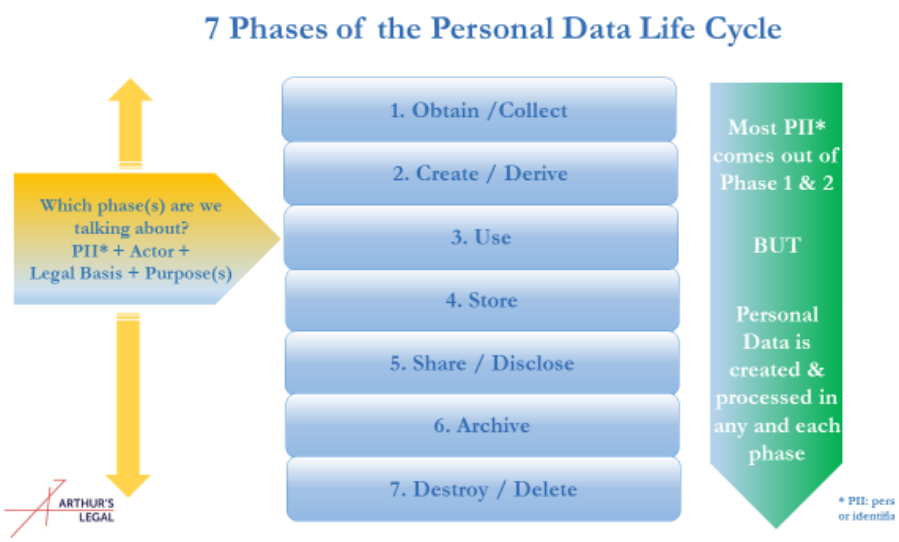
POSITION PAPER CONCERNING THE PUBLIC CONSULTATION ON BUILDING THE EUROPEAN DATA ECONOMY

1.	**INTRODUCTION**	The present position paper accompanies the input to the consultation provided through the online questionnaire by Arthur's Legal. In its multiple capacity as an organization providing Strategic and Legal Services & Systems, Arthur's Legal is well equipped to provide concrete views regarding the impact of the existing data localization restrictions within the European Union. More specifically, Arthur's Legal is highly interested in the matter of free flow of data for several reasons, including, for instance, access to data held by organizations with significant business in internet-based platforms. Moreover, Arthur's Legal in its capacity as a tech law firm has extensive experience through its daily practice on the impact of the data localization restrictions on the market both locally (Netherlands) and beyond within the broader market of the European Union. Note, in this respect, that should the data localization restrictions be lifted, the legal sector -mainly, the legal practitioners and courts- will be among those sectors to be subject to the impact of such removal. The present position paper argues that restrictions on the free movement of data across the EU Member States and on the location of data for storage or processing purposes are largely unjustified. Interestingly, those restrictions are not addressed in generic Internet of Things products and services. The latter, though, is quite easily understood as most restrictions are only applicable to certain industries, markets, or use. In any event, those restrictions remain a key challenge, especially, for hyper-connected ecosystems that are borderless and the data therein should be able to flow freely and unrestricted, at least within the European Union. Furthermore, the present position paper is fully aligned with the European Commission's objective to collect information in specific areas identified in the publication of the consultation[1]. The paper, thus, provides the concrete input requested, additional information raising from Arthur's Legal experience with interacting with customers of different sizes processing data of all types (SMEs, large corporations) and with the public sector. Taking into account the freedom of capital, goods, labor, movement, the overarching aim of this paper is to contribute in making EU Single Market present and future proof. To this end and on the basis of its active presence within the Internet of Things Community (eg. AIOTI, EU research projects on Internet of Things) Arthur's Legal participated in the parallel consultation concerning product liability and provided additional input via a separate position paper accompanying the input to the respective online questionnaire.

