



Global
Strategy
Group

The European Cloud market: key challenges for Europe and five scenarios with major impacts by 2027-2030

April 2021



Putting the European cloud at the service of the life economy.

Putting data, virtual in essence, into virtual storage, has long been predictable, which technology has come to impose. Unfortunately, as so often, Europe took longer than many to figure this out, leaving Microsoft, Amazon and Google with over 60% of the global public cloud market.

Today, this absence from Europe is very serious and it needs to be remedied as soon as possible.

First, it's an economic issue: By 2027, the cloud market in Europe could reach more than 260 billion euros (against 53 billion euros today), which would put it at the same level than the current telecommunications market (around 250 billion euros in 2020). And if Cloud operators localize their operations and investments in Europe, this could also create around 550,000 jobs between 2021 and 2027 and trigger significant investments (around € 200 billion over the period 2021- 2027). It would also be an opportunity to support the applications industry: the cloud is nothing without all the services that use it; a European cloud could make it possible to develop European software companies more quickly, in all senses of the word. It would also allow the health, education, culture, media, security, insurance and finance industries to be developed in a secure environment; all fundamental sectors in the future economy of life. This should therefore constitute an essential element of European recovery.

It is also a technological issue: Investing in the cloud would allow Europe to position itself as a leader in cutting-edge technologies such as processors, 5G, quantum encryption, edge computing ... And further still, biomimicry. All fundamental technologies in other sectors of the life economy: logistics, water and air management, renewable energies.

This is still a strategic issue: A European cloud would allow Europe to guarantee its digital sovereignty by ensuring its mastery of the management of personal and industrial data, which is absolutely not guaranteed in the current legal and regulatory context. (GDPR regulation, invalidation of the Privacy Shield, Cloud Act).

In this area, as in many others, the problem is global; the solution is European; the problem is political and cultural; the solution is industrial.

Jacques Attali



Disclaimer

This report («Report») has been prepared by KPMG SA («KPMG») for Talan SAS, InfraNum, OVHcloud and Linkt (Affiliate of Altitude group) – «Mandataries» – in accordance with the contract signed with them dated 15th January 2021 («the Contract») and on the basis of the scope and limitations set out below.

The Report has been written for the sole purpose of studying the current situation and challenges of the Cloud market in Europe, as specified in the Contract. It should not be used for any other purpose or in any other context whatsoever. In such a case, KPMG, its subsidiaries and other entities belonging to the KPMG Network declines any liability to any person relying on this Report.

The Report is intended for the exclusive use of the Mandataries under the terms of the Contract. No one, other than the Mandataries, is authorized to use this Report for any purpose whatsoever. KPMG, its subsidiaries and other related entities disclaim any liability or obligations to any person relying on this Report or its content, other than the Mandataries.

In accordance with the terms of the Contract, the scope of this study was limited by the time devoted to it and the information and explanations provided to KPMG. The information presented in this report was obtained by KPMG from the Mandataries and third party sources specifically identified in the appropriate sections of the Report. KPMG did not seek to corroborate such information or validate its plausibility. Furthermore, the results of the analyses presented in the Report were obtained on the basis of the information available at the time the Report was prepared and should not be relied upon in subsequent periods.

All copyright and other proprietary rights in the Report are owned by KPMG and unless otherwise explicitly stated in this communication or in the Contract.

Any decision to invest, engage in business activity, enter or exit the markets considered in the Report should only be made after obtaining independent advice and third parties should not rely in any way on the information contained in the Report. KPMG does not provide any business, financial, investment, or other professional services or advice through the Report. This Report is not a substitute for such professional advice or services, and should not be relied upon as the basis for any decision or action that may affect your business. Before making any decision or taking any action that could affect your business, please consult a qualified professional advisor. In particular, the Report does not constitute a recommendation or approval by KPMG to invest in or otherwise participate in, exit or use in any way the markets or companies referred to in the Report. KPMG and the Mandataries, their subsidiaries and other related entities disclaim all liability arising from the use (or non-use) of the Report, including any actions or decisions resulting from the use (or non-use) of the Report.

This Report was initially written in English and has been translated to French and German. In the event of any discrepancy between the French, German and English versions, the English version shall prevail.

This white paper was completed based on several types of inputs and resources

Interviews with French and German companies' CxOs

50+ in-depth interviews conducted with French and German **CxOs** of large and medium companies (CAC40, DAX, SBF120...), **technology and legal experts**, in order to nurture our analysis of the current market and challenge our recommendations.

Market studies and public documents

Detailed **market studies** of **partner companies** and **organizations** specialized and involved in **Cloud computing challenges and issues** along with **public and legal documents on data sovereignty related issues**.

Exchanges with cloud computing experts

Continuous exchanges with **cloud computing experts**, including internal experts (from KPMG and other contributors teams), economists and public bodies to **challenge and polish our recommendations**, further transformed into **actionable levers**.

A web survey conducted among European CxOs

A web survey of about 40 questions, conducted among **200+ CxOs of French and German companies** (average ~€150m annual revenue), measuring their level of cloudification, **their awareness of sovereignty concerns when choosing a cloud provider and their perception of data sovereignty**.

This study was conducted between January and March 2021, with a **dedicated KPMG team over a 8-week period**, from KPMG GSG (Strategy) and KPMG Legal.

InfraNum, French federation of Digital Infrastructure, has supported and actively contributed to this report regarding the French market analyses along with 3 other market key stakeholders

Key elements on the InfraNum federation



- A federation of **200+** members (companies actively engaging in **digital infrastructure markets** such as FttX, IoT players, telco, equipment suppliers, etc.)
- **Established in 2012** to accompany the very high-speed broadband French national plan.
- **Main objectives:**
 - Support **French digital development**
 - Promote the development **of digital uses in France**, by **supporting companies** in the **implementation of a neutral, open and shared digital infrastructure**
 - Develop partnerships between **public and private players** to enable local authorities to develop citizen uses, enhance the **value of their local economy and highlight the assets specific to each region**

Key elements on the other three contributors

In addition to InfraNum, three other contributors helped construct this study published by KPMG:



- **Talan**, European consulting company specializing in digital transformation



- **OVHcloud**, a European cloud provider



- **Linkt**, French B2B telecommunication company

InfraNum and contributors' active participation has allowed us to build **strong convictions about the future of the European cloud market** including on the main associated risks and challenges.

The European Cloud market: key challenges for Europe and five scenarios with major impacts by 2027-2030 Executive Summary (1/3)

- 1 The European cloud is a sizeable and attractive market offering a strong growth potential: from €53bn in 2020, the European cloud market is expected to reach €560bn by 2030¹ growing at an average rate in excess of 25%**
 - **Cloud services**, encompassing private, public and hybrid clouds for IaaS, PaaS and SaaS services, **meet a wide range of companies' IT needs, providing undeniable benefits:**
 - **Variabilization of cost structure** thanks to public cloud pay-per-use model, with little to no CapEx requirements
 - **Flexibility and scalability**, with the ability to instantly increase or decrease capacity to meet business needs
 - **Ability to focus on core activities**, with deployment and maintenance activities partially or totally outsourced to cloud providers
 - In **Europe, the cloud computing market is booming**, offering a massive value opportunity for the European economy:
 - A market size expected around €260bn by 2027 up from €53bn, comparable to current Telco market (~€250bn in 2020)
 - A competitive landscape dominated by 3 US-based "hyperscalers" (70% combined share of IaaS market), though with limited operations in Europe
 - Stakes for Europe are ~550k jobs creation and ~€200bn investments (over 2021-2027 period) in the event where cloud providers localize their operations & investments in Europe
- 2 From a legal and regulatory point of view, the cloud computing market presents high risks and deep inconsistency between American and European rules, which makes the current legal situation unsustainable**
 - Since 2016, **several data regulations have been implemented** in the US and in the EU (GDPR, US-EU Privacy Shield and the Cloud Act), trying **to establish a strict legal framework with regard to data flows; but the Privacy Shield invalidation** by the Court of Justice of the EU in 2020 **highlighted the deep** incompatibility of US regulations with the GDPR principles, **which appear irreconcilable**
 - As a consequence, **companies transferring Europeans' personal data to non-EU companies' servers (even if located in Europe) no longer have a legal basis** to do so and are subject to **legal risks but also industrial risks** with global cloud providers having access to their confidential data & IP
 - Our interviews² show that **this situation raises concerns and lead to financial and business risks**, such as for example:
 - A dismissal canceled as evidence provided by the company to justify it were hosted on non-compliant cloud providers datacenters
 - A European company not able to use relevant evidences of the theft of customers' data as these data were extracted from an access monitoring system stored and processed in the US without any legal basis for such processing

The European Cloud market: key challenges for Europe and five scenarios with major impacts by 2027-2030 Executive Summary (2/3)

- 3 The move to the cloud is a mandatory but constrained path for CIOs, based on multiple criteria of which data security and sovereignty are among the most important. The lack of knowledge for offers ensuring data sovereignty slows down cloud migration or make CIOs give up on data sovereignty criteria. Yet European actors offer main services to meet business needs and develop active Ecosystems to add SaaS and PaaS services to their catalogue, while ensuring transparent pricing models**
- The choice of cloud providers by decision makers (e.g., CIOs) is based on **multiple criteria ; amongst the most important are data security and data sovereignty ;** however, despite the importance of data sovereignty, **the lack of knowledge regarding offers ensuring data sovereignty slows down cloud migration or make CIOs give up on data sovereignty criteria**
 - Yet **European actors offer most of the services required to meet business needs and propose a growing offering of SaaS and PaaS services with their active ecosystems,** a breadth and depth of services which is progressively becoming comparable to hyperscalers'
 - **Furthermore, European cloud providers' prices appear more transparent** than those of hyperscalers, which yet manage to **dominate the market with aggressive and unconventional client acquisition practices** (e.g., bundling of SaaS and IaaS services), but also **complex exit conditions (lock-in) that make it difficult for cloud users to exit or switch from one provider to another**
- 4 The current European cloud market paradigm does not appear sustainable in the long run and the cloud landscape could therefore evolve into 5 potential scenarios**
- **Four macro-trends and multiple tensions make the current European cloud market unsustainable:**
 - Discrepancy between GDPR compliance and extraterritorial rules is leading to legal / business risks for EU companies using US cloud providers
 - Anticompetitive practices and strong commercial barriers to entry, are currently preventing a fair playing field in Europe
 - Market growing demand for personal and business data protection, are illustrating the raising awareness regarding data privacy and sovereignty
 - Visible and massive economic stakes are due to strong growth in demand for cloud services (especially SaaS) in Europe
 - **5 potential scenarios, each with its own benefits and different timescales, could lead to a new EU cloud market paradigm:**
 - Cloud as a Common Good, mainly driven by voluntary cloud services' interoperability, sector-wide common cloud ecosystems and multi-cloud ramp-up, allowing the growth of a European ecosystem increasing benefits for cloud consumers (end of lock-in) and fueling the growth of European cloud players. This scenario could materialize through the Gaia-X initiative which aims to establish an interoperable cloud ecosystem based on strong principles and values
 - Ramp-up of European providers, mainly driven by emerging market needs still under-addressed (incl. edge computing, AI for industrial data or the development of sovereign offers) and by public spending (B2G projects). This scenario could materialize with the support of the EU authorities that are strongly supporting the creation of a Single Data Market (IPCEI, Data Governance Act, EU cloud rulebook to come...)

The European Cloud market: key challenges for Europe and five scenarios with major impacts by 2027-2030

Executive Summary (3/3)

- Strong regulatory wave (similar to the one witnessed in the Telco market some years ago), with the emergence of a cloud regulator constraining cloud providers, especially hyperscalers, through levers such as greater price transparency, forced interoperability or open access to innovation. This scenario is strongly supported by decision-makers who are expecting healthier competition and take-off of EU cloud providers & ecosystem
- Europeanization of cloud providers, either through the Europeanization of their operations (e.g. local R&D spend, local procurement, local value creation) or through the effective European control of their local subsidiaries (as already in some countries), with EU authorities ensuring effective value creation at local level and strict alignment with European regulation
- Cloud activities separation, either functional (separation between cloud activities and other businesses, with clear split in terms of personnel, offices, IP) or structural (clear separation of cloud business into a separate legal entity, as it is already discussed in the US), leading to a “fairer” competitive playing field between European and US providers
- **Economic impacts** (value captured, jobs created and investments) **could vary significantly in function of the scenario; Europe may lose from 20 to 50% of the estimated economic impact**, if the available levers are not or not sufficiently activated

5 In the short term, to mitigate the risks of such an uncertain cloud landscape, a number of initiatives¹ should be implemented by Public and Private Executives

- There is a strong uncertainty regarding the future European cloud landscape, with deep potential impact for key stakeholders (companies and public services) that need to migrate to the cloud
- This uncertainty can be mitigated through a number of initiatives and decisions:
 - CIOs, CTOs and CISOs should consider a number of best practices for a compliant and secure migration: know your actual IT usage (data and workload), initiate a cultural shift towards a proactive cloud strategy and carefully select and manage their cloud platforms (through cloud providers' assessment)
 - CLOs should be better aligned with the changing and complex data regulation: map data transfers, assess transfer tools, perform risk assessment in case of non-compliance. Beyond regulatory compliance, data encryption can ensure data sovereignty but only under very strict implementation criteria
 - CMOs should develop a responsible and sustainable client promise in terms of data protection, leverage cloud certification as tangible proof point and differentiate from competition by ensuring effective GDPR compliance
 - Public-decision makers should bring a stronger support to the cloud migration, with standardized cloud-related public policies, a dedicated spending policy for cloud computing and the implementation of training program notably for IT-decision makers in local authorities. The relative slow pace of cloud adoption by local authorities points to great potential for local cloud providers that are able to meet their requirements in terms of data sovereignty



Agenda

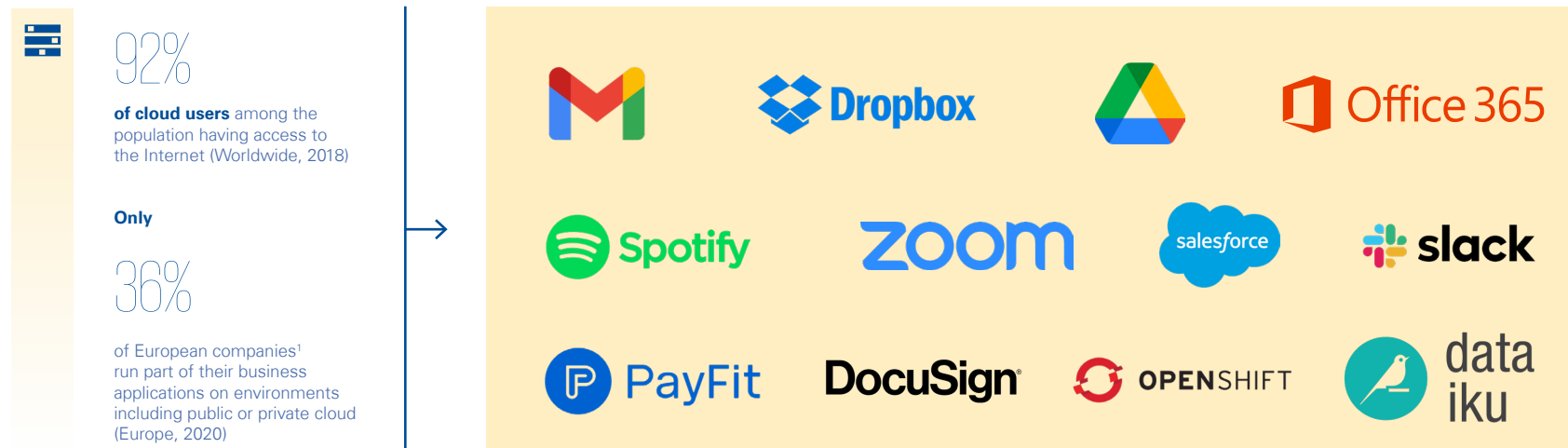
European cloud market: a high-stakes market for Europe, expected to quadruple in size by 2027	10
Migrating to the cloud: a mandatory but constrained path	22
Data-related legal uncertainties: what are the risks for European companies?	39
5 scenarios for the future of the European cloud market.....	55
Moving forward: best practices and initiatives for private and public stakeholders.....	72
Appendix	
Chapter 1	81
Chapter 2	89

1



European cloud market: a high-stakes market for Europe, expected to quadruple in size by 2027

In the last decade, individuals and professionals widely adopted cloud-based applications, with companies however lagging behind with lower adoption rates



- **Cloud-based applications** are defined as **applications accessible through the internet** hosted in physical servers
- Companies can choose to either **own or rent²** one or all of the **necessary cloud components "as a service"**: hardware / infrastructure IaaS, platforms PaaS or software SaaS

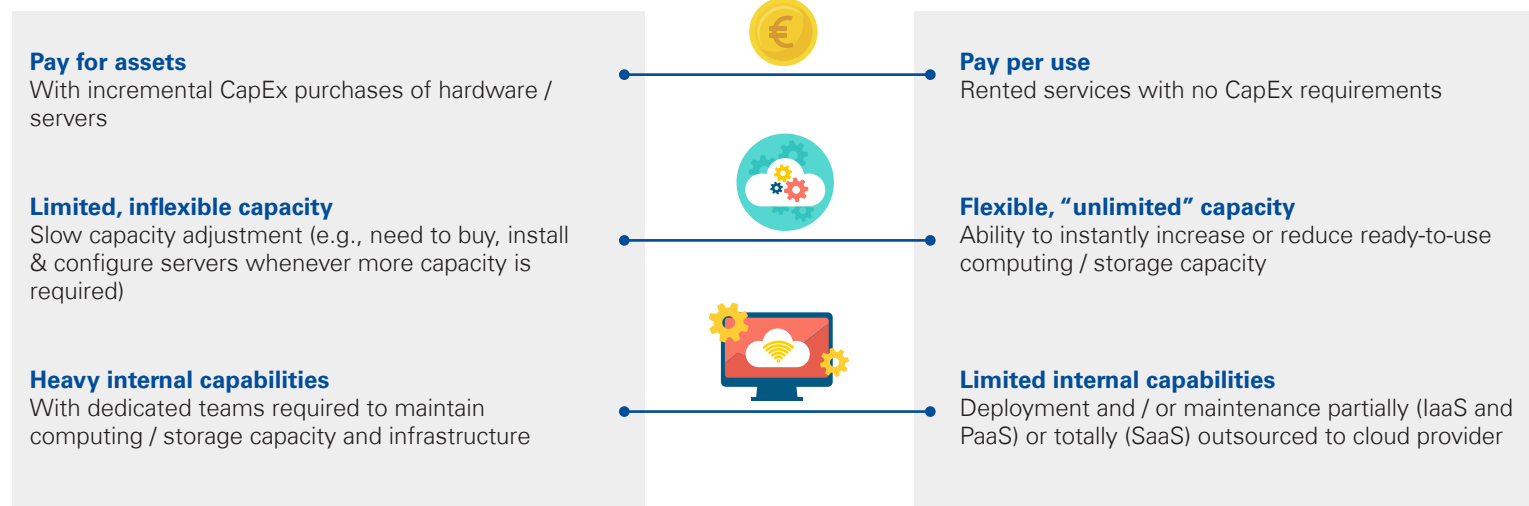
Note: (1). A survey with respondents from ~150k European companies (with approximately 83 % small enterprises, 14 % medium and 3 % large companies) (2) Or own for IaaS
Sources: Eurostat; Flexera; Vision Computer Solutions; GSG research and analysis;

Cloud offers companies with much more flexibility and service coverage, while strongly limiting internal investment compared to traditional model

TRADITIONAL i.e. owned servers in own space or third-party space

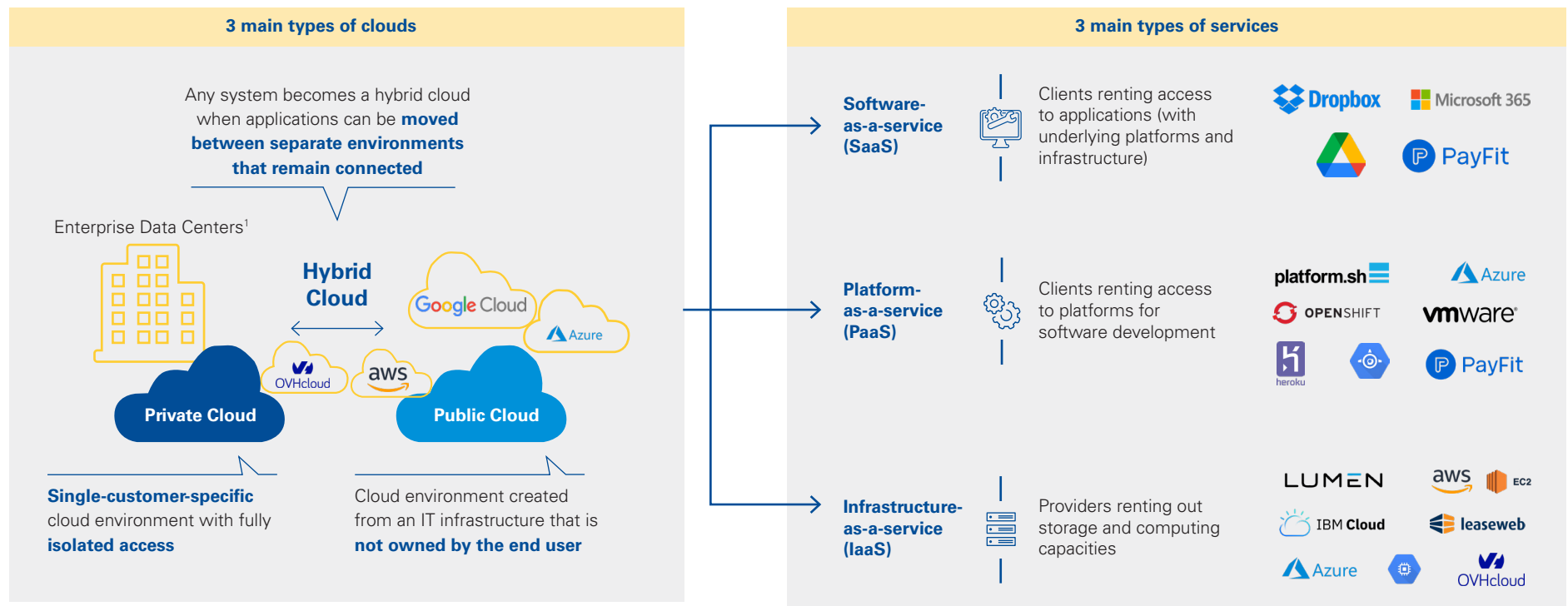


CLOUD i.e. rented servers from third-party



The market agrees on six “cloud” segments to sum up the large range of market offers

