertheless be part of a service contract between cloud provider and cloud user and thus serves the functioning of the internal market by avoiding lock-ins in the context of cloud service contracts. However, such a broad understanding of the concept of services would run counter to the regulatory objective of the principles of conferral, subsidiarity and proportionality of European legislation laid down in Article 5 TFEU. An unrestrained interpretation of the term "service" to include transactions that do not constitute a service per se, but can only be related to one, contradicts the principle underlying the EU that the sovereignty of the Member States is to be preserved as far as possible without this running counter to the objectives of the Community.

Since the planned regulations on cloud portability are part of the planned EU Data Act, the guarantee of effective data protection also comes into consideration as a regulatory object. If this were to be affirmed, the relevant competence standard would be Article 16 (2) TFEU.

In data protection law, there is already an obligation for data portability, namely in Art. 20 GDPR. According to this, the data subject has the right to receive the personal data concerning him or her that he or she has provided to a controller in a structured, commonly used and machine-readable format, and has the right to transmit this data to another controller without hindrance by the controller to whom the personal data were provided.

However, Art. 20 GDPR itself is not likely to be a suitable legal basis for the right to cloud portability, as the right to cloud portability is not intended to be limited to personal data and the subject matter would thus not be fully covered by the scope of the GDPR.

Moreover, the focus of the subject matter of the regulation is also unlikely to be on ensuring effective data protection. It is true that the right to cloud portability and the associated obligation of cloud providers to ensure the migration of cloud services as unproblematic as possible can also contribute to data protection by enabling data portability in practice. However, the core of the right to cloud portability is likely to lie more in ensuring a smooth flow of data than in protecting data.

Article 16 (2) TFEU is therefore unlikely to be a competence standard.

Furthermore, **consumer protection** could be considered as the main objective of the regulation. The relevant competence standards would then be Art. 114 (3), 169 in conjunction with Art. 12 TFEU.

However, the right to cloud portability is primarily directed at business users of cloud services, so that the guarantee of effective consumer protection cannot be the main objective of the planned regulation. Art. 114 (3), 169 in conjunction with Art. 12 TFEU can therefore also be ruled out as a rule of jurisdiction.

V. Flexibility clause and implied powers doctrine

If none of the above-mentioned rules of competence is considered relevant and the EU is therefore not explicitly authorised to legislate, there are two further institutions from which legislative competence could nevertheless be derived.

In addition to the explicit competence norms, the so-called flexibility clause applies according to Art. 352 TFEU. According to this, the Council, acting unanimously on a proposal from the Commission and after obtaining the consent of the European Parliament, shall adopt the appropriate provisions if action by the Union is required within the framework of the policy areas laid down in the Treaties and the necessary power to do so is not provided for in the Treaties.

Art. 352 TFEU is an exceptional provision which must in principle be interpreted narrowly. The Union's action must be necessary to achieve the objectives of the Treaties. This does not seem to the case with regard to the present draft regulation. There is nothing to suggest that the right to cloud portability is absolutely necessary for the achievement of the objectives of the Treaties.

In addition, there is the implied powers doctrine, which originates from international law and has been adopted by the ECJ. This comprises the annex competence known from German law, competence by virtue of a factual connection and competence by virtue of the nature of the matter. According to the implied powers doctrine, an international organisation must also have the competences that are absolutely necessary for the fulfilment of its tasks. These unwritten competences must be derivable from other (written) competences.

With regard to the implied powers doctrine, no competence of the EU can be derived either. Here, too, there is no compelling necessity for the regulation so that the EU can fulfil its tasks.

VI. Subsidiarity and proportionality principles

Should one, in deviation from the view held by Bitkom, consider one of the competence norms explained above to be relevant or derive the competence from the aforementioned principles, the competence of the EU to enact the regulations could still fail due to the subsidiarity principle from Article 5 (3) TEU. However, this would only apply if the matter could be regulated effectively at national level. Since the right to cloud portability is essentially about being able to switch a cloud solution between different providers who are not necessarily active in the same Member State, regulations at national level appear to be considerably less effective, which is why the subsidiarity principle would not apply in Bitkom's opinion.

Finally, the proposed regulation would have to be measured against the principle of proportionality enshrined in Article 5 (4) TEU. According to Article 5 (4) (1) TEU, the content and form of EU measures must not go beyond what is necessary to achieve the objectives of the Treaties. Consequently, the suitability, necessity and appropriateness of the regulation are examined.
With regard to the necessity of the regulation, it would then have to be examined whether there is a need for regulation at all, since in practice it does not usually happen that the porting of data is blocked by cloud providers.

The necessity would also be opposed by the fact that less intensive interventions, such as the introduction of generally applicable standards - such as standardised interfaces - and the self-commitment of cloud providers through codes of conduct - such as the obligation to conclude exit agreements - would represent an equally effective alternative to a right to cloud portability in the form of a binding legal act.

Finally, it is questionable whether the matter does not fall within the exclusive legislative competence of the member states anyway, since the right to cloud portability is thematically assigned to the area of **contract law**.

In the absence of an allocation to the EU, the enactment of regulations on contract law falls within the responsibility of the member states. The establishment of a right to cloud portability would interfere with the drafting of contracts between private cloud providers and with their freedom to decide whether and with whom to contract. Since such interference with private autonomy may in principle only be carried out at national level by the member states themselves, action at European level is likely to violate the member state sovereignty.