[1] https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy

2.	**SETTING THE SCENE**	It is rather common ground that markets are currently going through a stage of convergence largely resulting from the technical developments allowing large scale data flows. In particular, technologies that enable the expansion of the Internet of Things steer existing markets towards convergence, while creating new markets, both physical and virtual markets within the public and private sphere, at vertical and horizontal segments. From the point of view of convergence of the technical markets, certain elements and developments, including, the integration of smart systems, cyber-physical systems, smart networks, data analytics, cloud computing, robotics and robotics bring together different generic technologies with nano-electronics, wireless networks, low-power computing, adaptive and cognitive systems. Basically, the entire set of these developments can be grouped into five (5) main categories: 1. Things, 2. Infrastructure, 3. Data, 4. Services,5. Connectivity and Interoperability[2]. In this context, especially, with paradigm of the Internet of Things, free flow of data is highly relevant, as data is what actually keeps the Internet of Things moving and alive. In this respect, free flow of data concerns data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or within the Internet of Things, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as all other human readable or machine readable data. The life cycle of processing data commonly includes seven (7) phases, as captured in the figure below, which is applicable both for personal and non-personal data:

[2] Arthur van derWees, Janneke Breeuwsma and Andrea van Sleen: *"IoT Societal Impact – Legal Considerations and Perspectives"*, Book Chapter in "Digitazing the industry: Internet of Things, Connecting the Physical, Digital and Virtual Words", River Publishers Series in Communications, http://www.internet-of-things-research.eu/pdf/Digitising_the_Industry_IoT_IERC_2016_Cluster_eBook_978-87-93379-82-4_P_Web.pdf



In relation to the figure above, it should be stressed that data are not generated only through the first two phases, but also data created and processed in each and any phase. For example, when deleting data, other data describing the act of deletion may arise.

Despite the de facto need to liberalize flows of data, the legal regime governing data flows is highly rigid and fragmented. More specifically, quite a few Member States have implemented sector-specific rules and regulations that differ per Member State, thus, preventing the Digital Single Market as a whole, as well as, separate manufacturers, service providers and other vendors within European Union from benefiting from being able to promote their respective products, services and data to other Member States.

Taking into account the reality of data processing and the legal barriers to be further elaborated below, there is already wide consensus within European Institutions and Member States with respect to the removal of the data localization restrictions. For instance, the European Parliament is openly in favor of lifting barriers to the free flow of data recommending *"to recognize that digital innovation is a driver of economic growth and productivity in the entire economy; to recognize that data flows are a crucial driver of the services economy, an essential element of the global value chain of traditional manufacturing companies and critical for the development of the Digital Single Market; to seek, therefore, a comprehensive prohibition of forced data localization requirements and to ensure that [the Trade in Services Agreement] TiSA contains future-proof rules and prevents fragmentation of the digital world; to consider that forced localization requirements, i.e. forcing service suppliers to use local infrastructure or establish a local presence as a condition of supplying services, deter foreign direct investment from and to a party; to strive, therefore, to curb such practices to the extent possible within and outside European Union, while accommodating necessary exemptions*

		based on legitimate public purposes such as consumer protection and the protection of fundamental rights." [3] In the same spirit, fourteen (14) Member States are openly recommending liberalizing, in principle, data flows, as a means to boost economy, while introducing specific exceptions, where necessary: *"Proposed legislation should expand this principle to the entire Single Market and incorporate the following elements: Member States should as a general rule not impose direct or indirect data localization requirements on their territories. The scope of this rule should be broad, and should, where appropriate, also include public procurement; Exceptions should be applied when absolutely necessary and justified by a narrow range of public interests (e.g. public safety), and with a transparent procedure for enabling them; These rules should be defined and interpreted in a harmonized way across the EU; At the same time, Member States should at all times be able to restrict the flow of data due to national security. Addressing data localization is a first step toward further discussions on emerging issues for the data economy, such as ownership, portability, liability, My Data, and the open data principle."* [4] In this context, the Council of the European Union, agreed naturally on a draft regulation to ban unjustified geo-blocking between Member States aiming at removing barriers to ecommerce[5].
3.	**OBJECTIVES OF THE CONSULTATION**	The publication of the consultation on the free flow of data does build on the assumption that European Data Economy is affected by the existing restrictions mandating -to a large extent- data to be kept local. It is of high relevance to add to this that, as far as the key pillars of the Digital Single Market are concerned, one of its key pillars is to ensure that *"Europe's economy, industry and employment take full advantage of what digitalization offers."*[6] This pillar, though, currently appears to be a quite far-reached ideal, rather than a well-grounded reality. The technological means having emerged over the last twenty (20) years have not led to a substantial increase of productivity, while Europe is confronted with the challenge of the ageing population. Faced with rapidly ageing populations and slowing employment growth, mature economies need to boost productivity sharply if they are to escape stagnating living standards. In this context, the massive growth of productivity has become a pressing necessity and