Overview of Cloud computing environment per type of cloud and type of service




Note: (1). May be located either within the company (on-premise) or hosted by a cloud provider (hosted private cloud)
Source: GSG research and analysis

NON-EXHAUSTIVE

Ranging from collaboration to more business specific tools, cloud services cover a large portion of companies' IT solutions


Main usages in each servicing model type

IaaS (Mainly used by CIO office)



- #1** Computing capacity (Extra capacity for computing needs)
- #2** Storage (Blocks, objects and files)
- #1** Virtual private server (Storage and computing environments on dedicated virtual servers)
- Baremetal and hosted private cloud (Physical and fully dedicated servers)
- Virtual networking (Isolated and highly secured virtual network)
- Security (Access management)

PaaS (Mainly used by developers)



- #1** Database management (Features for configuring databases)
- #2** AI / ML platforms (Ready-to-use environment for AI / ML programming)
- #3** Big Data & Analytics (Open source frameworks)
- #4** Business process management (Workflow management)
- API management platforms (Create, publish & secure APIs)
- Container management services (Deploy & manage containerized apps)

SaaS (Mainly used by end-users)



- #1** Customer Relationship Management (e.g. Salesforce CRM)
- #2** Enterprise Resource Planning (e.g. SAP ERP cloud)
- #3** Collaboration tools (e.g. Teams, Zoom, SharePoint)
- 5 Emails /Messaging
- Office Suite (e.g. Office 365, Google Workspace)
- Web hosting (E-commerce)

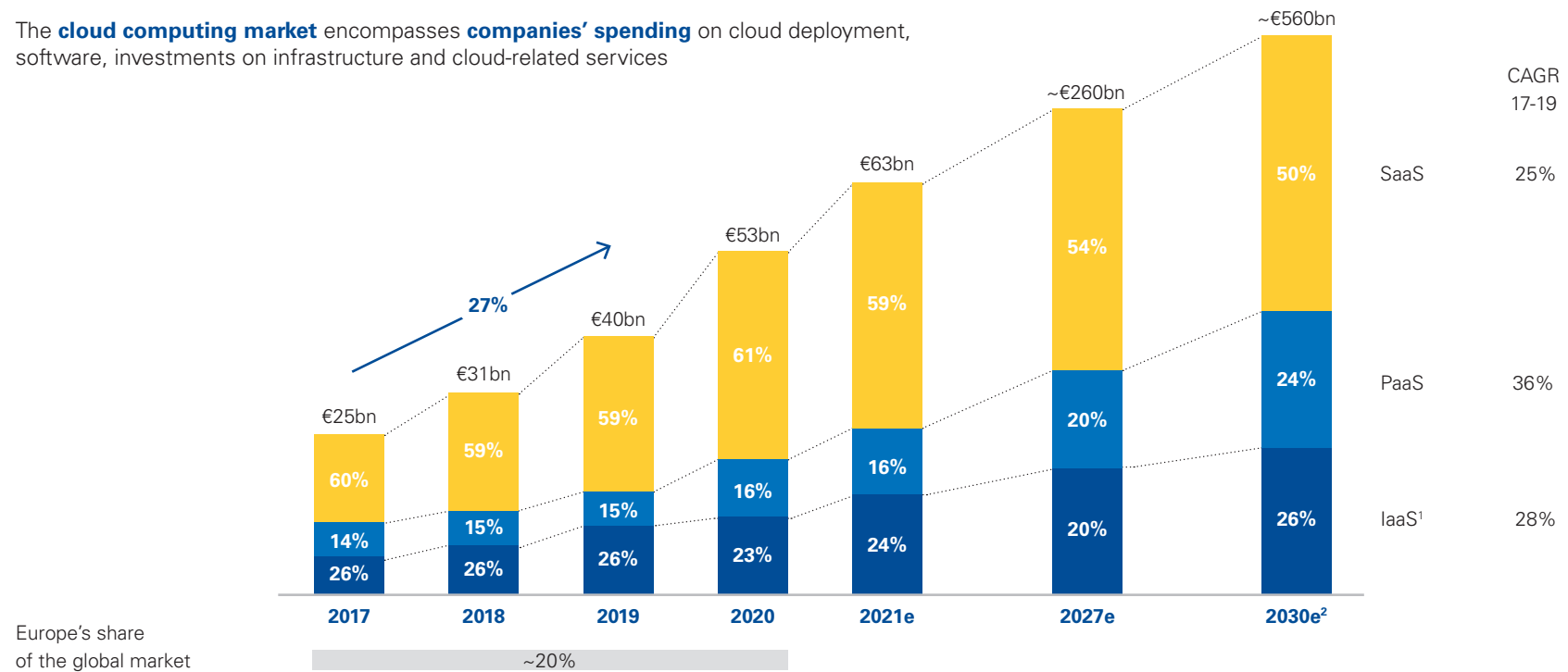
#X Ranking based on services revenue by category¹

Note: (1) Based on 2020 revenue in Europe (IDC)
Sources: Gartner; IDC IT Cloud services revenue; GSG research and analysis

The European market is a growing market (+27% p.a. during the 2017-2019 period) of €53bn in 2020 and is expected to reach c.€300-500bn from 2027

Evolution of European¹ IaaS, PaaS and SaaS market [2017-2030e, €bn]

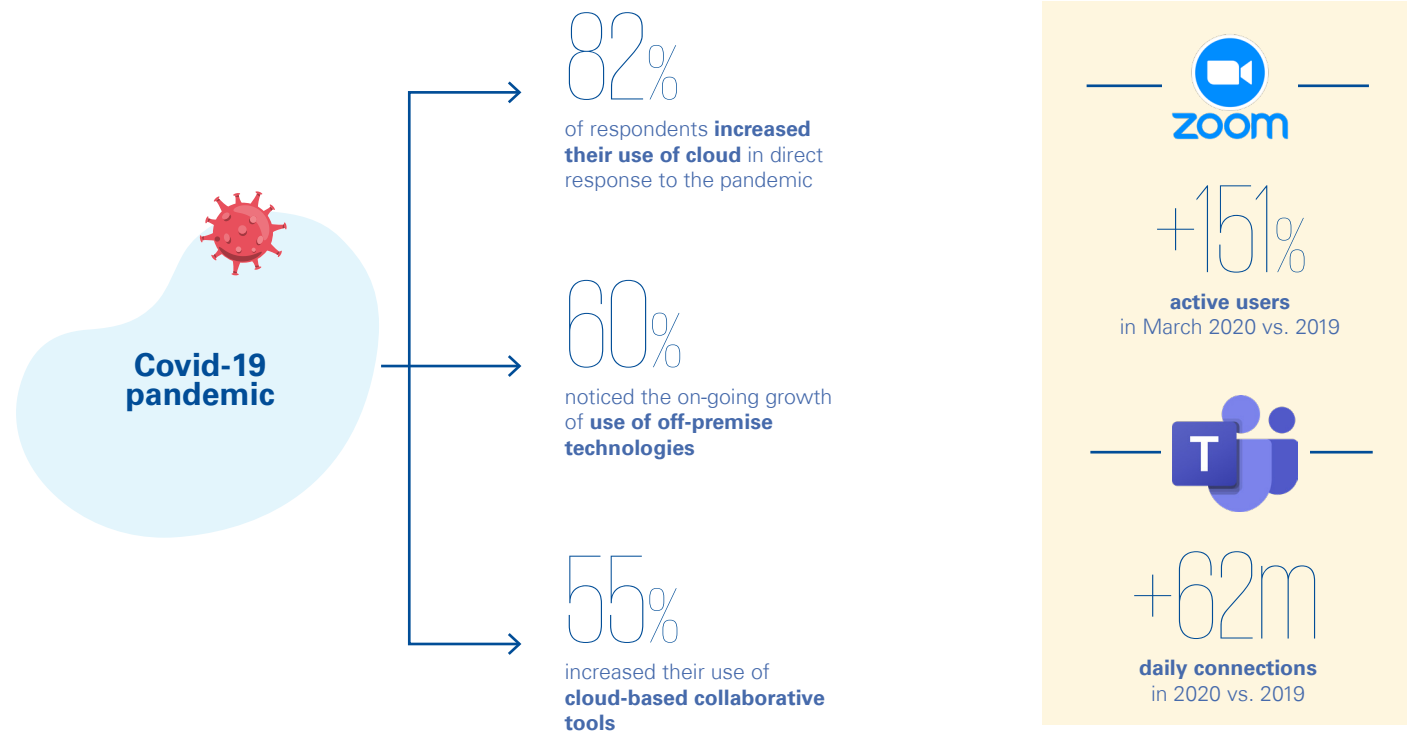
The **cloud computing market** encompasses **companies' spending** on cloud deployment, software, investments on infrastructure and cloud-related services



Notes: (1). IaaS market includes Public IaaS, Hosted private cloud and Baremetal cloud (2). GSG forecast
 Sources: IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018-2021 (IaaS, PaaS and SaaS); IDC-Predictions-2021 European cloud predictions; IDC-2019 Forecast (hosted private cloud); GSG research and analysis

Cloudification has been fueled by the recent COVID-19 pandemic, showing its strategic role as essential infrastructure and “resilience” enabler


Post COVID-19 status of worldwide cloud migration¹ [2020]



Note: (1). Out of the 250 surveyed IT leaders around the world
Sources: IT asset management firm Snow Software; GLG Industry Insights; Experts' interviews; GSG research and analysis



The stake for EU cloud providers is by 2027 a market of ~€260 bn in terms of spending, ~550k associated jobs and ~€200 bn investments (over 2021-2027 period)




~€ 260 bn
expected for cloud market size in 2027

Similar to following European markets

~€250 bn in 2020
Telecommunications market


~€190 bn in 2018
Textile market



550-600 K
jobs created,
for a 2027 market of ~€260bn

Many jobs located in regions, within Datacenters or regional offices:

- Integration Developers
- Project /Territory Managers
- Data Analysts
- Business developers
- Sales Reps
- Etc.

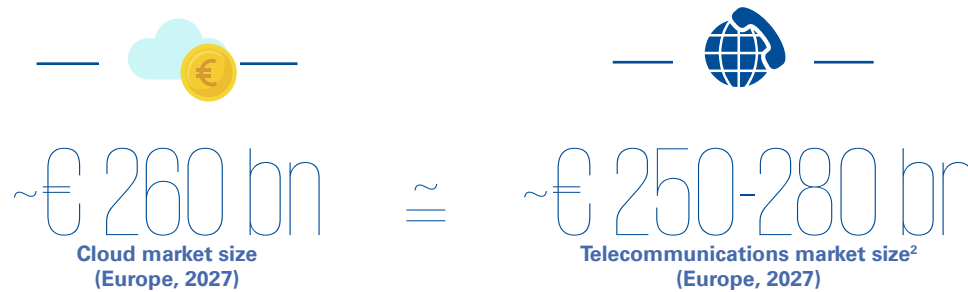


~€ 200 bn
expected investments
over 2021-2027 period

Key areas of investment for Cloud providers over the next 10 years will include:

- Energy efficiency improvement
- Data center architecture switch towards ARM processors, offering greater performance
- R&D in fields such as AI, cloud gaming, drug discovery...

Although expected to be comparable in size to the Telco market in the next ten years, the cloud market is still embryonic vs. the mature Telco market



The European Cloud market should be **comparable in size by 2030** with the European Telco. market

The Cloud market is expected to follow the footsteps of Telco sector to reach the same level of maturity through **local authorities' interventions**, becoming like:

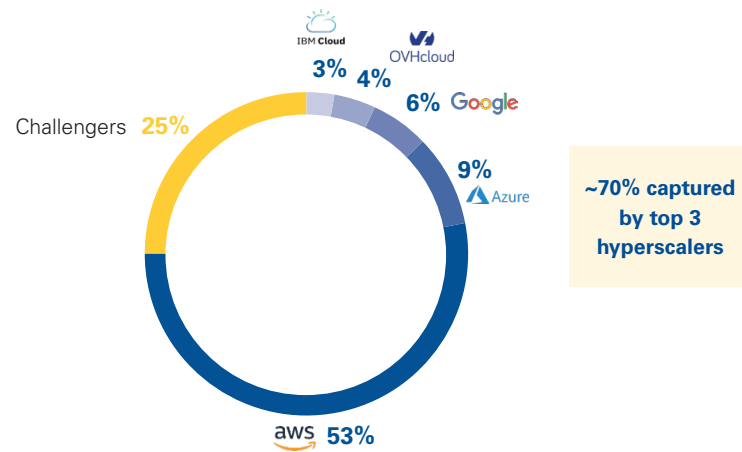
- A highly competitive market, with **licenses and high competition (~200+ mobile operators¹** across Europe in 2018) allowing for **good price competitiveness and pressure on profit margins**
- A highly regulated market governed by **public and competition authorities** (e.g. ARCEP), **local government agencies and telecom regulators** (e.g. BEREC, EU's telecom regulating agency) **fostering innovation and end-customer protection and regulating** on the other hand **consolidation / merger plans**

Notes: (1). MNOs: Mobile Network Operators (2). KPMG Estimate, assuming stability / slow growth vs. current situation (€ ~250bn)
Sources: Gartner 2019Q3 (public cloud); IDC 2019 Forecast (private cloud); ETNO 2020; The Delta perspective 2019; GSG research and analysis



The market is weakly competitive, with 3 global “hyperscalers”, US-based, dominating the cloud market – e.g. ~70% of IaaS market share

Breakdown of European cloud computing market (IaaS) [1H2020]



Landscape of top players in the French and German cloud market (IaaS, PaaS and hosted private clouds) [2020]

	France	Germany
Leader	aws	aws
#2	Azure	Azure
#3	OVHcloud	Google
#4	orange	T-Systems
#5	Google	IBM Cloud
#6	IBM Cloud	ORACLE

The vast majority (~70%) of European companies’ spending on cloud infrastructure (IaaS) is captured by non-European Cloud providers

Infrastructure & technology investments associated with cloud technology are also mostly located outside of Europe, e.g.:

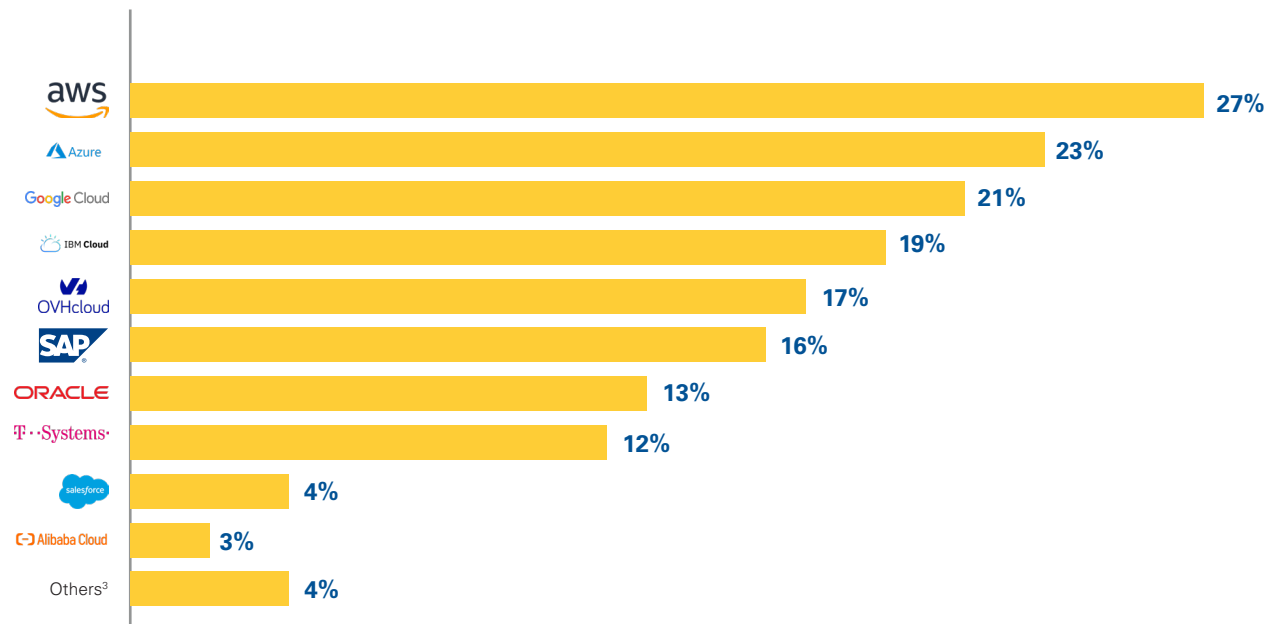
- Google Cloud invested +\$13bn in its cloud computing business in 2019, o/w **only 23% outside the US**, including Europe
- AWS’s investments are mainly located in US, as well as India (\$7.8bn invest. planned in 2020-2022 in the latter)

However, **European Cloud specialists and Telco operators are slowly gaining market shares** within their respective domestic markets (e.g., OVHcloud and Deutsche Telekom are in the 3rd and 4th position of their respective markets), regarding IaaS (incl. hosted private cloud) and PaaS

The domination is confirmed by the outputs of our conducted survey, with European CxOs choosing AWS, Azure and GCP to other cloud providers

Current cloud service providers within respondents' organizations¹

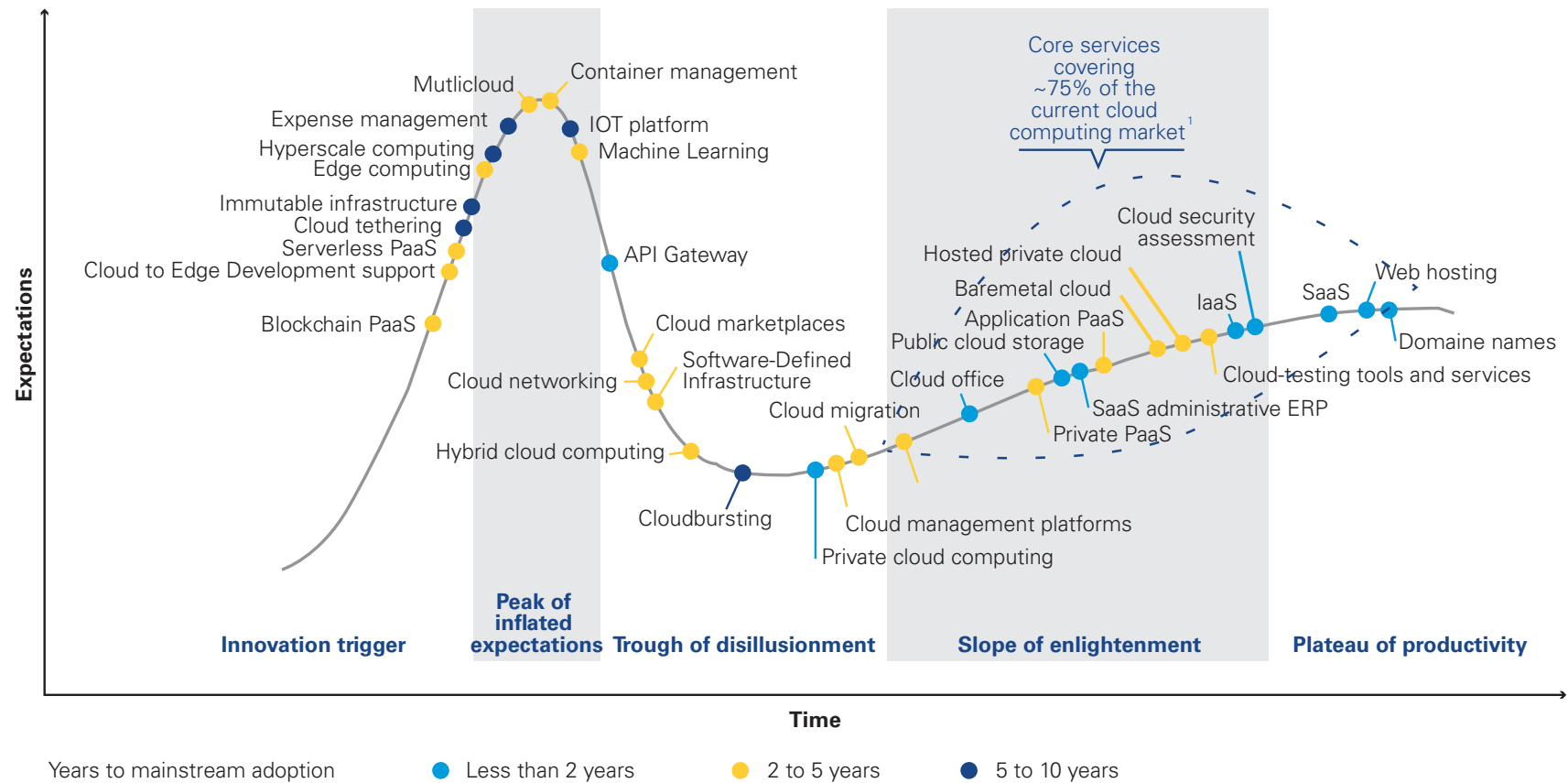
Who are your current cloud service providers², in particular for IaaS and PaaS? (several possible answers)



Notes: (1). Based on 200 French and Germany CxOs (2). Percentage based on the provider presence in the company, and not on the IT budget dedicated to this provider (3). List of other mentioned cloud providers: HCL, Scaleway, Veeva Systems, Huawei, TCS, QAD DynaSys Cloud
Sources: GSG Survey; GSG Analysis

Cloud computing is not yet a mature market, and will bring a large number of innovations in the coming years

Gartner hype cycle for cloud computing [2018]



Notes: (1). i.e. approximately 75% cloud market size corresponding to the circled list of core cloud services
 Sources: Based on Gartner hype cycle curve for cloud computing 2018; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021







2



Migrating to the cloud: a mandatory but constrained path

The overall adoption and growing demand for cloud computing solutions is driven by operational as well as financial optimization motives

Selection of main cloud adoption motives (non-exhaustive)

	Cost variabilization	Flexibility to increase or decrease capacity	Team collaboration while upholding data security	Agility & seamless deployment	Security and new resilience paradigm	Enabling agile business moves
						
Example of situation	<ul style="list-style-type: none"> • Mid-market company CIO & CFO facing high fixed costs due to on-premise data centers, and considering cloud migration... • ...in order to turn data centers-related fixed costs (owned servers) into variable costs (cloud), and thus contribute to stabilize the company's overall margin 	<ul style="list-style-type: none"> • CEO of a startup, whose recently released SaaS product is enjoying very strong usage growth, thus requiring: <ul style="list-style-type: none"> - Flexibility to increase storage / computing capacity to meet demand... - ...While retaining ability to scale back capacity at any time if required 	<ul style="list-style-type: none"> • Due to the Covid-19 situation, an employee can no longer meet with clients face-to-face, yet has to exchange information online and share heavy and confidential documents • The employee thus uses a cloud-based SaaS solution as secure bridge between the two organizations 	<ul style="list-style-type: none"> • CIO / CTO of a company willing to gain IT agility, and avoid manual management of data centers (cables, racks...),... • ...and thus considering cloud migration to manage its infrastructure "as code" and not as a physical infrastructure 	<ul style="list-style-type: none"> • A CIO / CTO of a company willing to secure the companies' data and increase disaster resilience • A private individual struggling with the storage of large files and considering uploading files on the Cloud for: <ul style="list-style-type: none"> - Ease of access, for him and his family - Avoidance of data loss / theft 	<ul style="list-style-type: none"> • CxO willing to both improve the performance of its existing activities and develop new ones, by leveraging the full capacity of nowadays new technologies: <ul style="list-style-type: none"> - Optimized client journeys - Launching new products with AI or high-computing capacity - Agile and fast scale-up of new activities

These various motives for cloud adoption are reflected in the different interviews we have had with Cloud computing decision-makers (1/2)

European Cloud computing decision-makers verbatim

Cost variabilization

“The replacement of our aging legacy-systems was the perfect opportunity for us to choose a more variable cost structure for our IT systems by going to the cloud.”