[3] REPORT containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA), (2015/2233(INI) by Committee on International Trade http://www.European Unionroparl.European Unionropa.European Union/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0009+0+DOC+XML+V0//EN#top

[4] "Non-paper on the Free Flow of Data initiative" , Joint support from: Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Slovenia, Sweden, United Kingdom , adopted in Brussels on December 2nd, 2016, available at: https://mc.gov.pl/files/free_flow_of_data_-_non-paper_od_lm_eu_member_states_dec._2.pdf

[5] http://www.consilium.europa.eu/en/press/press-releases/2016/11/28-geo-blocking/

[6] https://ec.europa.eu/commission/priorities/digital-single-market_en

		the "digital potential", also, increased through freeing up data flows appears to be a promising panacea to address it. Taking into account the points raised above, the discussion below has a double objective. First, it provides information in relation to the concrete areas identified by the announcement of the consultation (impact of localization restriction on free data flows, nature and scale of the barriers, proposed measures to tackle them, liability challenges, issues relating to data portability and standards). Second, it draws links with the bigger picture of growth within the European Union, as envisioned by the Digital Single Market.
3(i).	**WHETHER & HOW LOCAL OR NATIONAL DATA LOCALISATION RESTRICTIONS INHIBIT THE FREE FLOW OF DATA IN EUROPEAN UNION**	Based on Arthur's Legal experience, data localization restrictions at local and national level, do significantly inhibit the free flow of data in European Union for several reasons. First, there is a plethora of data location restrictions within the individual Member States, as well as an amplified set of diversified approaches at national level, which are often largely unreasonable or highly disproportionate. This plethora of restrictions results from the absence of well-defined standards and practices at the level of the European Union, while the absence of well formulated standards fosters further the implementation of data localization restrictions, thus, catching market players in a vicious circle. In particular, there are numerous regulatory instruments at EU level relating to the scope of the aforementioned consultation, including the Software Directive (91/250/EEC), the Database Directive (96/9/EC), the Trade Secret Directive (COM/2013/0813), the EU Antitrust legislation, the E-Commerce Directive (2000/31/EC) and the Unfair Terms in Consumer Contracts (93/13/EC) Directive. All these instruments of European law due to their nature as Directives are transposed in the national orders by virtue of legislative instruments of all kind, therefore, adding complexity and discouraging companies expanding their business in other Member States. Moreover, there are data localization restrictions hampering free flow of data emerging from national laws. In sum, those restrictions mostly relate to the handling of financial data, tax data, health data, book keeping data, gambling data, banking, as well as public procurement at national & local level. For instance, in the Netherlands public records -both paper and electronic- have to be stored in archives in specific locations in the country. Second, legal uncertainty steers business users of small size towards over-limiting and bounding themselves due to their fear of data location restrictions and due to the absence of sufficient transparency by key

		market players (eg. large cloud service providers) that would allow them to do otherwise. Finally, there is often a lack of common understanding and culture in key matters across sectors and Member States. Data localization restrictions bring about the absence of a harmonized understanding, as companies processing data across different Member States face increased administrative burdens and need to comply to different legal systems. Note that additional input as to how data localization restrictions create an impact on free flow of data will be provided in the sections below.
3(ii).	**THE NATURE & MAGNITUDE OF ANY BARRIERS TO ACCESSING SUCH DATA**	The nature of barriers blocking or constraining the free flow of data and, thus access to data, result primarily from laws and regulation, leading further the industry to legal uncertainty and lack of trust[7]. Conversely, often Member States –due to their trust in the industry – make use of their legislative powers to draft and enforce laws and policies that restrict the free flow of data. In addition, other commonly known barriers can be found in contractual agreements. For example, in case a certain party is entitled to a specific type of data (eg. on the basis of protection of its intellectual property), it can prohibit other parties from accessing it, using it or sharing it with other third parties through contractual clauses. Moreover, cybersecurity is often mentioned as the (legal) incentive for imposing the aforementioned restrictions. This goal, though, could be achieved otherwise as well, though, for instance, the adoption of safety standards at EU level, best practices and a solid liability framework Note that, from a cybersecurity point of view, a known physical location of data could even have an opposite effect, as it makes data easier to locate and target (by hackers). The data localization restrictions entail an extensive negative impact. They hinder large scale adoption of the Internet of Things as they highly vary per Member State and lead to a fragmentation of the market for Internet of Things infrastructures, platforms, devices as well as applications and related services. Furthermore, taking into account the typical characteristics of the Internet of Things devices and their dependency on the internet and other digital networks, barring Internet of Things devices not to transfer data across borders is, basically, against their very purpose and benefits.

[7] Judging from the experience of Arthur's Legal, the earlier discussed barriers linking to access to data are manifested, primarily, in practice by: a) denial of data access, b) by prohibitive prices and c) by terms and conditions considered unfair by our organizations (Please, see relevant answers to the online questionnaire of the consultation).

		The aforementioned barriers have a very detrimental effect on the security, resilience and business continuity of companies - and governmental organizations even - using, offering or operating on Internet of Things solutions to conduct business, while further impeding competition within and outside the Common Market. It is, for example, rather common for a Member State to oblige an Internet of Things or software vendor to have and maintain data center within its territory. Quite unsurprisingly though, not every Internet of Things or software vendor has the ability to establish a data center within each Member State. Consequently, those requirements may restrict the possibility of the provision of Internet of Things and software products and services, limiting the vendor in its business, and the consumers of that Member State in the choice regarding Internet of Things and software vendors, products and services.[8] Overall, it is of significant importance to stress that the barriers set above, are, in essence, the symptoms and that the deeper causes relate to the inadequacy of the legal framework governing Business to Business relationships, especially, in relation to the unfair contract terms and commercial practices. In this respect, experience with daily practice shows that there is a great degree of difficulty regarding the actual enforcement of rules relevant for the aforementioned relationships.
3(iii).	**WAYS OF TACKLING THOSE BARRIERS**	This section merely touches upon the ways that the aforementioned barriers could be tackled. Further input will be provided later in the discussions under sections 3(iv) and 4 elaborating on data portability and producing recommendations respectively. From a contractual point of view, parties should insist on ensuring through the contracts in place options that would allow them to have access to their data. This is clearly illustrated in case of a cloud customer wishing to change cloud service provider and, thus, port its data. To this end, cloud customers should consider the existence of an Exit Plan in place by the cloud service not only in case of an advert event, of "something going wrong", but in a standardized manner, well in advance, namely, when assessing a cloud offering, preparing, negotiating and entering into an agreement with a cloud service provider. From a regulatory point of view, the aforementioned Exit Plan could be rendered mandatory by law, as means to put pressure on large cloud providers to provide for it. The requirements of an Exit Plan for non-personal data could be set out along the lines of Article 20 of the General Data Protection Regulation (GDPR)[9] , which provides for the possibility

[8] AIOTI Digitisation of Industry Policy Document, October 2016, p. 24 - 25.
[9] Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