CIO, Energy industry

Flexibility to increase or decrease capacity

“To instantly face peak activity periods, cloud computing is the best option, as opposed to costly internal infrastructures with longer capacity ramp-up”

CIO, French state-owned company

Team collaboration while upholding data security

“Thanks to the cloud, remote work during the lockdown period was set up quickly; our teams were able to collaborate efficiently, anywhere and on any device.”

CIO, Global consulting firm

“For a small startup like ours, with limited financial resources to invest on internal infrastructure and permanent IT teams, the cloud is the go-to solution.”

CEO, French Startup

“During the first week of the lockdown in march 2020, Teams usage was multiplied by 20. We would have never been able to do this internally, in such a short period.”

CIO, Energy industry

“Cloud-based collaboration tools allow us to share sensitive files with our customers on secure and encrypted channels.”

CIO, Global consulting firm

These various motives for cloud adoption are reflected in the different interviews we have had with Cloud computing decision-makers (2/2)

European Cloud computing decision-makers verbatim

Agility & seamless deployment

“The size and geographical coverage of the cloud provider is very important as they need to be capable of adapting constantly to our global needs.”

CIO, Multinational chemical company

Security and new resilience paradigm

“Customer data is the most valuable asset of my company. In case of a disaster, my business can be resilient as my data is secure in back-up datacenters, managed by cloud providers”

CIO, International bank

Enabling agile business moves

“As we developed a Cloud-based state-of-the-art gaming platform for our national market, it made sense to allow foreign players to also use it in their own market – so we’ve now become a SaaS provider in some way”

CIO, Gaming industry

“As we are eyeing an expansion into North America, we can’t rely anymore on our French data centers and will be considering also using Public cloud”

CIO, Gaming industry

“By migrating our data to cloud environments, we automatically had access to on-point cybersecurity technologies and security roadmaps of our cloud provider.”

CIO, International bank

“We chose to migrate to the cloud as the most innovative solutions are provided as SaaS”

CIO, International bank

Providers' selection is based on multiple criteria – the most important ones being data security and data sovereignty

Key purchasing criteria in the cloud computing market (based on survey respondents answers¹)

KPC	Weight	Rationale
Data security and governance	●	“Our cloud provider should be able to ensure highly secure infrastructure and services to prevent internal and external data breaches ”. French CIO
Regulatory risks and compliance (incl. data sovereignty)	●	“When choosing a cloud provider, data sovereignty and regulatory compliance are as important as service quality .” German CIO
Certifications & Standards	◐	“As we are handling sensitive health data , we cannot afford using uncertified cloud services . We chose our cloud provider accordingly.” French CIO
Service portfolio width and quality	◐	“ Scalability and reliability along with access to basic and on-point innovative technologies are our top priorities when selecting a cloud provider.” French CIO
Cost	◑	“We need providers who can cover our functional and infrastructure needs at reasonable and transparent prices .” German CIO
Company notoriety & Credentials	◑	“We need to be able to count on a reliable and large cloud provider who can accompany us on the long term , covering our technology needs and geographical expansion .” German CIO

Note: (1). Based on 76 French and German CIOs respondents (both quantitative and qualitative inputs)
Sources: GSG Survey; GSG Analysis



Respondents believe data sovereignty is important with a particular focus on GDPR compliance & data center location

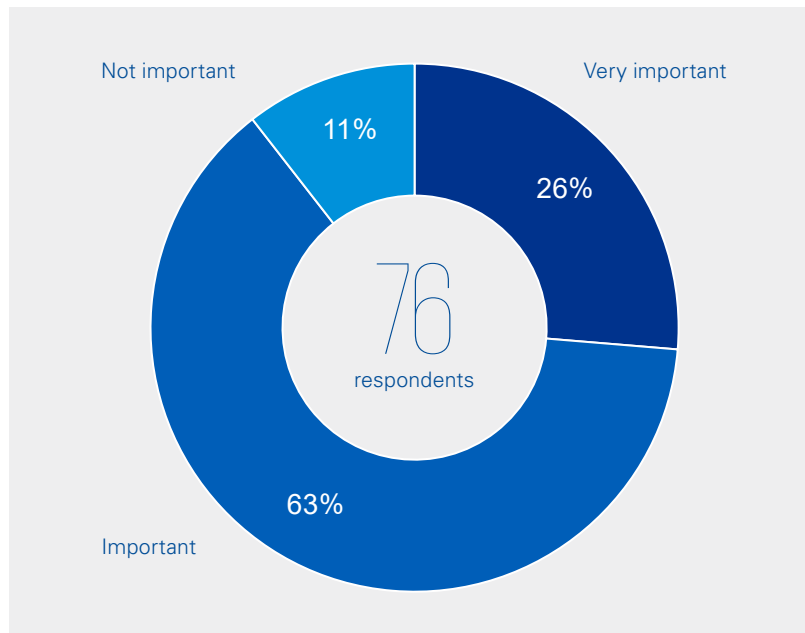


Regulatory risks and compliance (incl. data sovereignty)

Data sovereignty is mentioned as an **important** criterion in the decision-making process for selection of a cloud supplier for the vast majority of decision-makers interviewed ...



To what extent was / is data sovereignty a **criteria**n in choosing your cloud provider(s)?²

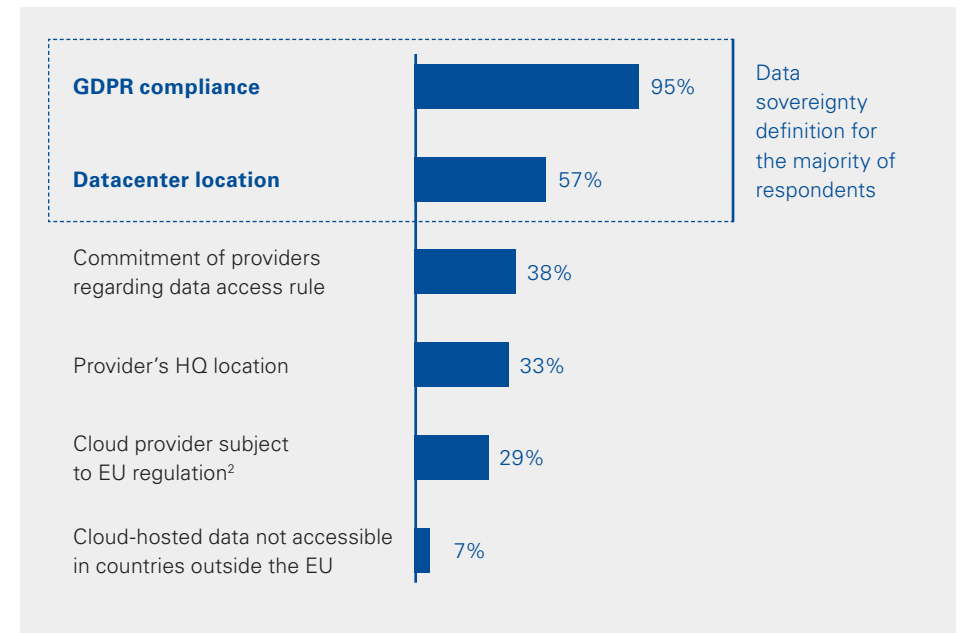


...Yet, sovereignty can take multiple meanings, especially two key dimensions

(compliance with GDPR regulation and datacenter location)



According to you, which ones of the following items **best describe data sovereignty?** (several possible answers)¹



Notes: (1). Based on 76 French and German CIOs respondents (2.) Cloud provider subject to EU regulation, exempt of extraterritorial legislation (e.g. Cloud Act)
Sources: GSG Survey; GSG Analysis

Despite the importance of data sovereignty in choosing a cloud provider, CxOs states that they are left with limited options



Regulatory risks and compliance (incl. data sovereignty)

Compromise at the expense of data sovereignty, considering offer too limited

“We **refuse to implement a cloud strategy** at the company level for data sovereignty reasons, but with peaks of activity, **cloud remains the only fast and efficient backup option.**”

CIO, European logistics service provider

“I would like to see the **emergence of European cloud providers**, it would facilitate internal alignment on cloud migration, due to concerns about sovereignty. But is it going to happen and when? I can't wait years with my aging systems ...!”

CIO, International oil & gas company

“As of today, there is no **satisfactory sovereign offer for health data**. Data migration to a sovereign cloud only seems **conceivable in the medium term, at least by 2022.**”

CIO, French state-owned company

Accept an incomplete data sovereignty compliance

“We chose a US cloud provider as soon as our **legal team approved the contract** – which wasn't reviewed since, **despite major regulation changes.**”

CIO, International oil & gas company

“Our **sovereignty concerns** are resolved by locating the data exclusively in the European Union, even if they are **detained by US providers.**”

CIO, International oil & gas company

“Even when the cloud provider guarantees the hosting of data in Europe, **extra-territorial ancillary transfers**, such as maintenance and technical support, still occur.”

CIO, International oil & gas company

The lack of knowledge for offers ensuring data sovereignty limits the growth of EU cloud market, with some companies giving up or slowing down cloud migration



Abandon cloud migration due to data sovereignty concerns

“A memo of the French Ministry of Interior and the Ministry of Culture **prohibits the storing of public documents on non-sovereign datacenters**. Such limitations **render cloud migration impossible** given the **limited number of sovereign offers on the market.**”

CIO, French state-owned company

“We **categorically refuse** to put our customer data **on the cloud for sovereignty reasons**, so we opted for on-premise storage for all our data and software.”

CIO, International gaming industry company

“As we have **no guarantee of the location** of the different components of the **cloud provider’s value chain** (storage, compute, maintenance), we have **no other choice than use internally managed datacenters** for our sensitive data.”

CIO, international bank

“The Executive Committee was very clear regarding the location of our customers’ data. **They need to remain in-house and must in no case be hosted by third parties.**”

CLO, European logistics service provider

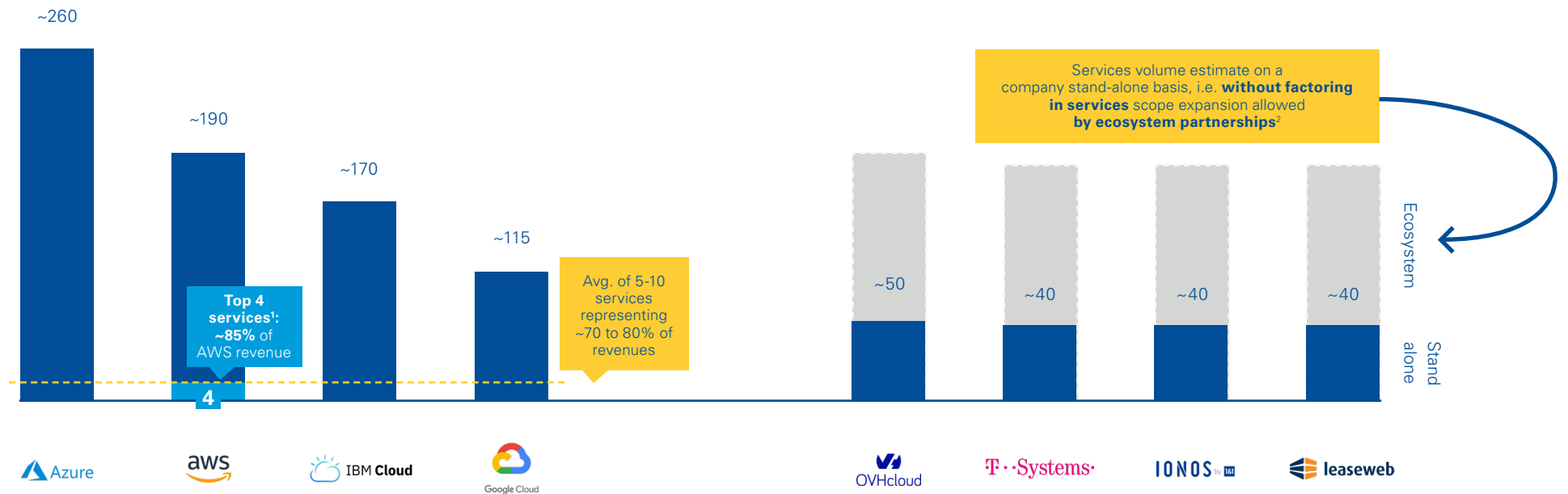
“When our data is **stored on-premise, sovereignty audits** are quite easy to conduct, which is **technically impossible** when using **the facilities of a third party provider.**”

CLO, European logistics service provider

Hyperscalers offer a wide range of services but the majority of their revenues is generated by few of them



Number of cloud services and products (within private, public and hybrid clouds) for some major cloud providers [2020]



Notes: (1). Basic services : EC2 (Elastic Compute Cloud, compute capacity), EBS (Elastic Block Store, block storage), RDS (Relational Database Service), S3 (Simple Storage Service, object storage) (2). See following slides for additional information
Sources: GSG research and analysis; Companies' websites; CloudPegBoard; Cloudability State of Cloud 2018

Yet the European Cloud ecosystem appears dense and rich, beyond simply generalist cloud providers



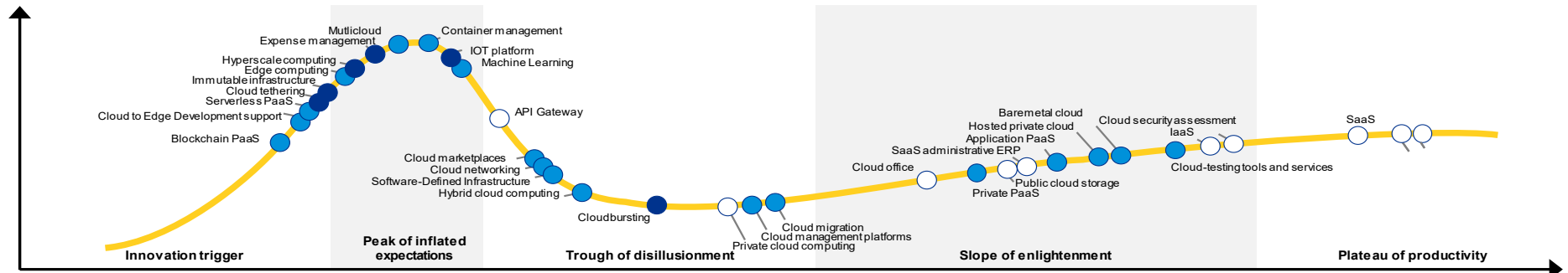
A dense European ecosystem of technology providers (non exhaustive)

Internet software & services	Cloud computing services	Artificial Intelligence	
		Internet of Things	
<th data-bbox="277 1145 790 1212">CyberSecurity</th> <td data-bbox="864 1212 1377 1361"> </td> <td data-bbox="1451 935 1957 1145"> </td>	CyberSecurity		
		Data management & services	

By leveraging their ecosystem, European players deploy an extensive offering with a breadth and depth mostly comparable to hyperscalers' ones



Cloud providers' offer positioning on the hype cycle for cloud computing [2018]



	Blockchain PaaS	Cloud to Edge Deve. Support	Serverless PaaS	Cloud Tethering	Immutable Infrastructure	Edge Computing	Hyperscale Computing	Expense management	Multicloud	Container Management	IOT Platform	Machine Learning	API Gateway	Cloud marketplaces	Cloud Networking	Software-defined infra.	Hybrid Cloud Computing	Cloudbursting	Private cloud computing	Cloud management platforms	Cloud migration	Cloud office	Private PaaS	Public Cloud Storage	SaaS Administrative ERP	Application PaaS	Hosted private cloud	Baremetal cloud	Cloud-testing tools & services	IaaS	Cloud Security assessment	SaaS	Web hosting	Domaine names
aws	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Azure	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Google Cloud	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Ovhcloud ecosystem	1	●	2	●	●	●	●	●	●	●	3	●	●	●	●	●	●	●	●	4	5	6	7	●	●	8	●	●	●	●	●	●	●	

● Provided by Company ● Provided by Ecosystem

Notes: (1). TON Ventures (2). Google Anthos, Clever Cloud (3). SmartHub (4) Cloudify (5). Capgemini, Atos, Sopra Steria, Partito (6). Sharepoint, Office 365 (7). Google Anthos (8). Platform.sh, Clever Cloud
Sources: Gartner hype cycle for cloud computing 2018; Wipro; Companies' websites; GSG research and analysis

European challengers, such as OVHcloud, through their dense ecosystem, have an exhaustive service portfolio covering most customers' functional needs (1/3)



Providers' services and their functional coverage¹ – Main offers



Note: (1). Based on communicated information on companies' websites
Sources: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Companies' websites; GSG research and analysis

European challengers, such as OVHcloud, through their dense ecosystem, have an exhaustive service portfolio covering most customers' functional needs (2/3)



Providers' services and their functional coverage¹ – Main offers



Notes: (1). Based on communicated information on companies' websites (2). Examples of offers available through marketplace
 Sources: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Companies' websites; GSG research and analysis

European challengers, such as OVHcloud, through their dense ecosystem, have an exhaustive service portfolio covering most customers' functional needs (3/3)



Providers' services and their functional coverage¹ – Main offers



Notes: (1). Based on communicated information on companies' websites (2). Examples of offers available through marketplace (3). Other partners include Zimba, Droptcloud and Nextcloud (non exhaustive)
Sources: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Companies' websites; GSG research and analysis

Despite unattractive communicated prices, global providers manage to dominate the market with aggressive and unconventional client acquisition practices...



Subsidies during client acquisition phase

“To facilitate our cloud migration to the public cloud of an international cloud provider, I was supported during 6 months by **5 full-time consultants, for free.**”

CIO, French state-owned company

“I was offered **a voucher of €100m** by an international cloud provider **in exchange for 5-year exclusivity contract.**”

CEO, German Fintech

“**My first year** as a global cloud provider services user **did not cost me a penny which helped motivate our migration to cloud.**”

CIO, French software provider SME

“Some global cloud providers’ goal is to **lock clients** in their ecosystem as fast as possible, which is **why data upload (contrary to download) is free.**”

CIO, global consulting firm

Tied selling, bundling or exchange of services

“The signature of a large **core-business supply contract** with an international cloud provider was **subject to one key condition:** the migration of our data on their public cloud.”

CIO, international oil & gas company

“I initially wanted to use Office 365 on another cloud environment, other than Microsoft infrastructure, but **I quickly faced the reality of it being way more expensive.**”

CIO, French software provider SME

“One of the reasons that accelerated the decision of changing our current cloud provider is **the aggressive practices of its salespeople.** We were often **forced to take and pay for other cloud services that we did not need.**”

CIO, global consulting firm

“Notorious office tool suppliers **market IaaS and SaaS bundled products**, at extremely attractive prices, costing **five times less than competitors’ IaaS only offers.**”

CIO, European logistics service provider

...in particular through the bundling of SaaS and IaaS services for software products historically running in local environment



A historically large customer base using **desktop software**, now being leveraged by some hyperscalers...

From¹

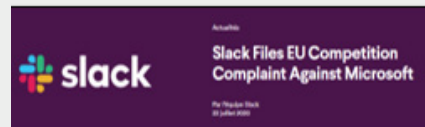
to



Office 365

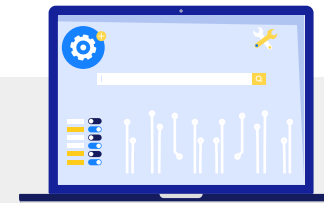


... through a bundling & tied selling of **IaaS + SaaS** offers, sometimes breaking BYOL ("Bring Your Own License") principle through technical and financial constraints...



"Microsoft has **illegally tied** its Teams product into its market-dominant Office productivity suite, **force installing it, blocking its removal**, and **hiding the true cost** to enterprise customers."

Slack press release, July 2020



As a consequence, a number of historic software providers are currently bundling their legacy software products (now in SaaS) with their IaaS products...

While often both products had historically and can technically been separate²

Note: (1). Non-exhaustive, examples of providers' products ; (2). E.g., Office 365 currently sold separately from Azure in China
Sources: Companies' websites; GSG research and analysis

Adding to the unconventional client acquisition practices, complex exit conditions make it difficult for cloud users to exit or switch from one provider to another



High barriers to exit & Vendor lock-in

“Once you’ve uploaded all your data on their [international cloud provider] cloud, you **realize that you are trapped** as the cost of moving it elsewhere is extremely high.”

CIO, global consulting firm

“We made the **quick and easy choice** to use proprietary APIs provided by international cloud providers, instead of developing our own, **knowing how difficult and costly** it would be to get out of it.”