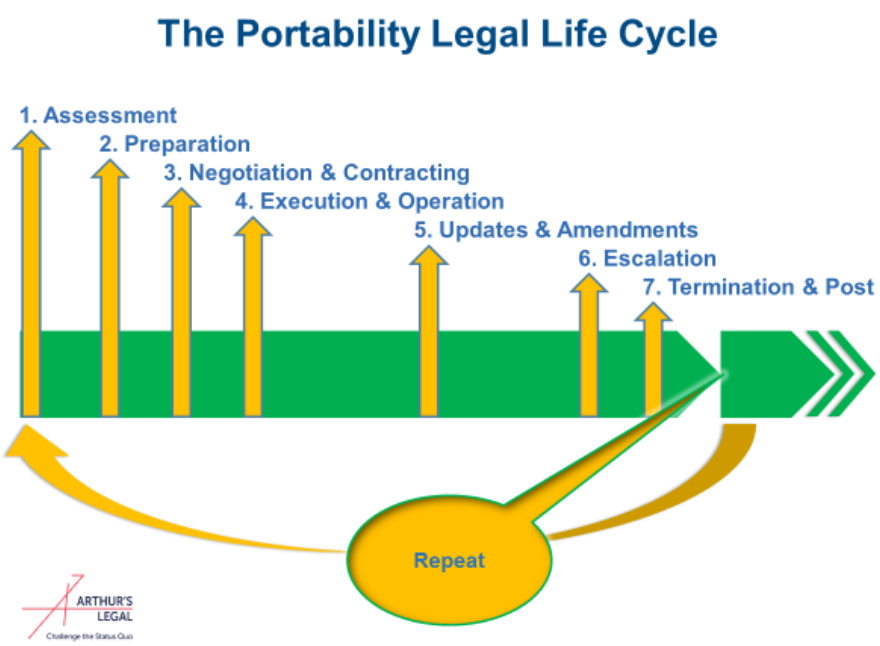
		of data to be provided to individuals *"in a structured, commonly used and machine-readable format"*. Moreover, it stays with the regulator and the principal market players how precisely to steer market engagement towards commitment to the same standards. Finally, from a broader perspective, public and private organizations need to better educate employees in charge of data handling. Experience shows, that for convenience purposes, employees may deny or accept requests to access to data depending on the particularities of the request and of the specific context. This "human factor'', of course, may be of critical importance, in case of key societal interests at stake (eg. national security, public safety).
3(iv)	**EMERGING INTERNET OF THINGS & ROBOTICS LIABILITY CHALLENGES**	As previously mentioned, freeing up flows of data is highly relevant for the Internet of Things and robotics, inevitably, giving rise to the associated liability concerns. As known, these issues are, also, the main topic of a separate consultation on the rules on liability of the producer for damage caused by a defective product. In relation to that consultation, Arthur's Legal has submitted separate position paper assessing in detail the emerging challenges within the Internet of Things concerning product liability and, more specifically, Directive 85/374 relating to the liability for defective products ('Directive 85/374').The most important conclusions of that paper are outlined below. One of the most important issues regarding (product) liability in relation to Internet of Things is the lack of a legal framework. As Internet of Things devices mainly consist of software, the fearful prognoses is, they will often fall outside the scope of , Directive 85/374, as it is clearly written for stand alone, tangible products and not for software or Internet of Things devices which are intangible and/or connected to the multi-dimensional Internet of Things network. As a result, the definitions and principles which are the very backbone of Directive 85/374 miss their intended effect or are not even applicable: • The definition of "product" requires unjustly a product to be tangible in order to fall within the scope of the directive; providing the developers and vendors an easy way to exempt themselves from product liability by calling their (software) products and the provision thereof 'services'. • The fact that the definition of "defective" in article 6 focusses on a safety level users are entitled to expect, is problematic as consumers, in principle, have relatively low expectations when it comes to the quality and safety of software and Internet of Things

		devices, since defective software with safety risks is and has always been the standard. Moreover, the capability of Internet of Things devices to act autonomously makes it very hard to describe or foresee what kind of safety level they have, let alone what kind of safety level people are entitled to expect. This is particularly relevant, in cases that these devices have a self-learning or adaptive ability. • The principle of strict liability misses effect. First and foremost, this results from the fact that the burden of proof in article 4 of Directive 85/374 is too high; taking into account that the Internet of things characterizes itself as a multi-dimensional network of different developers, vendors, network providers and other stakeholders, it is nearly impossible for the average consumer to trace back a defect, let alone the causal relationship between the damage and the defect, as required by article 4. Another important factor, causing the principle of strict liability to miss its intended effect, is the fact that the responsibility – and therefore liability - for the quality of the software often is gradually shifted to the consumer to a certain extent, by obliging the consumer to timely downloaded/deploy updates and patches. • The definition of damage is not fit for purpose anymore, as it focusses on damage caused by death, injury or damage to any other item of property other than the product itself. This is in contrast to the damages in relation to defective software and Internet of Things devices which characterize themselves mostly as financial damages and damages to the defective device or software program itself. Normally, the abovementioned negative effects and voids would be countered by other laws and rules, applicable through article 13 of the Directive, such as contractual law. However, because of the characteristics of the industry itself and the strong market position of software developers and vendors, the complementary effect of contract law is largely limited. Software and Internet of Things device developers and vendors generally use (standard) contracts which contain very poor user conditions and only a bare minimum of warranties and liabilities.
3(iv)	**PRACTICES AND ISSUES RELATING TO DATA PORTABILITY, INTEROPERABILITY AND STANDARDS**	Portability of data is closely linked to freeing up data flows. Should data portability become a widely-endorsed practice, it will naturally facilitate data flows. Note that Arthur's Legal is currently carrying out the EU funded study on "Switching Between Cloud Services Providers", SMART

2016/0032, addressing the specific matter of data portability in the cloud setting[10].

So far, there have been successful cases of services offering portability of data, including, doctors, Dentists, and other "traditional" service providers. The digital era, though, is now beyond being young and innocent, digital data and technology are need to have, one cannot do without, and it is time that non-traditional providers of services become aware of how important their services are, and that customers need to have a say about their own data.

Nevertheless, EU market is still largely immature with respect to data portability, as it is, basically, either impossible for cloud customers to export their data or the features to export data are undeveloped or even not working properly. The difficulty to port data is so extensive, that cloud customers often do not even consider portability as a critical feature of a cloud offered service before selecting it in the first place. In relation to this, the figure below depicts the different stages of the portability life cycle, before a cloud computing agreement is concluded, while it is if force and after it is terminated.



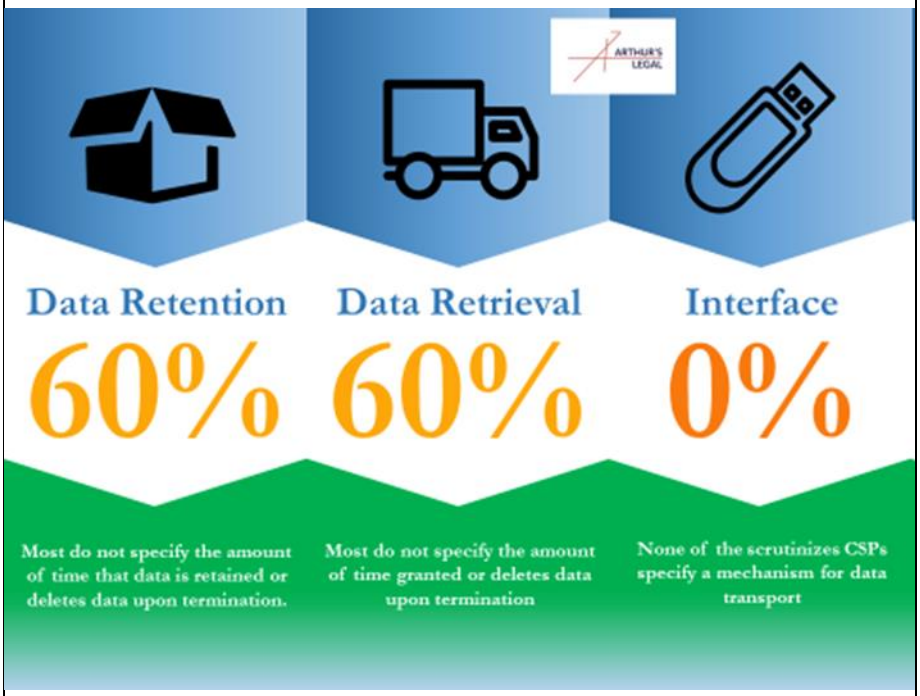
From a legal point of view, portability is hampered due to a series of reasons relating to the existing contractual agreements, the behavior of important market players and the inadequate adoption of standards.