CIO, international oil & gas company

“For public authorities, cloud contracts must, **by law, be reviewed regularly**. Thus, public cloud providers, with their **lack of portability and high exit costs, are not an option.**”

Head of the Technical Infrastructure Department,
French public authority

“Our developers made the choice of using **innovative and easy-to-use proprietary solutions** of a global cloud provider. We were not opposed to it, until we faced **migration problems**, and had to consequently **go over budget.**”

CIO, global consulting firm

Long-term and committed contracts, with unclear pricing terms

“If you decide to terminate your contract with some international cloud providers 3 years before its end, you **will have to pay the full amount of the remaining 3 years.**”

CIO, French software provider SME

“Between **the high early termination fees of fixed term contracts and the spending commitment clauses** set by some global cloud providers, changing cloud providers along the way becomes a **very costly decision.**”

CIO, French state-owned company

“Attracted initially by **the cheap upfront storage prices** offered by our chosen global cloud provider, and unaware of the remaining incurred costs, our **total cost of ownership grew rapidly** as our **systems got more complex.**”

CEO, German Fintech

“Today, we are not yet able to **forecast our cloud costs** due to the **complexity of the contract**, the **difficulty** to have a clear understanding regarding **the scope of services provided** and our **lack of maturity regarding these topics.**”

CIO, European logistics service provider

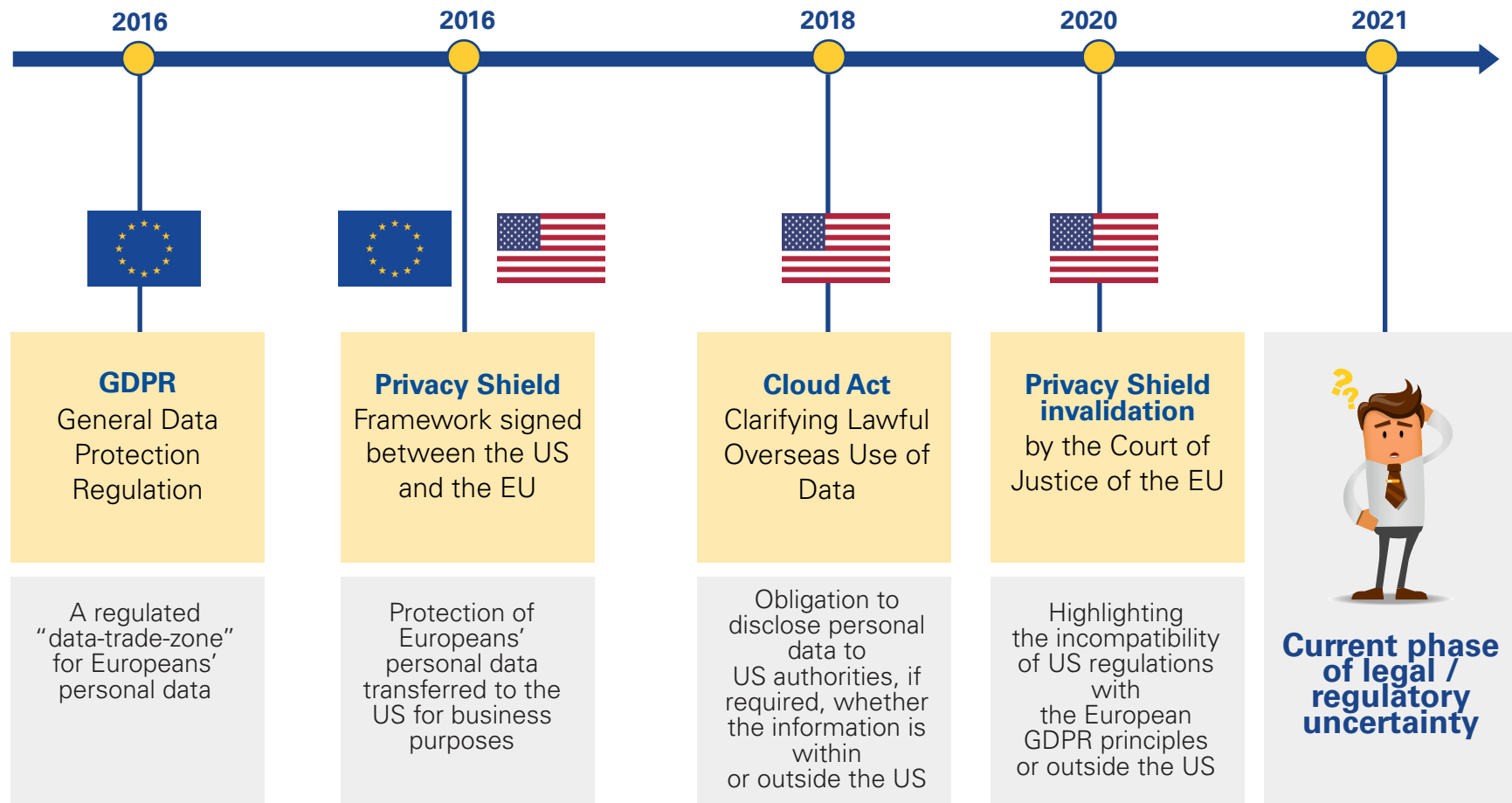
3



Data-related legal
uncertainties:
what are
the risks for
European
companies?

Since 2016, the introduction of new regulations pertaining to data in the US and the European Union have had significant impact on Cloud computing

Main recent regulations pertaining to the cloud market



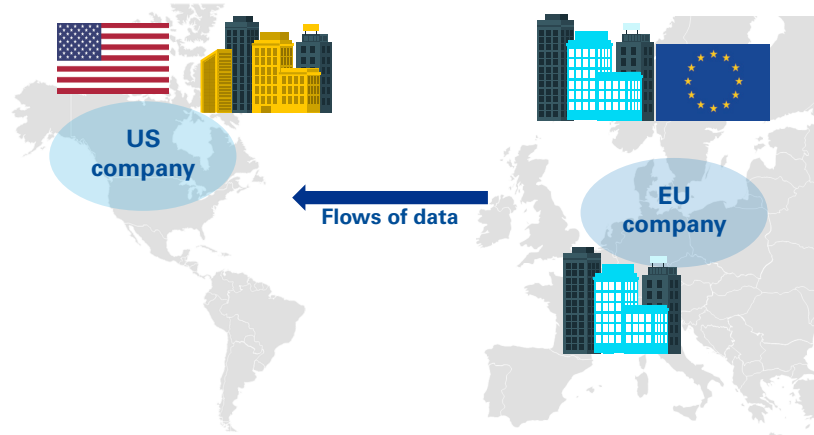
Sources: KPMG Avocats and GSG research and analysis



See Appendix for additional information

These regulations have tried to establish a strict legal framework with regard to flows of European data involving US companies (in and outside the EU)

Flows involving US companies – outside the European Union



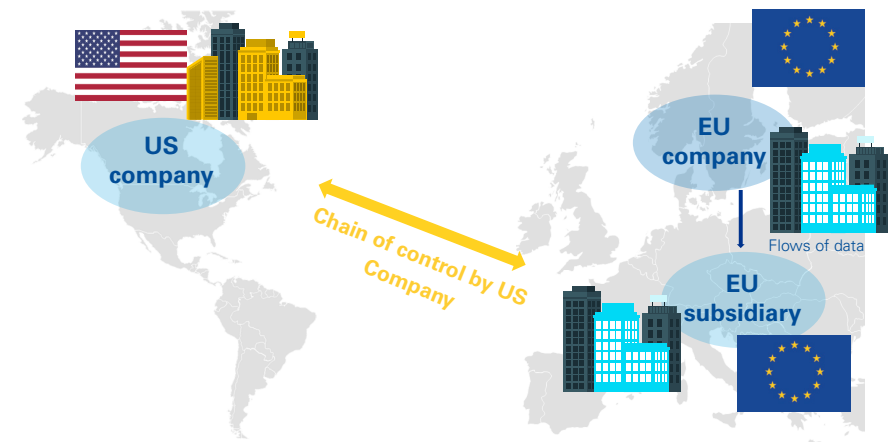
Such transfers of data were allowed since the effective and adequate level of protection was ensured by the **Privacy Shield**

BUT



In July 16th 2020, the EU Court of Justice **invalidated the Privacy Shield agreement**, considering that the US surveillance programs were not compatible¹ with the GDPR principles (Schrems II Case)

Flows involving US companies – in the European Union



Such transfers of data are **allowed under the GDPR through processor contract (including standard contractual clauses) and joint controllers' contract**

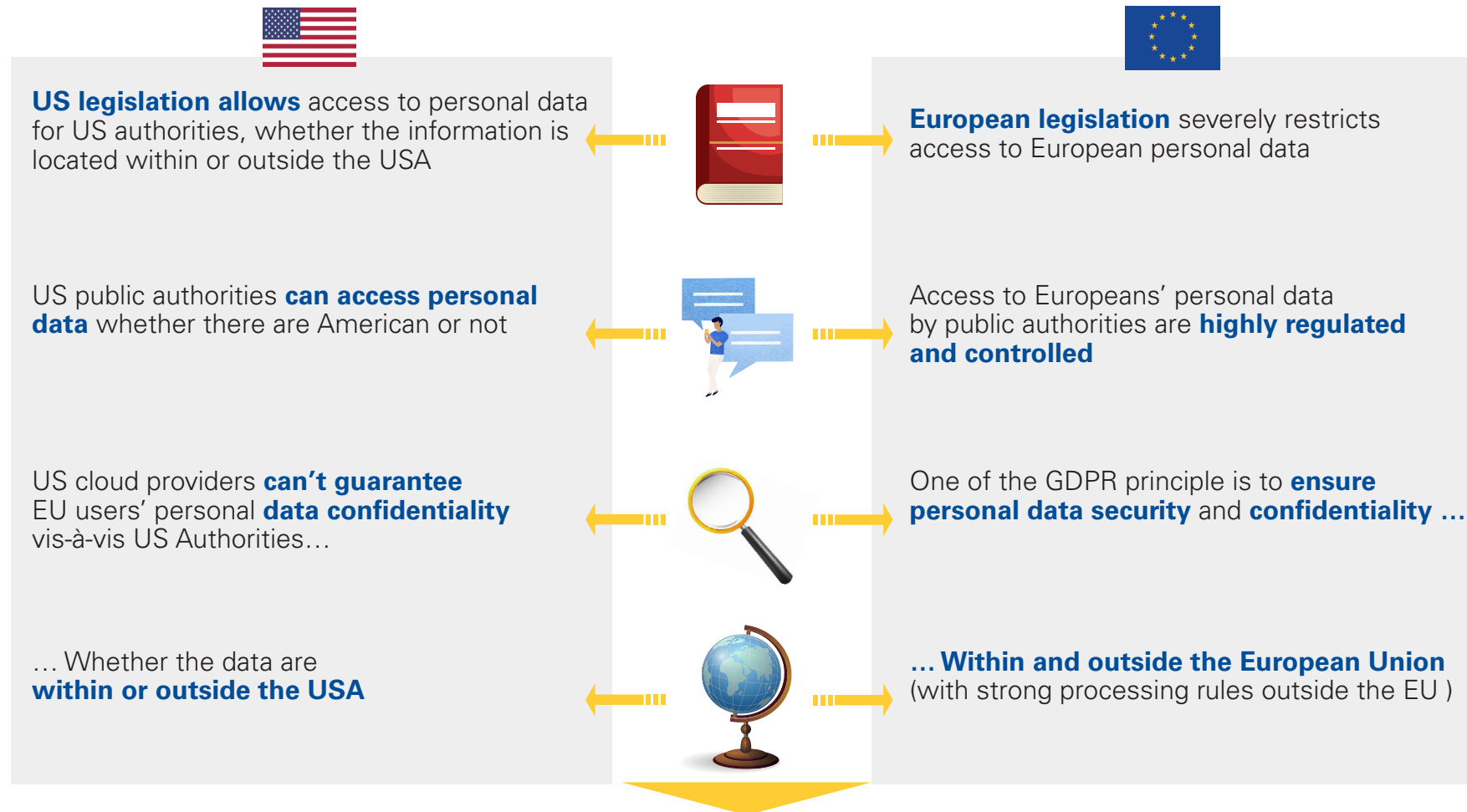
BUT



National legislation
(such as the Cloud Act)
prevails on contractual frameworks

Note: (1). The US legislation is allowing public authorities to access any personal data that are transferred on US soil, namely the "Foreign Intelligence Surveillance Act" (FISA) and the Executive Order 12333
Sources: KPMG Avocats and GSG research and analysis

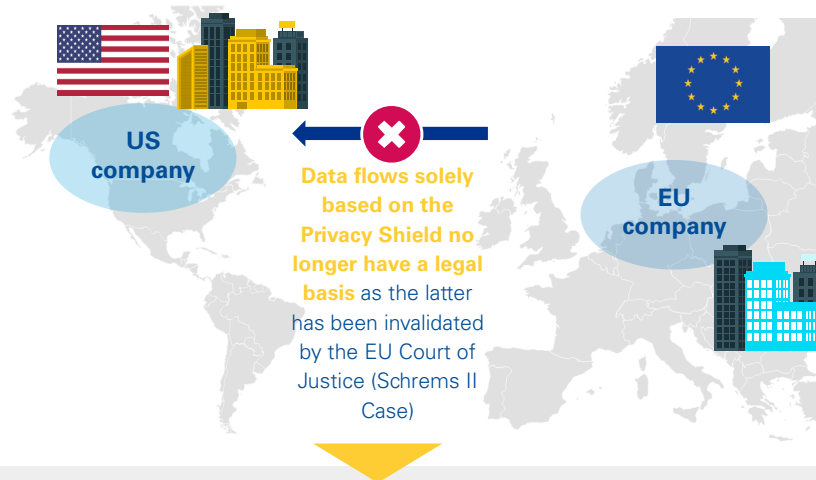
However, current US regulation appears structurally irreconcilable with European GDPR principles, which aim to protect EU citizens' personal data



This regulatory incompatibility appears quite irreconcilable

Companies transferring European's personal data to non-EU companies' servers no longer have a legal basis to do so under Privacy Shield and may be subject to prosecution

Outside the European Union



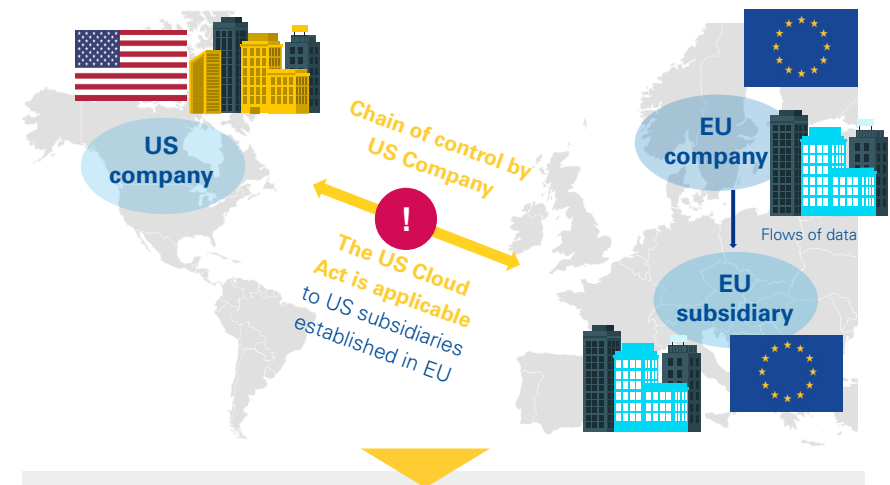
European Data Protection Board (EDPB) tried to fix this legal uncertainty arising from the invalidation of the Privacy Shield through an accountability Roadmap around the transfers : **Know Your Transfers (KYT)** composed of 5 authorized and 2 prohibited¹ uses-cases

Experience has shown that the 2 prohibited uses-cases are in fact the most common cases of data transfers

As-is situation

The legal uncertainty remains and could only be resolved by a change in US legislation on privacy

Within the EU



As National legislation prevails on contractual frameworks, **the American Cloud Act is applicable to American subsidiaries established in the European Union:**

- American public authorities could access the personal data held by EU subsidiaries without consideration of their localization
- Contracts concluded between an EU data controller and European subsidiaries could be challenged for non-compliance under the GDPR

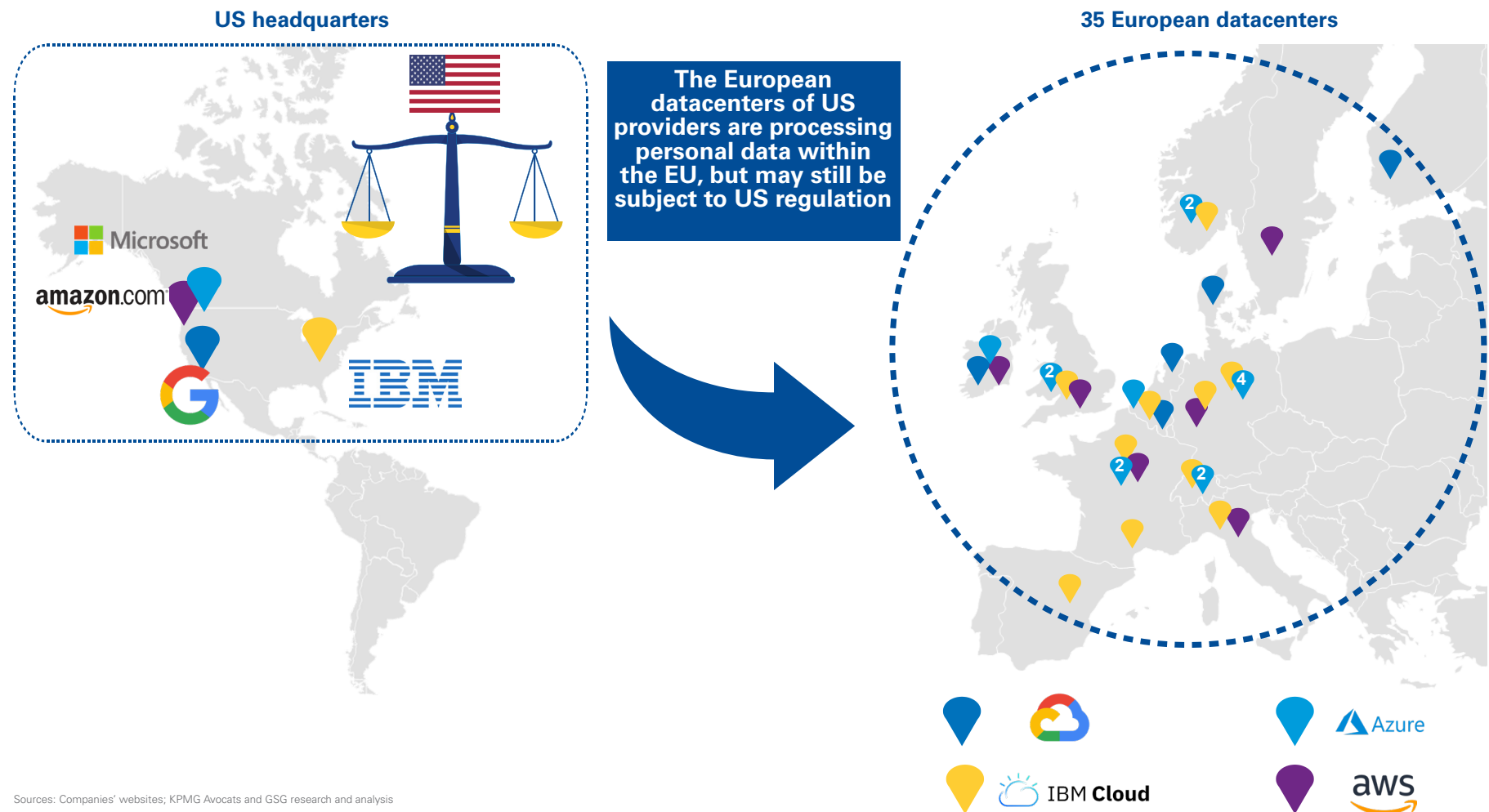
As-is situation

Companies subject to the GDPR can be held liable for non-compliance to security measures vis-à-vis regulation authorities, clients and consumers

Note: (1). "Transfers of data to cloud services providers or other processors which require access to data in the clear" and "Remote access to data for business purposes"
Sources: KPMG Avocats and GSG research and analysis

Locating Europeans' personal data within European datacenters of US providers still does not guarantee their security as they may still be subject to US law

US cloud providers' datacenters in Europe [2020]



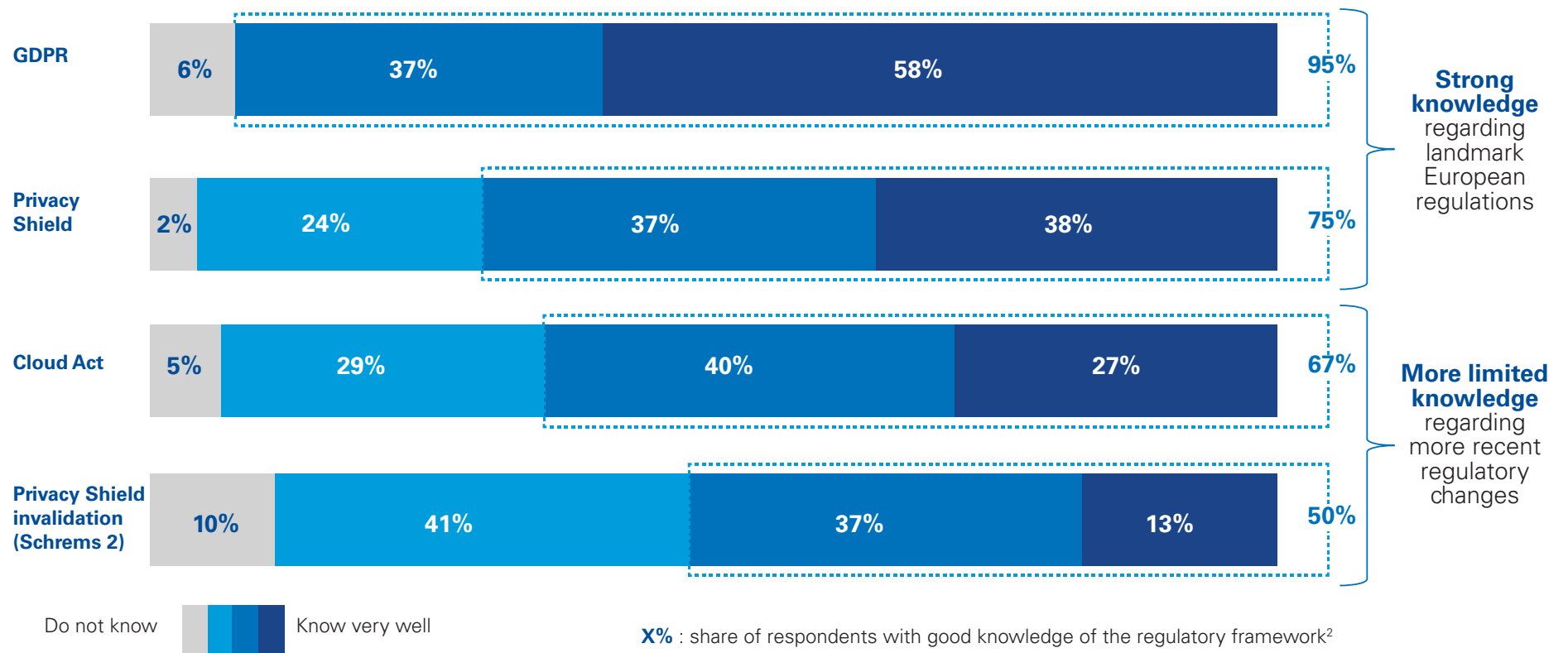
Sources: Companies' websites; KPMG Avocats and GSG research and analysis

Among cloud computing decision-makers, the level of knowledge regarding data regulations is variable; strong for GDPR but limited for Cloud Act and Schrems 2