In particular, contracts often do not provide at all for an Exit Plan which would provide for the import and export of data and which would detail

[10] The discussion under section 3(iv) is largely based on the Switching Between Cloud Services Providers SMART 2016/0032 D2 Interim Report drafted by IDC and Arthur's Legal. The report was delivered to the European Commission on the 28th of March 2017. Note that the final report will be made publicly available after the end of the study.

		the necessary technical specificities. An appropriate Exit Plan in place appears to be absent not only from the master agreement, but, also, from the accompanying Service Level Agreement (SLA).The Exit Plan relevant would specify the set of Service Level Objectives (SLOs) that are requested for the import and export of data and applications. Note that the SLOs, especially, relevant for data portability are identified as follows under the Cloud Service Level Agreement Standardization Guidelines endorsed by the European Commission: a) the data portability format, b) the data portability interface and c) the data transfer rate. In particular, the inclusion of the SLO on the data portability format would specify the electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service. As a consequence, in the absence of an SLO on the data portability interface, there are no mechanisms which can be used to transfer data for one cloud service to another or any specification of transport protocols and the specification of APIs or of any other mechanism that is supported. Finally, due to the absence of an Exit Plan, there is no minimum rate set at which cloud customer's data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface.

From a contractual perspective, including cloud service level agreement, master services agreement and other related legal documentation, based on Arthur's Legal own sources and ongoing independent research, specifically, on cloud computing, service level objectives, pre-procurement and compliance, these and similar – as well as additional – issues and other challenges arise. For instance, based on extensive and independent research on the services level agreements and related legal documentation publicly available about ten (10) international and national cloud service providers in the IaaS domain made available in the Netherlands, the following summary has been identified regarding certain essential topics regarding data portability:



Aside for the earlier described situation in the contractual landscape, the existing standards governing data portability are effectively used. Standardization efforts, however, do not necessarily ensure the adoption of interoperable data formats, interfaces or data transfer rates as market players tend to stick to the use of their own standards, thus, leading to the fragmentation of the market. Also, even though certain standards may facilitate technical and customer-centric arrangements, the penetration rate in the relevant market (so, the use of such standards and arrangements therein) is very low.

Note that security standards (ISO 27k series, SSAE 16 SOC series) are the most relevant standards for portability. Currently, there are no other relevant or otherwise useful standards on the market or used by providers that facilitate data portability, interoperability, privacy, data protection, cloud or data management or Service Level Agreements. However, even the security standards mentioned will become out of date and not