European respondents' knowledge of pieces of data regulation



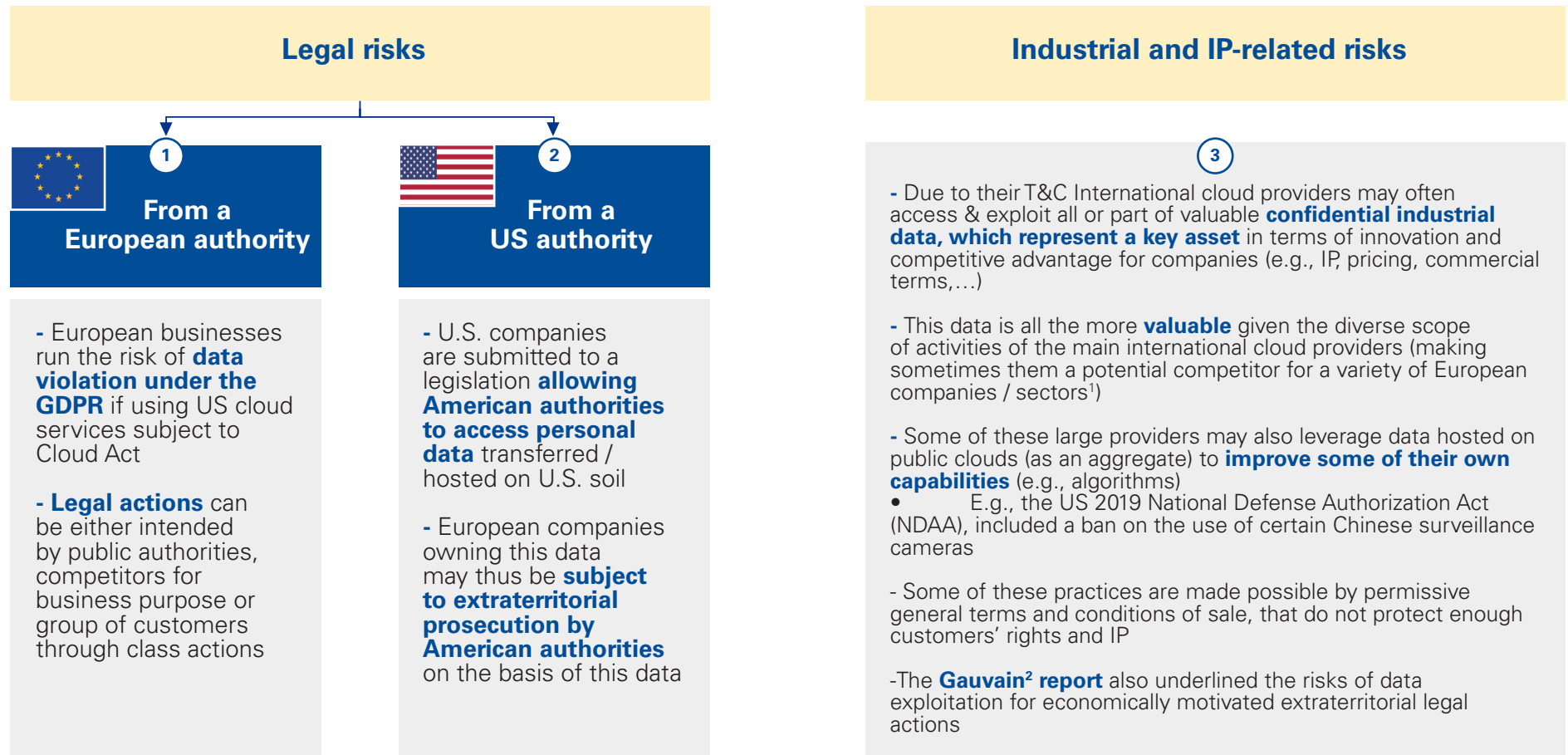
Please specify your level of knowledge regarding these regulations¹



Notes: (1). Based on 200 French and German respondents, incl. 76 CIOs and 124 CMOs / CEOs / CLOs / COOs. May not add up to 100% due to rounding (2). Answers from "Know well" to "Know very well"
Sources: GSG Survey; GSG Analysis

Today's state of uncertainty presents multiple risks for European companies

Main risks identified for European companies using US / non-EU cloud providers regulation



Sources: Experts' interviews; KPMG Avocats and GSG research and analysis

Note: (1). as diverse as retailers (e.g., Amazon), aerospace (e.g., Blue Origin), automotive (e.g., Waymo)...(2) Gauvain report on the protection of companies against extraterritorial laws and measures, June 26, 2019

In the European Union, companies that do not comply with GDPR principles run the risk of severe financial penalties, such as Google fined €50M by the CNIL

Financial penalties in case of non-compliant with GDPR



From a European authority

1

Art. 83 GDPR



General conditions for imposing administrative fines

According to GDPR rules, financial penalties can amount up to €20m, or represent up to 4% of the annual turnover, but lack of uniformity on sanctions in the EU

2018-2020

€280m+ in fines

160,000+ notifications of violations

Example of financial penalties imposed to Google (2019)



- In January 2019, the French CNIL¹ imposed a **financial penalty of €50m against Google LLC**, in accordance with the GDPR, **for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization**

«The non-compliances detected deprive users of fundamental guarantees regarding data processing that may reveal entire area omission of an indefinite article. »
(CNIL press release, 2019)


- Furthermore, the French CNIL has announced the end of the leniency period on March 31st 2021 – As of this date, French companies will have no further excuses for their non-compliance to the GDPR



Note: (1). CNIL: Commission nationale de l'informatique et des libertés
Sources: DLA Piper GDPR Data Breach Survey 2020; KPMG Avocats and GSG research and analysis

In the US, the Cloud Act allows access by U.S federal authorities to data stored in foreign countries, with potential sanctions in case of non-compliance


Principles allowing data access by US authorities



From a US authority


2

Principle



Data stored outside the U.S. with a service provider that is subject to U.S. law may be transferred to the U.S. government under a Court subpoena

Existence of agreements



Within the framework of the Cloud Act and in order to facilitate and properly regulate the exchange of information, countries may enter into **executive agreements** with the United States. In this case, both nations would be able to submit direct orders to suppliers for electronic evidence needed, **without involving the other government.**

Potential related penalties and situations for European companies

The Cloud Act does not specifically provide for sanctions in the event of non-compliance with injunctions made to service providers, potential consequences would include:

US service provider with or w/o Europe subsidiary	<p>Authorized authorities can turn against the U.S. service provider. If a subsidiary exists in Europe, as a parent company, the American provider have control over its subsidiaries, and thus, over their data.</p>
EU service provider with subsidiary in USA	<p>Authorized authorities may only turn against the European service provider's US subsidiary. The US subsidiary can appeal the decision of the US court. Furthermore, the US subsidiary cannot be obliged to provide the information if it has neither legal control nor technical access to the data.</p>
EU service provider without a subsidiary in the USA	<p>No possible leverage against these service providers as:</p> <ul style="list-style-type: none"> - The Commission made clear¹ that GDPR requires executive agreements (even if transfer requests are based on foreign court orders) - Moreover, transfers of personal data are subject to several additional conditions (e.g.: suitable safeguards) - If an European provider comply with a U.S. court order when there are no executive agreements between the U.S. and the EU country in question, then the European provider will be in violation of EU law²

Notes: (1). in its letter to the Supreme Court in the Microsoft case (2). This has been confirmed by more recent decisions of the Commission (i.e. Schrems 2)
Sources: KPMG Avocats and GSG research and analysis

Furthermore, US Cloud Providers' contracts are usually standard form contracts, making it nearly impossible for their clients to negotiate their contractual terms

Examples of excessive dispositions found in several US Cloud providers' contract

3

Excessive terms regarding intellectual property of Cloud Providers' clients

Several US Cloud Providers are implementing **license clauses**, requiring the client to grant its Cloud Provider a **royalty-free, worldwide, non-exclusive right and license** for the duration of the client's intellectual property rights consider using all the clients technologies, brands, content, product information, data, materials and other products or information **provided or made available by the client to the Cloud Provider**.

That kind of clause can be very problematic since such wide license is :

- **imposed** by the US Cloud Provider and **non-negotiable** by the client,
- not always limited to the provision of the service,
- allowing the Cloud Provider to **use, modify, copy and distribute its clients' intellectual property rights** when such intellectual property rights are made available by the client while using cloud services

Excessive terms regarding payments and termination terms of Cloud Providers' contract

Regarding the possibility for companies to change their hosting providers, several Clouds and Hosting providers implements **payments clauses that survives the end of the contract**. In other terms, such contracts do not allow the clients to terminate the contract before its term and all payments due under the contract shall survive the termination or expiration of the contract.

That kind of clause is abusive since it is :

- **imposed** by the US Cloud Provider and **non-negotiable** by the client,
- providing that if the client wants to terminate the contract, it will **still be liable for all sums due under** it, even for the period not consumed, it being specified that for certain contracts, the sums due for one year may amount to several thousand/million euros



Our interviews show that this situation raises fears of multiple actions in the next years and lead to financial and business risks for companies (1/2)



CASE EXAMPLE 1:

A dismissal canceled for reasons based on data hosted on US cloud

- A sales manager provides **sensitive data to a competitor**.
- Following a litigation regarding his dismissal, the company defends itself by **producing data demonstrating the sales manager's failures** (logs, unauthorized access, emails, absence, working time, etc.).
- This data is either hosted in US cloud providers' datacenters or generated by cloud-based systems or tools, offered by US providers.

- **This evidence**, although technically valid, **could be legally challenged as having been collected illegally**

- Consequently, the judge could decide that the decision of dismissal is unfounded and sentence the company

CASE EXAMPLE 2:

A European company can't take legal action after a theft of customers' data hosted by US providers

- A company is subject to a **theft of customers' data** which was stored and processed in the US.
- Following investigation, the company managed to **identify the thieves**, and was considering **taking the case to court**.
- However, the company realized that **the relevant evidences** were extracted from an access monitoring system **stored and processed in the US** without any legal basis for such processing.

- The company will be dealing with the high risk of **challengeable evidences, preventing it from contestable fair compensation of its damage**. Furthermore, the company would also face the possible invalidation of the transfer and therefore the need to redeploy the flows of data, with a risk of administrative fine for lack of GDPR compliance



Our interviews show that this situation raises fears of multiple actions in next years and lead to financial and business risks for companies (2/2)

CASE EXAMPLE 3:

Transfers of personal data even between a franchisor and its franchisee must be framed respectfully regarding the GDPR

- A group of retail franchisees have entrusted the franchisor with the **storage of customers personal data**.
- The franchisor is granted an access to such data with the aim to run **marketing campaigns** (e.g., via e-mail).
- The personal data transfer was not framed enough or controlled, therefore it was difficult for the franchisor or the franchisee to **identify whether a customer had given or withdrawn its consent** for receiving marketing campaigns by email.

- **Some customers file complaints before the CNIL and CNIL sentences the franchisor and forbids the data transfer.**

- Therefore, the franchisees are no longer able to perform their marketing campaigns anymore and **could turn against the franchisor** for loss of money because they can no longer do their advertising campaign and have lost money.

CASE EXAMPLE 4:

Europeans citizens can no longer have a guarantee regarding the security of their health data

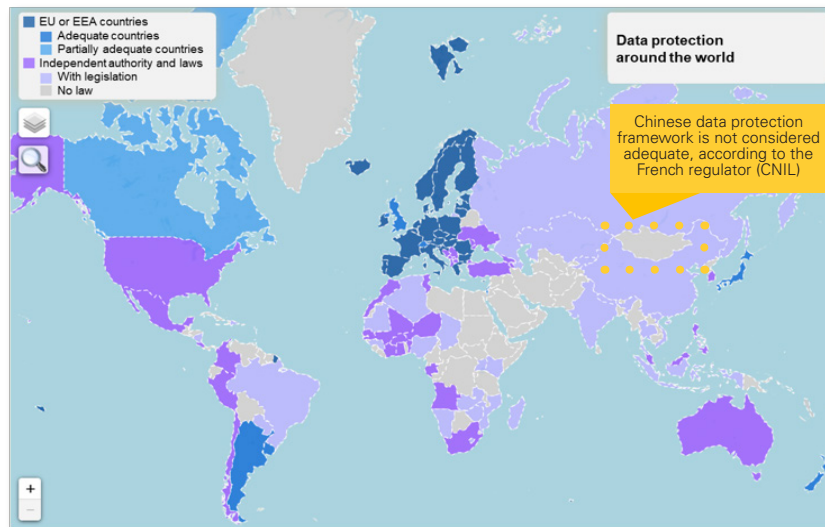
- An organization in charge of a concession of public service which includes **health data analysis, has contracted with a US cloud services company to the storage of those data**.

- The delegating authority could make an injunction to **change the data host**, or even **terminate the contract** with no compensation, on the grounds that US transfers of health data are not RGPD compliant.

- **Citizens** concerned by this data transfer **could take legal action** against the delegate.

Beyond the US, other regulations such as in China are also granting extraterritorial actions, leading to similar sovereignty issues for Europeans

Data transfers between the European Union and China must be handled with adequate security measures...



- China is **not recognized as adequate** by the European Union
- Consequently, **personal data transfers** are possible between China and the European Union, but must be regulated, through the implementation of adequate **transfer tools** (e.g. Standard Contractual Clauses or Binding Corporate Rules)

...but yet do not fully prevent from potential extraterritorial actions by Chinese govt. for national security reasons

China's Cybersecurity Law (2017)

- Provides guidelines to maintain network security, protect the rights and interests of individuals and organizations, and promote the development of technology, including:
 - **Data storage within China**
 - Organizations and network operators **submitted to government-conducted security checks**

Data Security Law of the People's Republic of China¹ (2021)

- **Scope:** applies to all "data activities," including the collection, processing, control and storage of data involving national security, business secrets and personal data
- **Extraterritorial application:** Article 2 states that jurisdiction extends to "organizations and individuals outside of" China who engage in data activities that harm China's national security or the public interest of the Chinese people

- **Transfer tools** that have been put in place **do not seem sufficient** to protect Europeans personal data
- If Chinese cloud providers succeed in gaining market shares in Europe, **European companies will be required to pay the same of attention to the Chinese regulation** as they are currently to the US one

Please read details in Appendix

At the end, European data sovereignty is the combination of a set of approx. 8 criteria, to be considered as a whole for full compliance and business risk avoidance

What is data sovereignty?



What is a European Sovereign Cloud?

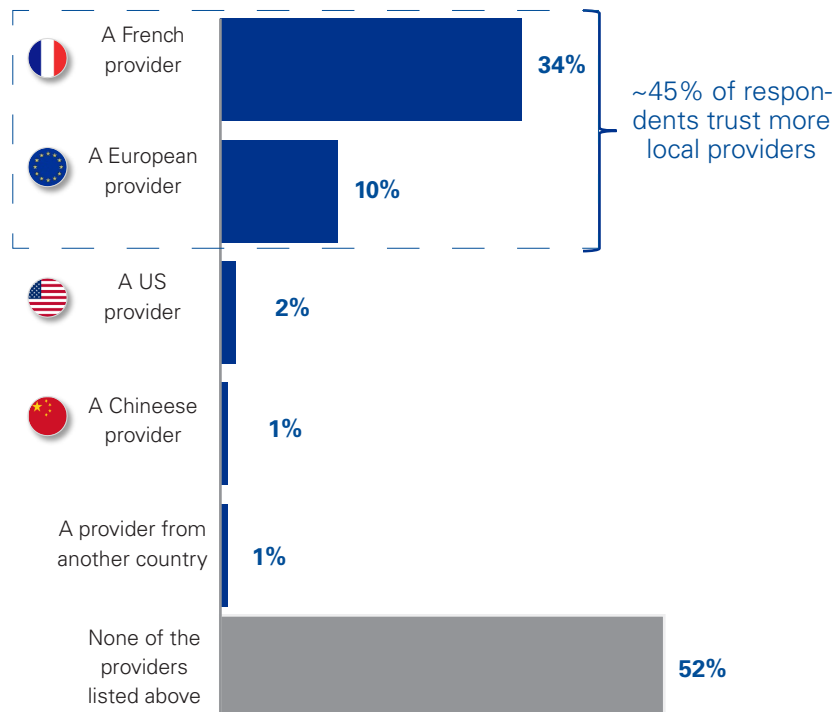
Data localization in EU	- Data is located in Data Centers in the European Union.
No access to data from non-adequate countries	- Service provider's data is technically not accessible from non-adequate countries (non GDPR compliant).
EU exclusive jurisdiction	- Service provider is exclusively subjected to EU jurisdiction and exempted from extraterritorial laws.
GDPR compliance regarding foreign authorities' requests	- Policy regarding responses to non-EU countries authority requests is appropriate and GDPR compliant.
Do not use client data	- Service provider is committed (in its Terms of Service) not to use client data, even to optimize its services.
Sovereign subcontractors	- Service provider's subcontractors have also to be sovereign , by meeting specific sovereign criteria.
European support	- Customer support has to be located in Europe.
Local law contracts	- Contract signed have to be subject to local laws.

In the coming years, data sovereignty will also raise as a commercial issue, as European consumers have growing expectations on this dimension

Respondents' concerns about their data sovereignty



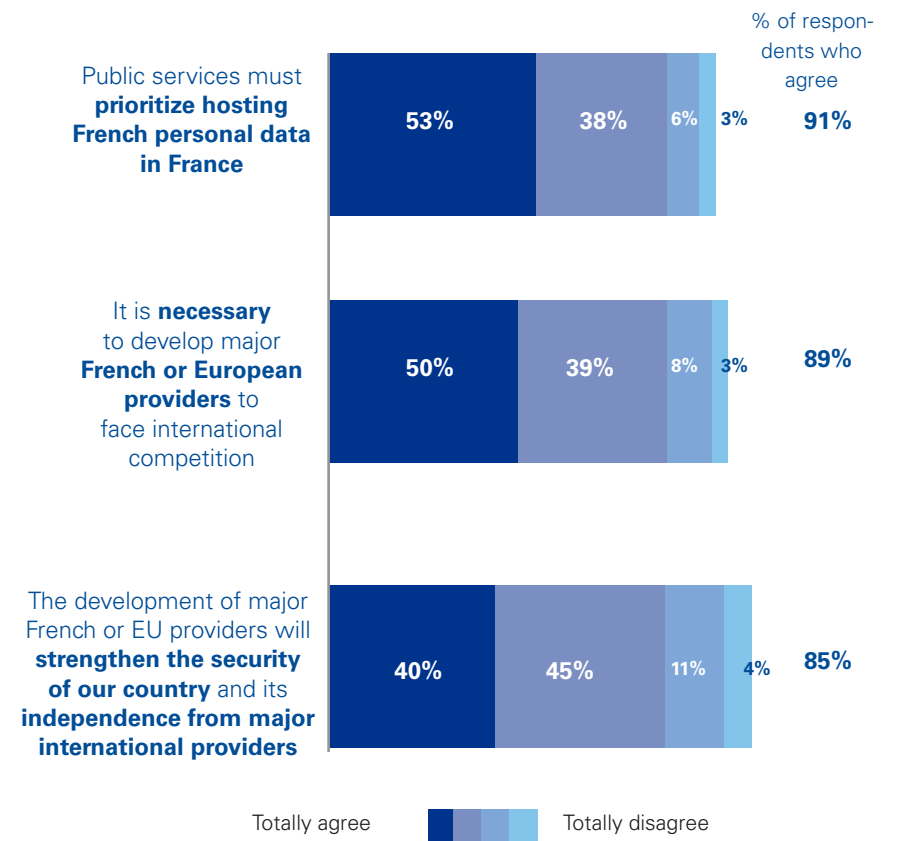
When it comes to the protection of your personal data, what provider would you trust more?



Respondents' expectations about their data sovereignty



To what extent do you agree / disagree with the following statement when it comes to data protection?