		compliant to the set of regulations and directives, including PSD2, GDPR and NIS Directive. Those regulations, though, have caught up and overtaken these (and other) standards. Moreover, with respect to cloud computing in the context of which data portability is highly relevant for further enabling data flows, large cloud service providers seem unwilling to cooperate. Large cloud service providers often abuse their dominant position in the market and show a certain degree of indifference towards the specific issue of portability. Although the adoption per se of such a behavior does not constitute an issue of strict "legal interest'' rather surfacing broader governance considerations, this behavior does have a substantial impact on the conclusion of cloud contract, that -same as regulation- aim at governing, in essence, the behavior of contracting parties. The current situation regarding data portability and, thus, the free flowing of data could be improved by introducing a portability right that would cover all types of data including non-personal data submitted to online platforms and cloud service providers, but also data generated by algorithms and sensors. The focus of such a right would be to facilitate the portability of data, leading potentially to less termination of services and undoubtedly boosting Digital Single Market. Furthermore, the beneficiaries of such a right should be entities of the private and public sector, SMEs, governmental institutions and, of course, consumers. Finally, in view of facilitating access to data and improving technical and semantic discoverability and interoperability the following parameters need to be taken into account, without any exception: common metadata schemes (including differentiated access, data provenance, quality), data catalogues, use of controlled (multilingual) vocabularies, common identifiers, the inclusion of an Exit Plan in contracts, data format and application interoperability, the data interface (mechanism for data transport, and for application portability), the data retention management and the data retrieval management. Most importantly, the increase of transparency by cloud providers on this matter is highly needed, as it is, basically, impossible, to understand their position in relation to legal, operational and financial matters linking to interoperability and data portability.
4.	**CONCLUSIONS & RECOMMENDATIONS**	New technologies lead to change. Change is a catalyst that can be feared, but can also be embraced and used to optimize the current status quo of society and economy, and sometimes even leapfrog technologies that have already been improved. Especially, the hyper-connected aspect of Internet of Things technologies will have quite some impact on the society and economy, and may raise certain ethical or legal discussions on new and existing topics, such as the necessity of lifting barriers to the free flow of data within European Union.

		To this end, there are certain elements that need to be taken into account with respect to the actual processing of data and its further enabling by the technological developments. First, data travels as never before; second, data is contextual and should be seen from different dimensions; third, data ownership is no longer realistic[11] and the emphasis, instead, should be put on control. In this context, the current legal landscape mostly dictating data to be kept local is not fit for purpose, as it does not promote growth and innovation. The legal implications create an impact, especially, on SMEs with limited resources that wish to expand their business in other Member States and are confronted with excessive administrative burdens by national laws. In that sense, the existing data localization restriction and, conversely, the necessity to free up data flows is not merely an issue of legal interest or a legal concern, but it relates more broadly to economy, employment, growth. As an antidote to the current situation and in view of seamlessly encouraging companies of all sizes to expand and economy to flourish, we address the following set of recommendations directed to regulators and companies. In particular –and in addition to the points raised earlier in the analysis-, regulators are invited to: • lift restrictions relating to storage of data (Phase 4 of the Data Lifecycle presented earlier under section 2 of the present document. • maintain data localization restrictions in specific cases and, following sufficient justification. • aim through their interventions on how to increase transparency, foster trust and lead to transformation. • take extensively into account that data should not be treated as a four-letter word. The concept of data encompasses data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine readable data. Note that further recommendations in specific topics (eg. regarding the burden of proof in case of damages caused by smart devices) are provided through the answers to the online questionnaire.

[11] Data Ownership BEREC Workshop (Enabling Internet of Things), 1 February 2017 (Minutes of Meeting):"With regard to the question of data ownership Mr van der Wees of Arthur's Legal and AIOTI held the opinion that data ownership in the digital space was "dead". The relevant publication can be found at: http://berec.europa.eu/files/document_register_store/2017/2/BoR_(17)_16_Arthur'sLegal_Presentation.pdf

		In the same spirit –and in addition to the points raised earlier with respect to specific topics, such as data portability under section 3 (iv) - companies are invited to: • approach compliance with legal rules as an enabler for their business. • engage their personnel in an accountability culture with respect to the handling of information. • invest on security measures. • to commit to soft law instruments in place, such as the SLA Standardization Guidelines endorsed by the European Commission. In any event, what is highly relevant for all sides concerned with freeing up data flows is that the de facto reality of data processing mandates the following: efforts should be steered on ensuring effective control by distributed means.
5.	**FURTHER ELABORATION**	Arthur's Legal is keen on further elaborating on the above items at European Commission's request.

Arthur's Legal, Amsterdam