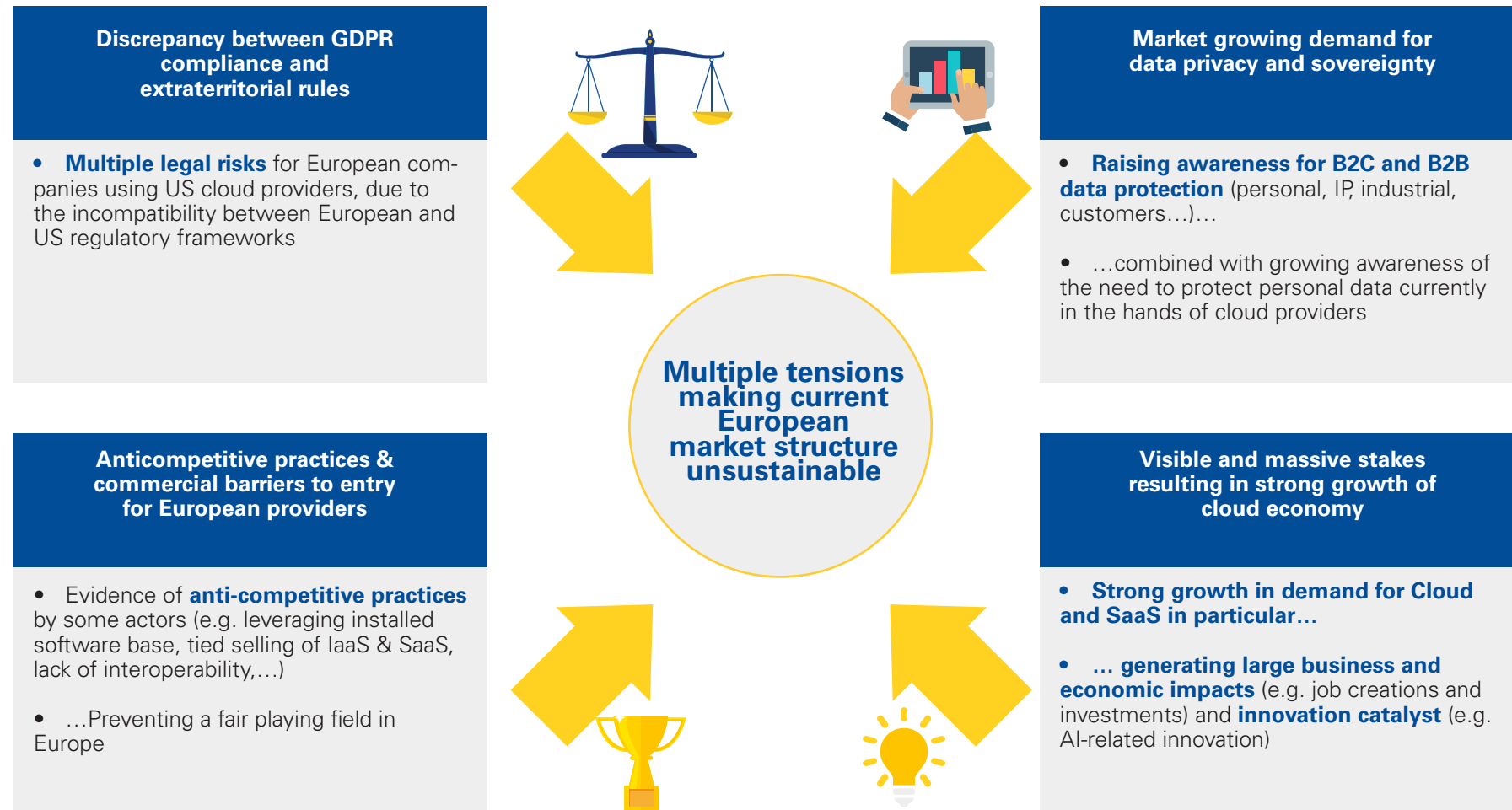


4

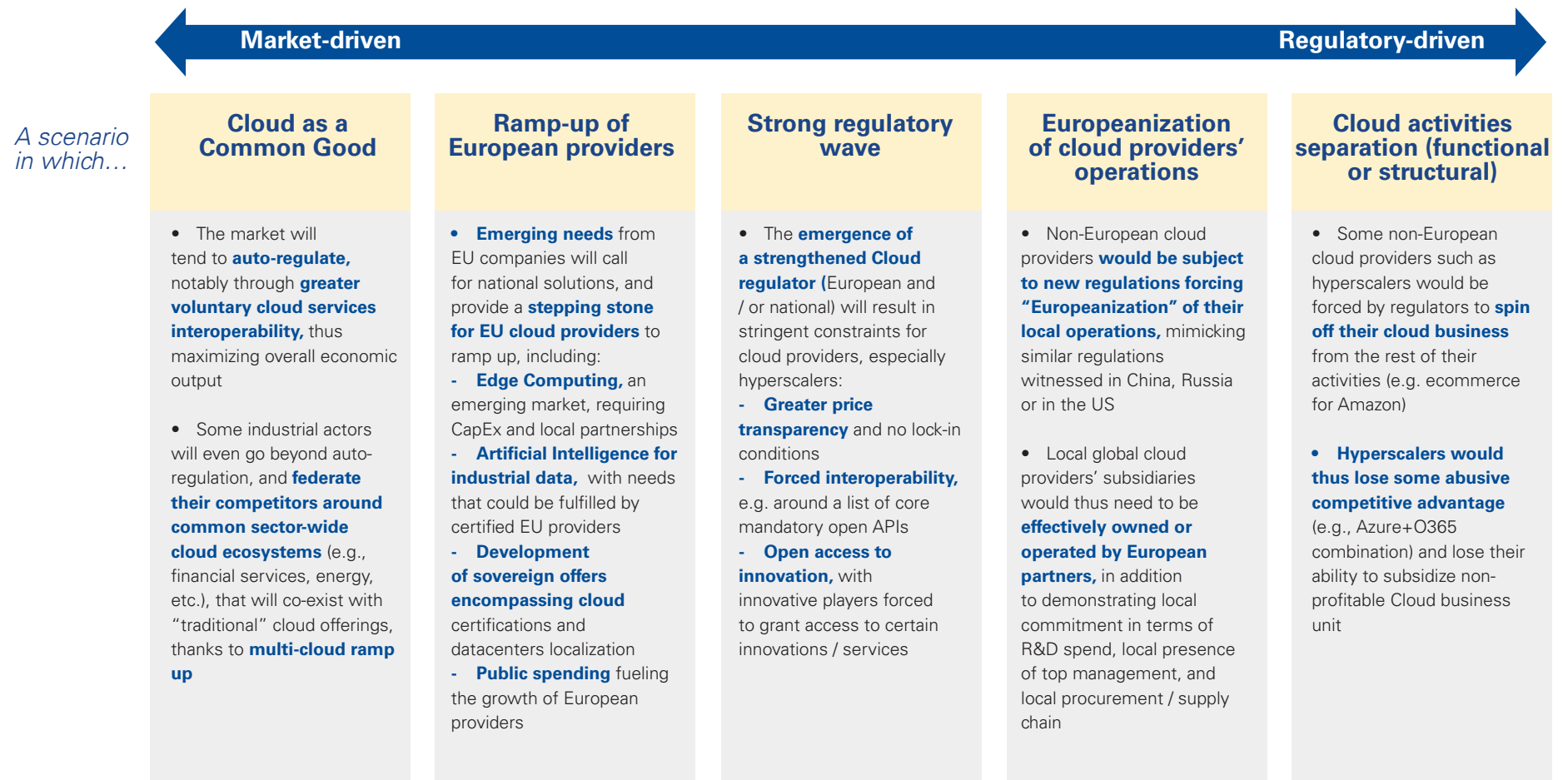


5 scenarios for
the future of the
European cloud
market

Current European market paradigm does not appear sustainable in the long run, due to four macro-trends

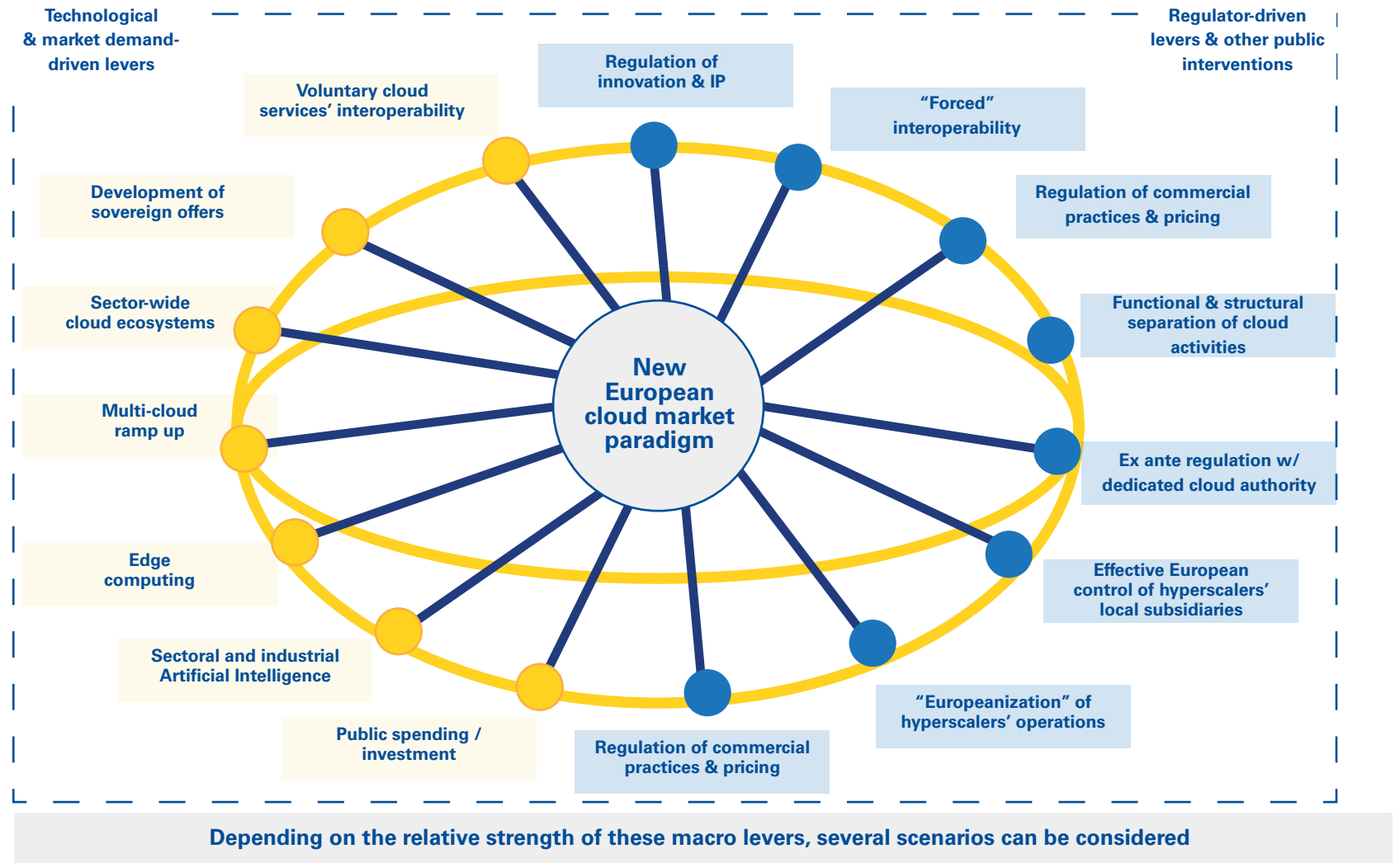


The European cloud computing landscape could therefore evolve into a number of potential scenarios...

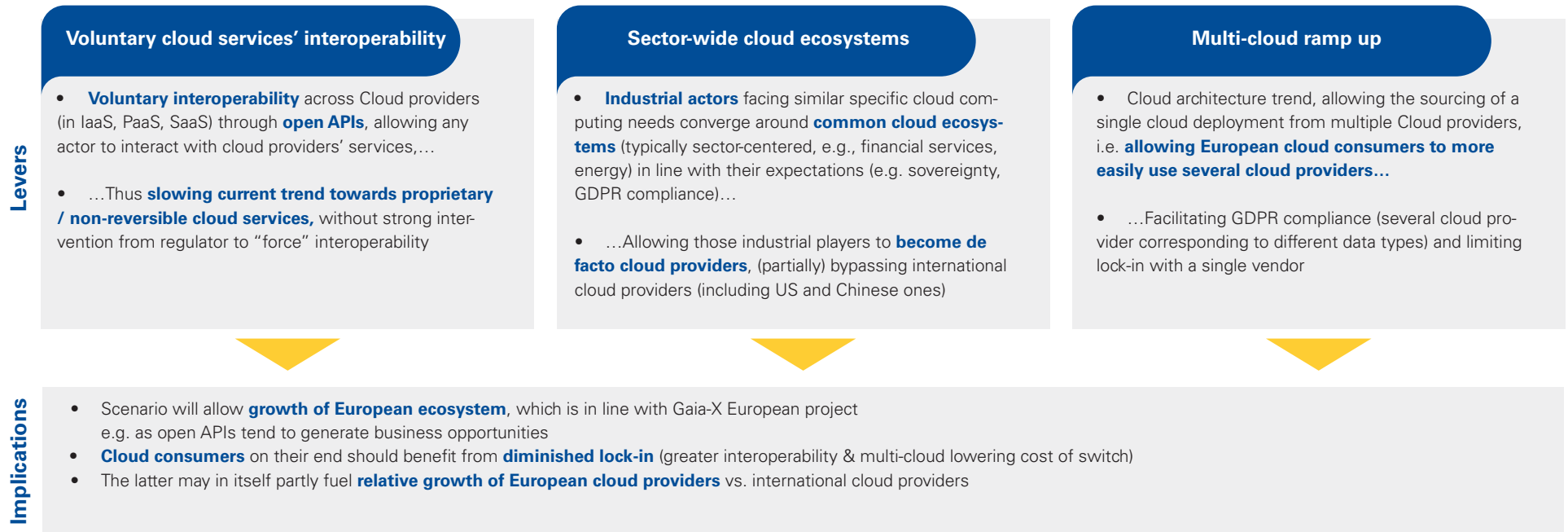


Scenarios are not fully exclusive and may be combined for compounded effect (e.g., accelerated ramp-up of European providers through enforced interoperability, Europeanization of chains of controls unbundled Cloud business, etc.)

These scenarios are characterized by a confluence of multiple macro levers, both market- and regulator-driven



Scenario 1 : Cloud as a Common Good



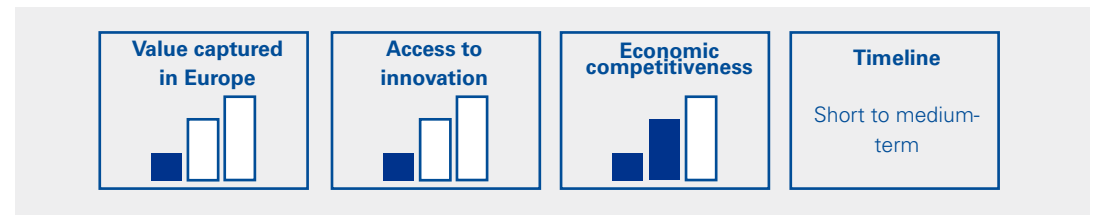
Role in the transition to the scenario



Key: ○ — Minor role — ● Major role

Scenario efficiency

and associated impact on economics metrics for Europeans



Key: ■ Limited impact ■ Strong impact

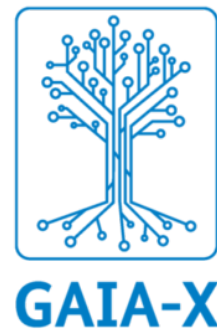
ILLUSTRATIVE

This scenario could materialize through Gaia-X European initiative, which aims to establish an interoperable data exchange protected by European laws



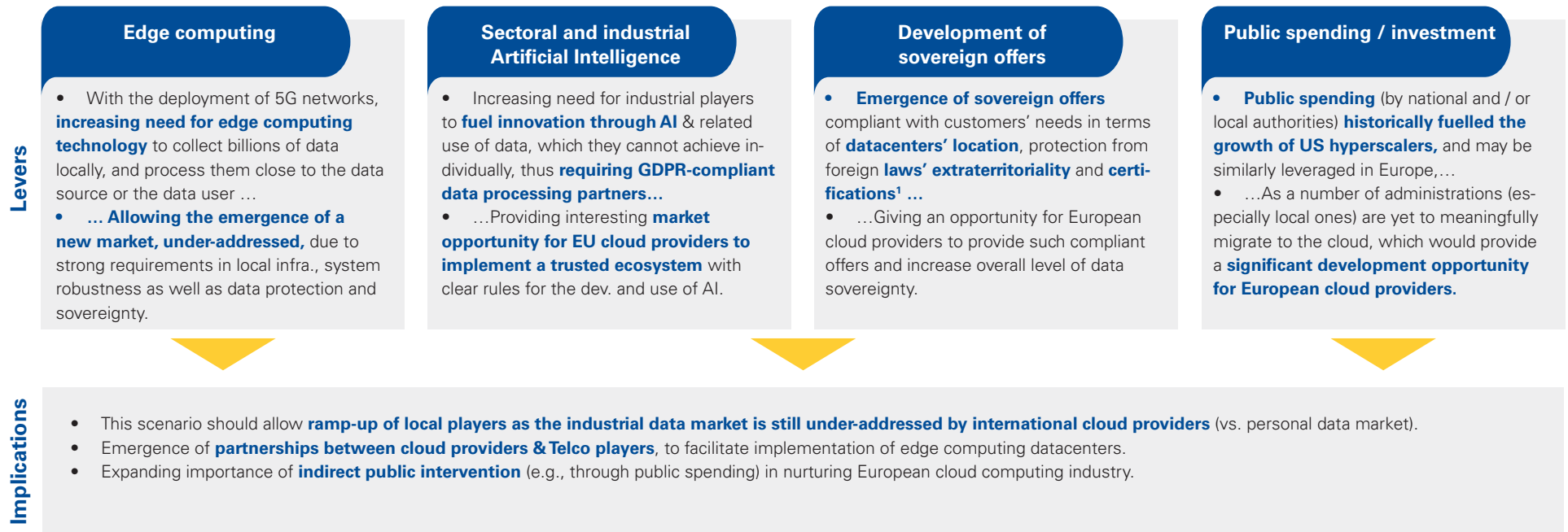
The Gaia-X association is a label to identify services compliant with **GAIA-X compliance label** ; this label will be awarded only to solutions that will satisfy criteria defined by the Board of Directors and based on the work of the Technical Committee and the Policy Rules Committee. Companies relying on a GAIA-X compliant service will be sure that the **solutions comply with European law**, that it offers **data portability**, the **highest criteria of data security**, a **clear transparency on data usage and applicable regulation**, the **guaranty of reversibility** and all **the relevant criteria which reflect the purpose of GAIA-X**. This trust mark can be awarded to both **members and non-members** of the GAIA-X association.

Any company or organization, including non-European players, **can join Gaia-X association**. **Members must respect the initiative set of principles and guiding policies, including the following ones:**



- European data protection:** compliance with the European legislation and ability to apply different levels of protection based on the type of data and use case.
- Open data infrastructure** that promotes transparency and standardized contracts and procedures, to reduce complexity and costs.
- Free market access** to make it easier for businesses across various industries to exchange data, thus stimulating cross-industry collaboration.
- Modularity and interoperability** permitted through the link up and the data integration from different cloud platforms, removing barriers to access and allowing smaller, specialist cloud services to compete.

Scenario 2: Ramp-up of European providers



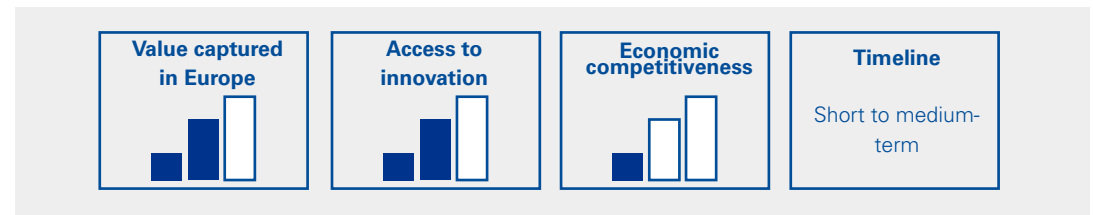
Role in the transition to the scenario



Key: ○ — Minor role — ● Major role

Scenario efficiency

and associated impact on economics metrics for Europeans



Key: ■ Limited impact ■ Strong impact

Note: (1). European Cybersecurity Certification Draft Scheme for Cloud Services by ENISA, incl. SecNumCloud in France or C5 German equivalent
Sources: Clients and experts' interviews; KPMG Avocats and GSG research and analysis

ILLUSTRATIVE

Ramp-up of European providers may happen more strongly in new markets, for which local secured cloud could be preferred to global cloud providers' solutions



Overview of market opportunities for the ramp-up of EU providers

Under-addressed markets...

... with specific needs ...

... that could be better addressed by EU providers

Edge computing

- Local datacenters with **high computing capacity** for local treatment of generated data
- Secure** and **sovereign** infrastructure adapted to **host industrial data**.

Artificial intelligence for industrial data

- High **computing capacity datacenters** capable of running **robust AI and ML algorithms**
- Secure** and **sovereign** cloud ecosystem required for critical industrial data.

Sovereign offers

- Sovereign, secure** and **certified cloud environments** allowing European companies to **migrate their critical data to the cloud**.

For European data (incl. critical industrial ones), EU providers could ensure **local and secure computing** and **storage capacities** within a sovereign environment

“We are starting a new phase with the rise of **industrial data**. Europe, as the most industrial continent, must position itself as a **leader in this field**. The **future of AI is inherently linked to the intense use of data**: there is no AI without data.”
T. Breton (Oct. 2020)

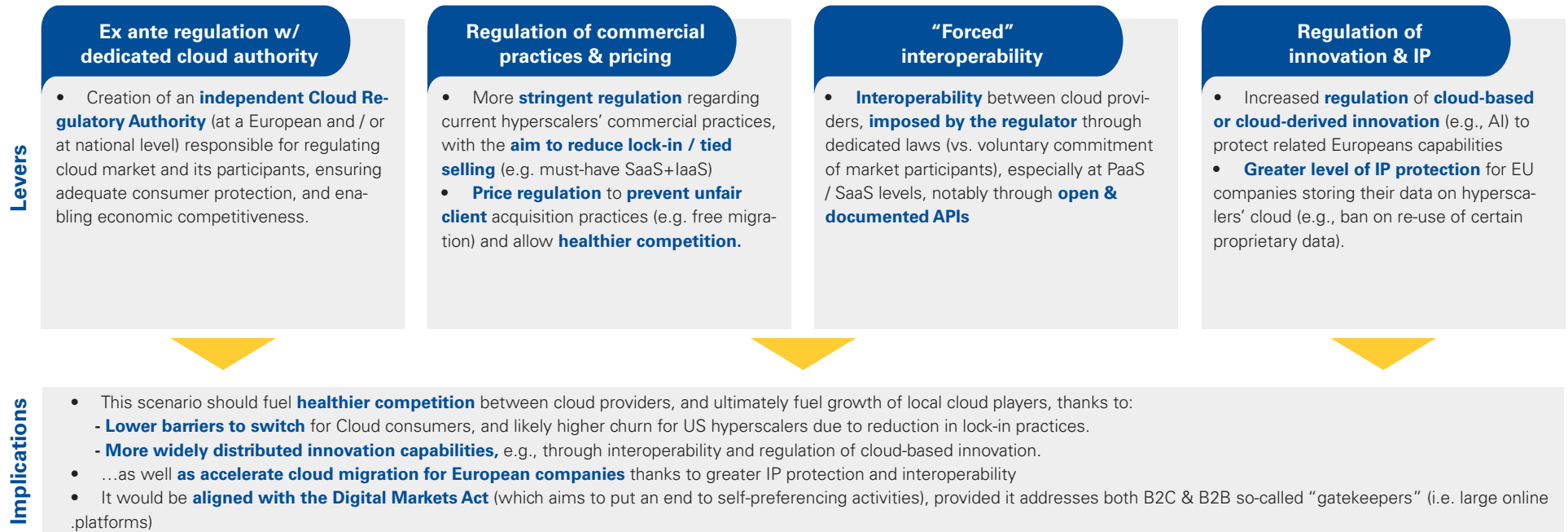
European Commission proposal

These market opportunities are reflected in the **European Commission's** goal to **create a Single Data Market**, with **European cloud providers** as the cornerstone of the project. The implementation of such a market may be facilitated by the following measures:

- Technological and financial support** to create a secure and sovereign European cloud infrastructure capable of **hosting and computing industrial data**.
- Creation of a **100% European** and sovereign **data manipulation value chain** through EU processors alliance.
- Development of self-regulatory norms and standards by industry stakeholders in Europe, namely **EU Cloud Rulebook, covering cybersecurity certification scheme, competitive fairness and code of conduct on energy efficiency of data centers**.
- Additional projects, such as the **Important Project of Common European Interest (IPCEI)**¹ on Next Generation Cloud Infrastructure and Services, should contribute to effectively foster European data leadership and sovereignty².

Notes: (1). Under IPCEI framework, EU Member States are able to set-up important projects of common European interest, that are based on authorized state aid and which include major contributions to growth, employment and competitiveness of the European industry (2). Project mentioned in particular in the Member States' Joint Declaration on Building the Next Generation Cloud in October, 2020
Sources: Clients and experts' interviews; KPMG Avocats and GSG research and analysis; Special Commission on « Artificial Intelligence in a Digital Age »

Scenario 3: strong regulatory wave



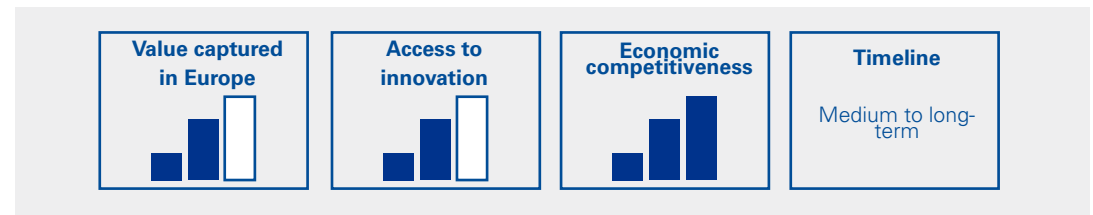
Role in the transition to the scenario



Key: ○ Minor role ● Major role

Scenario efficiency

and associated impact on economics metrics for Europeans



Key: [Limited impact bars] Limited impact [Strong impact bars] Strong impact

ILLUSTRATIVE

Germany is among the first EU countries to adopt new laws aligned with GDPR, and even goes further on some topics (incl. health data and digital competition)



German Digital Care Act aims to regulate health data usage, prohibiting their storage by US providers

A regulation dedicated to health data...

- In Germany, since 2020, digital health apps are governed by the **Digital Health Applications Regulation**

...generating specific rules regarding cloud computing

- Any health data collected by health apps **cannot be transferred outside the EU**
- Federal Institute for Drugs and Medical Devices **will not approve apps that store health data on any cloud service owned by a US company**, even with European branches and servers



10th amendment to the German Competition Act aims to create a “regulatory framework for digital competition”

An Act against Restraints of Competitions...

- In 2021, implementation of the **10th amendment to Act against Restraints of Competition** (Digital Competition Act), with the government's intension being to create a “regulatory framework for digital competition”

...aiming to strongly limit the market power of digital giants

- A novel regulatory approach targeting a limited number of **large «gatekeepers and intermediaries» in digital markets**
- Key principles:**
- The **German Federal Cartel Office** (FCO) can issue a declaratory order that a company's market position is of **«paramount cross-market significance»** – based on several factors (markets dominance, vertical integration, financial strength, access to data or other resources)
 - The FCO obtains **the power to impose ex-ante prohibitions for a number of listed practices** even on markets where the company is not dominant
 - The company bears the burden of proof to defend itself
- Type of conducts of such companies that the FCO may now prohibit:
 - **Self-preferencing** when providing access to supply and sales market (e.g. exclusive pre-installation offers)
 - **Impeding the interoperability** of products, services or data

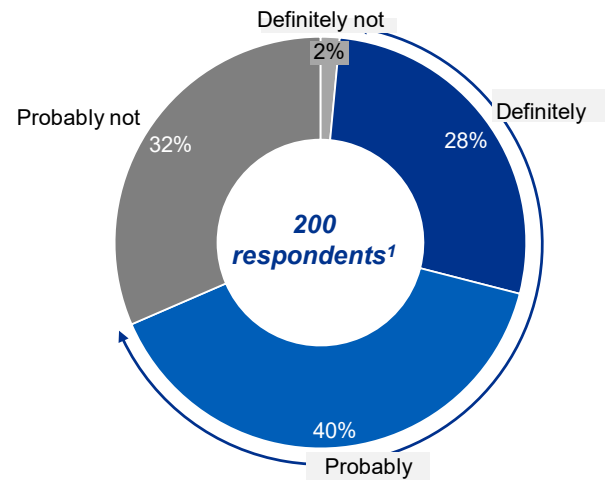
Survey results show an expected reinforcement of regulation by decision-makers, which could lead to a change of cloud providers in favor of European ones



European cloud computing decisionmakers' expectations regarding European regulations and their choice of cloud providers



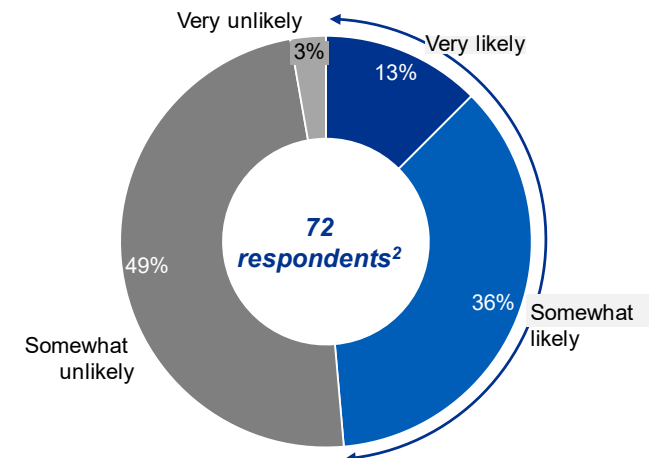
Do you expect a reinforcement of **European regulation** in the next 3-5 years?



68% of respondents expect a reinforcement of the European regulation in the near future



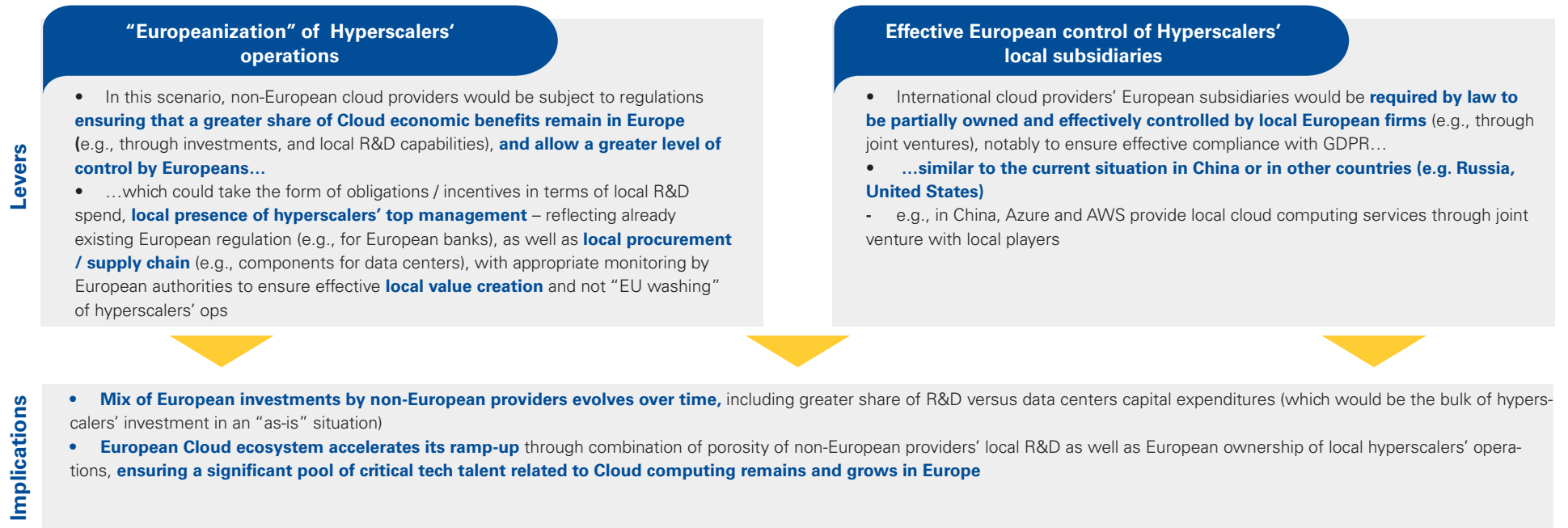
How likely or not is your company to **adjust its choice of cloud providers in favor of European ones** within the next 3 years, for legal and / or marketing reasons?



49% of respondents could favour a European cloud provider for legal or marketing reasons

Notes: (1). Based on GSG survey with 200 European CxOs respondents (2). Based on GSG survey with 72 European CMOs, CLOS, CEOs and COOs respondents
Sources: GSG Survey; GSG Analysis

Scenario 4: Europeanization of cloud providers' operations



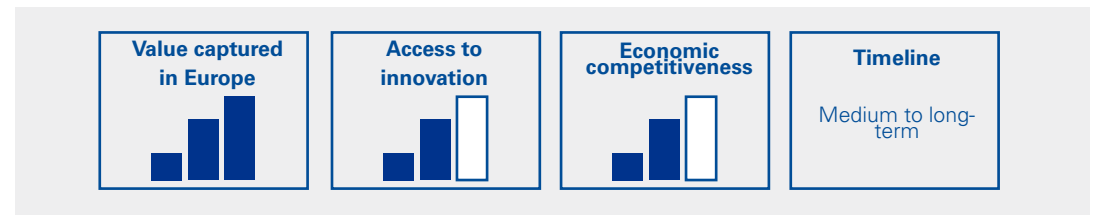
Role in the transition to the scenario



Key: ○ Minor role ● Major role

Scenario efficiency

and associated impact on economics metrics for Europeans



Key: [Limited impact bar] [Strong impact bar]

ILLUSTRATIVE

In some countries, such as China or the US, governments already imposed control by local players of part of foreign cloud providers' activities



China's Cybersecurity Law imposes foreign cloud providers to partner with local companies to serve Chinese customers

- **China's Cybersecurity Law**, approved in 2017 and gradually implemented and fleshed-out since then, imposes strong requirements to foreign cloud providers, including:



Data localization: All companies conducting business activities in China must store their data within Chinese borders.

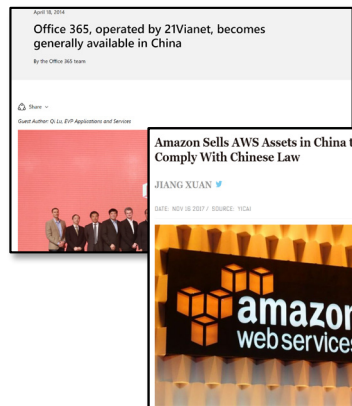


Internet Data Centers: Foreign-owned companies are not permitted to apply directly for IDC Licenses ; it is only allowed through JVs or partnership with Chinese local operators.

The US, concerned about data handled by foreign apps, has often considered divestments in favor of US companies

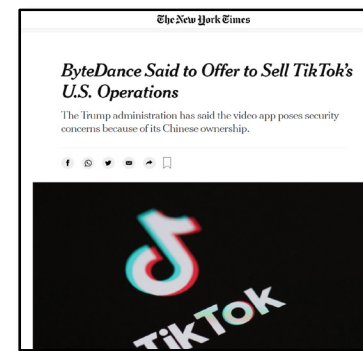
The US has been increasingly scrutinizing foreign apps over the personal data they handle, threatening them with sanctions or ban:

- In 2020, **Trump threatened to ban TikTok if it was not sold to a US player**, due to national security concerns over this app – ByteDance (TikTok Chinese owner) thus considered divesting its U.S. operation but the sale was consequently put on hold with the election of J. Biden as new president.
- In 2020, **Chinese gaming company Beijing Kunlun Tech sold Grindr**, a popular dating app it bought in 2016, after **being ordered** by the Committee on Foreign Investment in the United States (CFIUS) **to divest**.



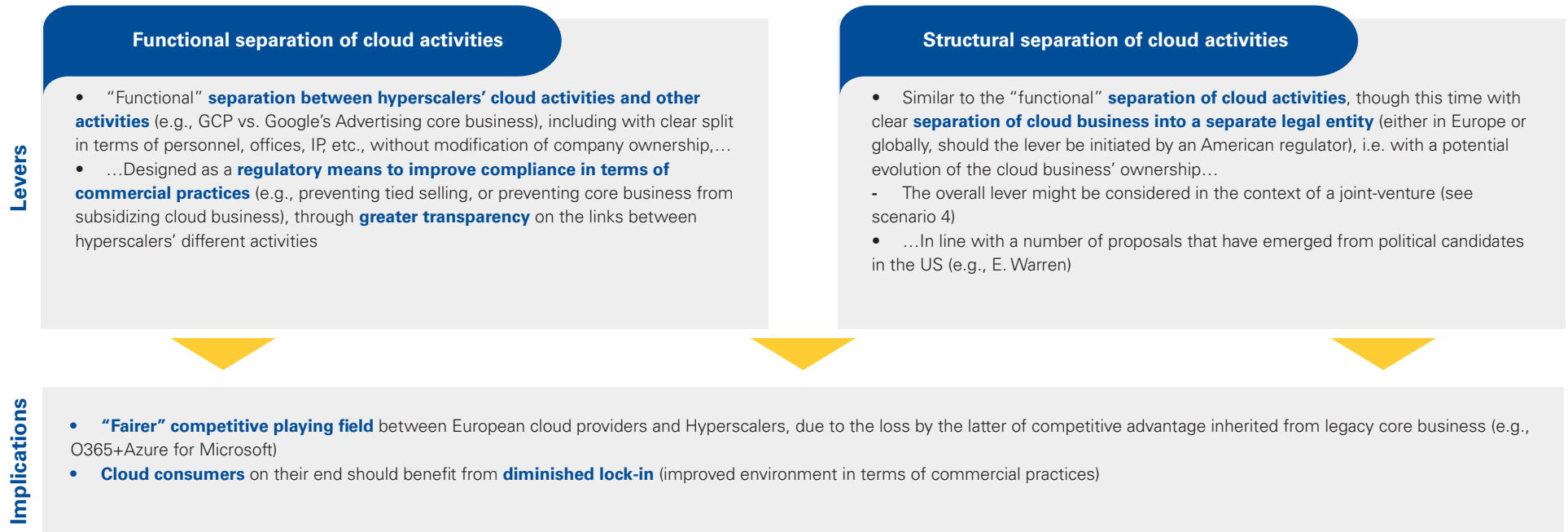
“As part of a strategic partnership agreement, **Microsoft will license its technologies to 21Vianet**, which becomes the official service provider of Microsoft Azure, Office 365 and Dynamics 365 in China.”

“In order to comply with Chinese law, **AWS sold certain physical infrastructure assets to Sinnet**”



“What's the right answer? Have an American company like Microsoft take over TikTok. Win-win. Keeps competition alive and data out of the hands of the Chinese Communist Party,” Republican Senator L. Graham

Scenario 5: Cloud activities separation (functional or structural)



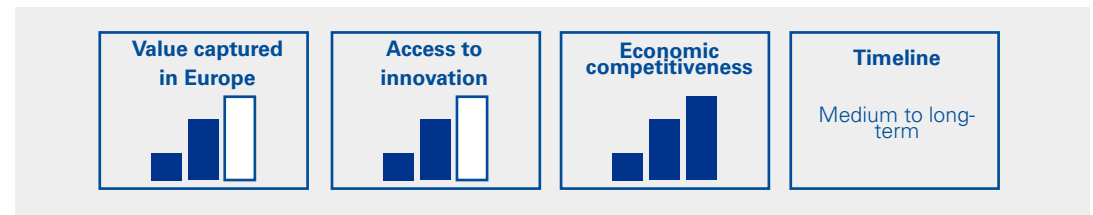
Role in the transition to the scenario



Key: ○ — Minor role — ● Major role

Scenario efficiency

and associated impact on economics metrics for Europeans



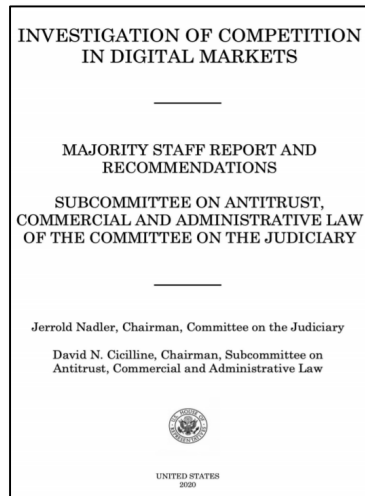
Key: ■ Limited impact ■ Strong impact

ILLUSTRATIVE

In the United States, the calls to break up Big Tech are getting louder and there is an increasing need to reduce their power over economy and society



U.S. House reports on competition in digital markets, with a focus on the need for antitrust reform...



Recommendations including:

- **Reduce conflicts of interest** through **structural separations** and **line of business restrictions**
- Promote innovation through **interoperability and open access** (data portability)
- **Reduce market power** through merger presumption

... are supported by an increasing share of politicians and citizens wishing to "Break them up"



"These companies would be **prohibited from owning** both the platform **utility and any participants** on that platform. Platform utilities would be required to meet a **standard of fair, reasonable, and nondiscriminatory dealing with users**. Platform utilities **would not be allowed to transfer or share data with third parties.**"
Senator E. Warren (March 2019)

"Slack simply **wants fair competition and a level playing field**. [...] Slack is asking the European Commission to take swift **action to ensure Microsoft cannot continue to illegally leverage its power from one market to another** by bundling or tying products." Extract from Slack's European Union antitrust complaint against Microsoft (July 2020)



What the federal government is doing is reasserting a fundamental rule for all business: You cannot simply buy **your way out of competition**," T. Wu, new White House adviser and outspoken advocate for aggressive antitrust enforcement against U.S. technology giants (March 2021)

As a conclusion, the future of the European cloud could be a combination of several scenarios, each with its own benefits, at different timescales

	Role in the transition to the scenario				Scenario efficiency and associated impact on economics metrics for Europeans				
	EU regul. & gov.	EU cloud prov.	EU indus. clients	Rationale	Value captured in Europe	Access to innovation	Economic competitiveness	Timeline	Rationale
#1. Cloud as a Common Good				<ul style="list-style-type: none"> Key role of cloud providers (incl. EU ones) to create an ecosystem in line with indus. needs (e.g. interoperable) 				Short to medium-term	<ul style="list-style-type: none"> Limited local value capture – (any provider can position on these offers) but with benefits in terms of overall EU competitiveness
#2. Ramp-up of European providers				<ul style="list-style-type: none"> EU providers would position on new under-addressed markets, where European industrials have strong requirements 				Short to medium-term	<ul style="list-style-type: none"> Value captured in Europe as industrials needs (AI, secured cloud) can only be met for the most part by EU providers
#3. Strong regulatory wave				<ul style="list-style-type: none"> Changes mainly driven by creation of reg. authority and implementation of ex ante regulation 				Medium to long-term	<ul style="list-style-type: none"> Market should open up to an healthier competition (no more lock-in, price regulated), with benefits in terms of competitiveness
#4. Europeanization of cloud service provider operations				<ul style="list-style-type: none"> Need for stricter regulation in Europe to improve control on data location (c.f. Chinese rules) 				Medium to long-term	<ul style="list-style-type: none"> Global cloud providers should comply with EU laws imposing local cloud activities, ensuring value creation stays in Europe
#5. Cloud activities separation				<ul style="list-style-type: none"> Functional or structural separation imposed by the European regulator to create a “fairer” competitive playing field 				Long-term	<ul style="list-style-type: none"> Structural changes should promote competition, ensuring better access to innovation and more EU value creation

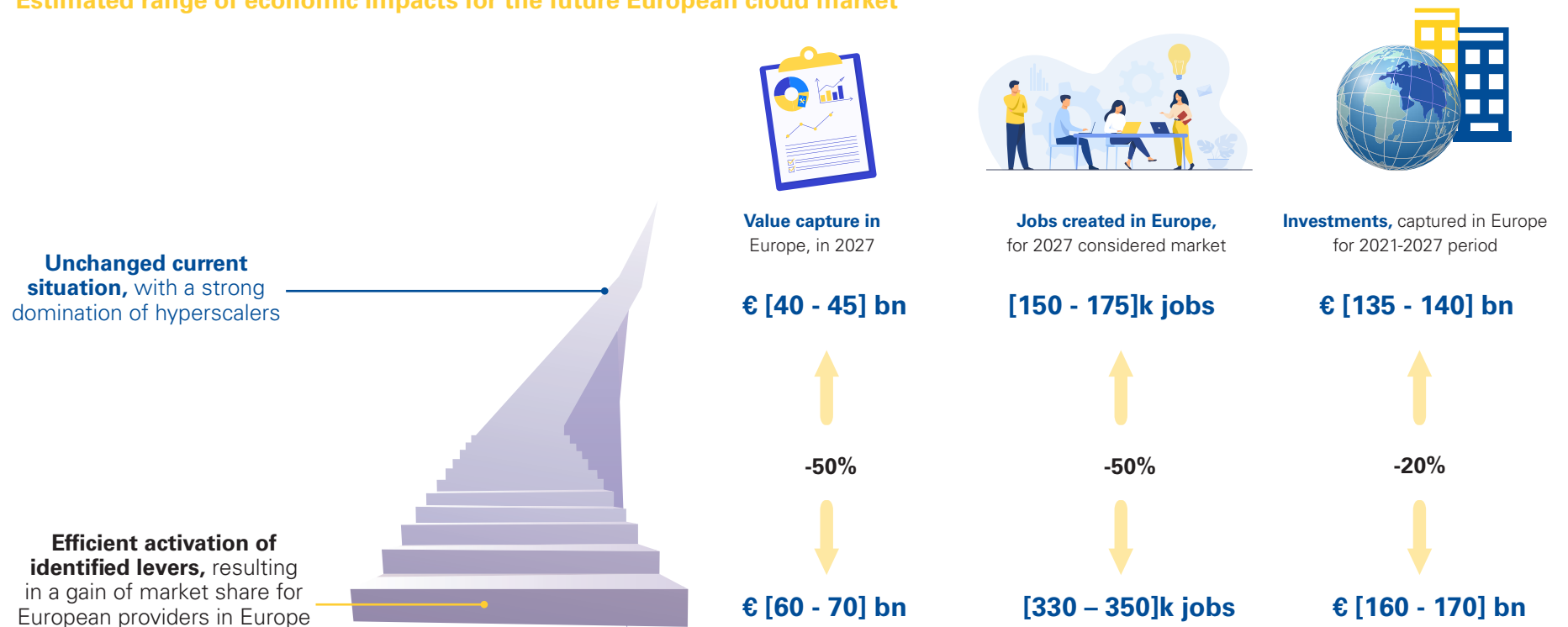
Key: Minor role Major role

Key: Limited impact Strong impact

HIGH LEVEL ESTIMATES

In case of insufficient activation of identified levers, Europe may lose from 20 to 50% of the estimated economic impact of cloud computing market

Estimated range of economic impacts for the future European cloud market



Economic impacts of cloud in Europe (incl. value captured, jobs created and investments) **will vary** in function of the actual scenario (potentially combined or not) or levers activated

5



Moving forward:
best practices
and initiatives for
private and public
stakeholders

These current challenges, and uncertainty regarding the future European cloud landscape, carry risks for key private sector stakeholders...

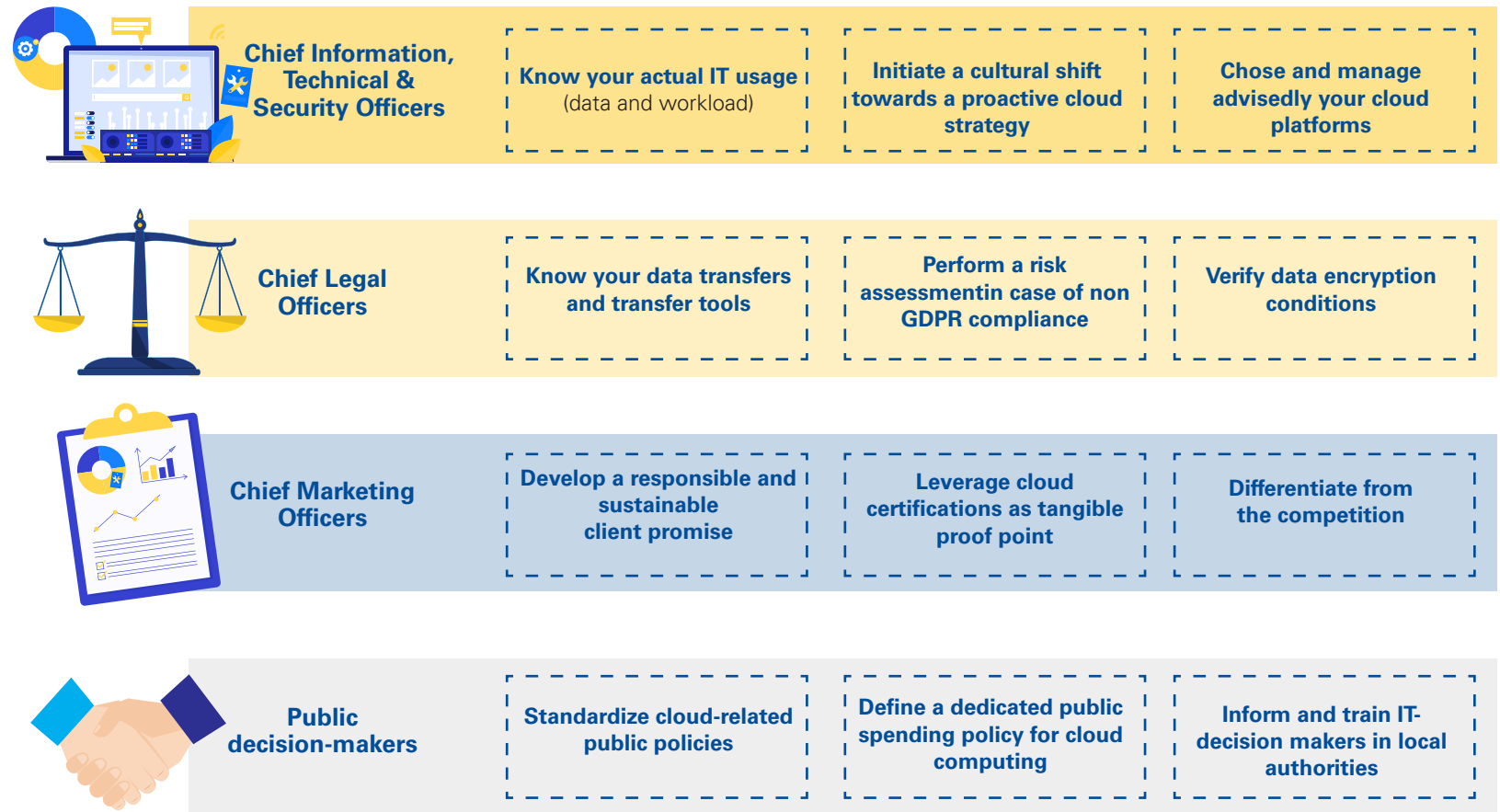
Uncertainty regarding the future European cloud landscape



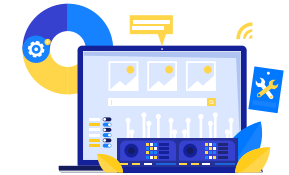
Potential repercussions fo key market stakeholders

- | | |
|--|---|
| For Chief Information, Technical & Security Officers | <p>Information & computer technologies related risks:</p> <ul style="list-style-type: none"> • Misalignment of IT and business strategies • Loud cost overruns, missing competitive advantage provided by the cloud • Lack of interoperability, vendor lock-in • Ineffective infra. configuration leading to security loophole |
| For Chief Legal Officers | <p>Legal and regulatory related risks:</p> <ul style="list-style-type: none"> • Non-compliance with GDPR rules • Being subject to extra territorial laws • Loosing control over strategic data |
| For Chief Marketing Officers | <p>Marketing and customer relations related risks:</p> <ul style="list-style-type: none"> • Not using state-of-the-art apps. (sales & marketing), leading to damaged customer experience / reputation erosion • Loss of customers |
| For Public decision-makers | <p>Public data management related risks:</p> <ul style="list-style-type: none"> • Management of sensitive data, with limited public financial means and support • Not taking advantage of the value created by data aggregation |

...which may be mitigated through a number of initiatives related to CIOs, CLOs, CMOs and public-decision makers



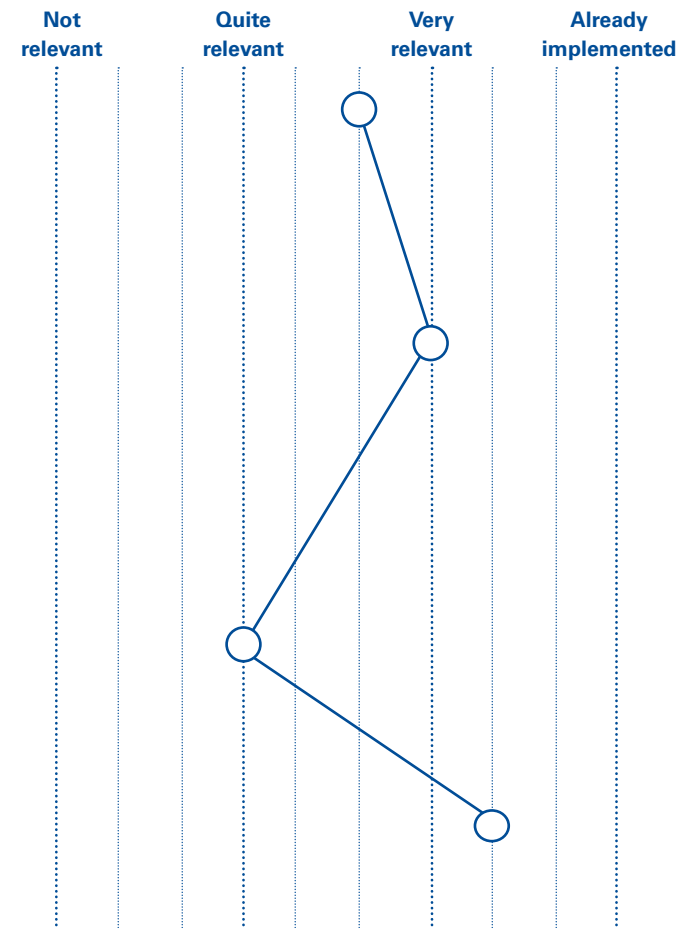
CIOs, CTOs and CISOs looking to unlock their cloud infrastructure potential should consider a number of best practices for a compliant & secure migration



Best practices and initiatives to be implemented by CIOs / CTOs / CISOs

Best practices	Initiatives
<p>Know your actual IT usage, incl. your data</p>	<ul style="list-style-type: none"> • Classify your data, by level of confidentiality (C1 to C4), with specific attention to personal and/or sensitive data • Set up the right governance all along the data lifecycle by level and type (e.g., storage location & duration, access & authorization, purpose)
<p>Know your actual IT usage, incl. your workload</p>	<ul style="list-style-type: none"> • Assess your workload, in close collaboration with business stakeholders), including: <ul style="list-style-type: none"> - Amount and type of computation (CPU, GPU, HPC)² needed - Scalability of workload (VM, container or not scalable at all) - Workload usage (frequency, by whom, duration, why, with which input data, for what output data)
<p>Initiate a cultural shift towards a proactive cloud strategy</p>	<ul style="list-style-type: none"> • Initiate several cultural shifts, at various level of the company: <ul style="list-style-type: none"> - At HR level, with a shift in sourcing (from manual and hardware related jobs into software development jobs) - At IT level, with the need to adopt a proactive security posture and cloud resilience in the infrastructure deployment
<p>Chose and manage advisedly your cloud platforms</p>	<ul style="list-style-type: none"> • Perform cloud providers' assessment (e.g., regarding crisis situation SLA, data sovereignty, data transfers & access guarantees) and consider a multicloud strategy to avoid a future potential lock-in situation • Leverage best practices from software development to treat your infrastructure as code (Devops, CI/CD)

Overview of initiatives relevance¹



Notes: (1) based on GSG survey with 76 European CIOs answering to the following question :“ How relevant would it be for your company to implement any of these actions?” (2). CPU: Central Processing Unit, GPU: Graphics Processing Unit, HPC: High-Performance Computing
Sources: Experts' interviews; GSG survey; GSG Analysis

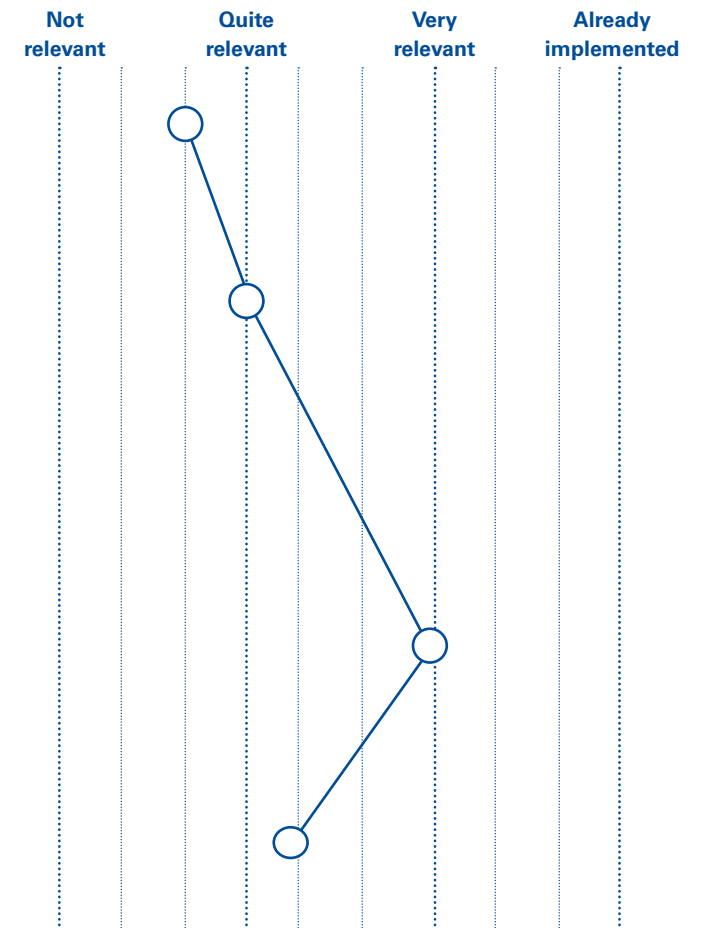
To be aligned with the changing and complex data regulation, CLOs should map data transfers, assess data repatriation and perform a risk assessment



Best practices and initiatives to be implemented² by CLOs

Best practices	Initiatives
<p>Map out your data transfers</p>	<ul style="list-style-type: none"> • Identify services providers established outside the EU or likely to carry out transfers outside the EU (processes most at risk) • Identify processing of personal data entrusted to these providers and the legal basis associated (consent, legitimate interest, etc.)
<p>Assess your transfer tools</p>	<ul style="list-style-type: none"> • Identify the transfer tools you are relying on (adequacy decisions, binding corporate rules, codes of conduct, ad hoc contractual clauses, certification mechanisms, etc.) • Analyze local legislations to assess whether the GDPR transfer tool you are relying on is effective in all circumstances
<p>Perform risk assessment in case of non-GDPR compliance</p>	<ul style="list-style-type: none"> • In case of non-compliant transfers or tools, assess the associated risk (authorized or prohibited uses cases) and the need for supplementary measures <ul style="list-style-type: none"> - Authorized use cases: reinforce your contract (e.g., data protection clauses, binding corporate rules, contractual clauses) - Prohibited use cases (most common): repatriate your data in a GDPR-compliant country (incl. assessments regarding costs, time required and operation restraints) • Re-perform at appropriate intervals this risk assessment
<p>Verify data encryption conditions</p>	<ul style="list-style-type: none"> • Assess data encryption conditions (often perceived as the quick and efficient way to become GDPR-compliant), incl. modalities, relevance, effectiveness and volume of data encrypted

Overview of initiatives relevance¹



Notes: (1) based on GSG survey with 124 European CxOs answering to the following question : " How relevant would it be for your company to implement any of these actions?" (2) based on the recommendations of the European Data Protection Board
Sources: Experts' interviews; GSG survey; GSG Analysis

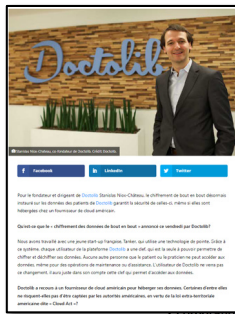
ILLUSTRATIVE

Beyond regulatory compliance, data encryption can ensure data sovereignty, but only under very strict (and often non-respected) implementation criteria



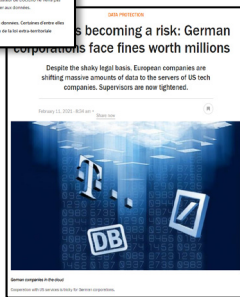
While data encryption is one of the most effective mechanisms for protecting data access...

- Key Management Service (KMS) and other encryption methods (e.g. asymmetric algorithms) **protect the data from external breaches and malicious acts**, in addition to the robust security layers provided by cloud technologies and infrastructure



“The protection of our user’s personal data is our first duty. Today’s decision to generalize end-to-end encryption on Doctolib is the best example of this. As long as you encrypt the data with encryption keys from a trusted third party, the hosting provider is of little importance.”

Doctolib CEO



“Deutsche Bahn has built a very comprehensive encryption concept according to the state of the art, allowing a full protection of our data on the cloud.”

Deutsche Bahn spokesperson

... proper implementation should be carried out to ensure protection from foreign regulations’ extraterritoriality

Key factors to take into consideration for data encryption



Insure an **independent storage of encryption keys by a third party** (i.e. different providers for cloud services and KMS), as KMS offered by cloud providers can ensure data security but usually does not guarantee data sovereignty



Assign the implementation of **encryption methods to highly skilled specialists and dedicated teams**



Manage data encryption as a **complex project** with a thorough **deployment roadmap**, taking into account the **specificities of the company’s current IT system** and the **potential high incurred costs**

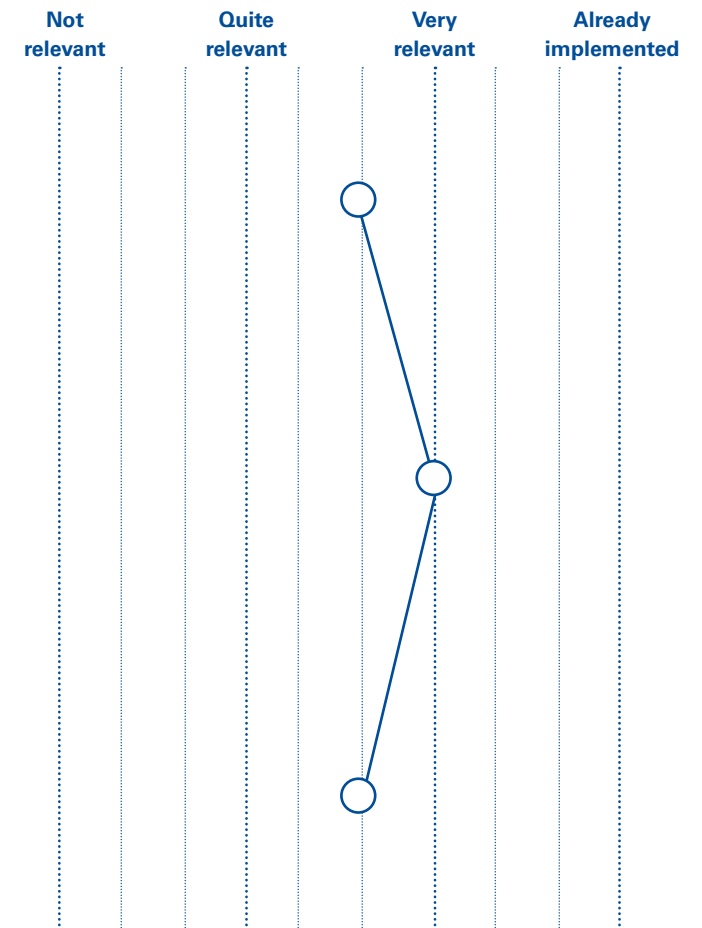
CMOs also have a role to play, aligning their customer value proposition with IT choices in terms of data protection & sovereignty



Best practices and initiatives to be implemented by stakeholders – CMOs

Best practices	Initiatives
<p>Develop a responsible and sustainable client promise in terms of data protection</p>	<ul style="list-style-type: none"> • Acknowledge the growing importance of data privacy, protection and sovereignty for customers and the business risks associated if they are not taken into account (e.g. client churn) • Make sure that the company's cloud policy choices reflect this importance (e.g., sovereignty criterion in selecting a cloud provider, adequate processes in place...) • Tie company's data protection choices to overall value proposition, demonstrating to clients and prospective clients how much the company values their data,... • ...With greater chance to avoid potential brand damage, e.g., in case of personal data leak outside Europe
<p>Leverage cloud certifications as tangible proof point</p>	<ul style="list-style-type: none"> • As a way to prove the company's commitment, ensure the company selects providers with relevant certifications,... • ...and display those certifications as proof point that the company is taking the topic of data protection and sovereignty seriously
<p>Differentiate from the competition</p>	<ul style="list-style-type: none"> • Ensuring effective GDPR compliance – e.g., by contracting with a European Cloud provider – is a way to differentiate from the competition, thus reinforcing the customer value proposition • Communicate about the company's cloud policy choices and use it as a sales argument • Identify state-of-the-art cloud-native applications for marketing (e.g. marketing campaign management) and sales (e.g. CRM)

Overview of initiatives relevance¹



Notes: (1) based on GSG survey with 124 European CxOs answering to the following question : " How relevant would it be for your company to implement any of these actions?"

Public-decision makers can support local communities digitization, esp. through cloud policies standardization and financial support of cloud-related initiatives



Best practices and initiatives to be implemented by public-decision makers¹

Best practices	Initiatives
<p>Standardize Cloud-related public policies of data protection</p>	<ul style="list-style-type: none"> • Define guidelines for cloud-related policies at national and local levels, and elaborate an associated roadmap, in order to: <ul style="list-style-type: none"> - Support local public decision makers in the identification of sensitive data by providing concrete examples (e.g. health data, personal HR data, etc.) - Mutualize local needs regarding cloud migration at local level, to limit costs and ensure a consistent approach
<p>Define a dedicated public spending policy for cloud computing</p>	<ul style="list-style-type: none"> • Allocate massive and long-term public spending to support the ramp-up of European cloud providers (e.g. migrate all digitized public archived to European cloud providers)
<p>Inform and train IT-decision makers in local authorities</p>	<ul style="list-style-type: none"> • Inform local / decentralized IT-decision makers on sovereign and local options for cloud migration with European cloud providers to: <ul style="list-style-type: none"> - Limit concerns related to cloud migration - Ensure local / European cloud migration, on sovereign public clouds • Train local IT-decision makers regarding the need to classify their data and to initiate cloud migration on non-sensitive ones (for cost, security and flexibility reasons)

Example: smart cities and public data

- **Data** is one of the major **prerequisite for the emergence of smart cities**, where it is important to clarify:
 - **who owns** the data generated
 - **who can** access to it
- Smart cities main challenge is their ability to **cross-reference data from different sources**: various networks (water, gas, electric), connected devices (IoT) within street furniture, ... – in this context, **data governance is key**
- **Open data and cloud computing**, if well understood, could be considered as enablers



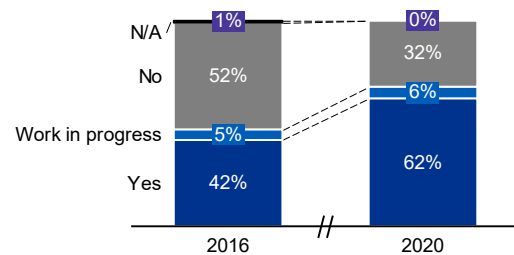
Note: (1) for example, local and regional authorities
Sources: Experts' interviews; GSG research and analysis

The relatively slow pace of Cloud adoption by local authorities, underpinned by legal & tax matters, points to greater potential for local Cloud providers and edge computing more broadly

A still slow pace of adoption...

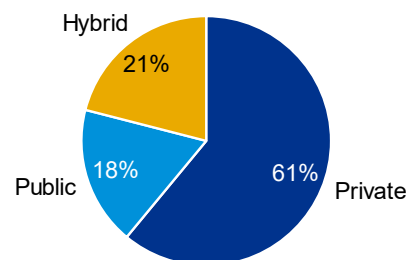
Use of (at least 1) Cloud services by local / regional authorities in France

- 2016-2020, % -



Split of Cloud services used by local / regional authorities in France

- 2020, % -



...Due to various barriers...

- Previous **legal barriers** preventing hosting of public data on data centers located outside French territory, only recently¹ lifted
- Local / regional authorities' preference for investment in own data centers vs. IaaS, due to:
 - **Data sensitivity** (e.g., citizens data)
 - **Long time horizon of authorities**, increasing relevance of investment vs. cloud rental

"Our current accounting organization favors capital budgets (CapEx) rather than operating ones (OpEx);"

Head of the Technical Infrastructure Department of a French public authority

- While IaaS use has been very limited, **SaaS use has become widespread** for apps outside their core missions

...To be addressed by Cloud players

- While local authorities will likely keep a proportion of their infrastructure on-premise, the **lifting of legal barriers** naturally creates an **opportunity for Cloud players to capture a greater share** vs. on-premise
- Data sensitivity will also likely remain a strong issue, to be partially alleviated through the use of **local Cloud providers**, which may be deemed more trustworthy by local authorities
- Local authorities may however still want to explore **investment in own local cloud facilities to be mutualized across several local authorities**
- These elements are in line with the **recent French administrative cloud strategy (March 2021)**, which underlines the importance of data security and sovereignty, the importance of choosing competent cloud providers, and the need for the state to support the cloud sector

Note: (1) French initial "Sovereign Cloud" strategy, lifted through November 2018 Cloud doctrine incentivizing use of Cloud solutions by local / regional authorities and 2019 Code du Patrimoine amendments allowing hosting of certain types of public data / archives in data centers located outside French territory
Sources: "MIPS 2020 collectivités territoriales" survey, Experts' interviews, GSG research and analysis

6



Appendix -chapitre 1

Abbreviations and used terminology

Terminology	Definition
API	Application Programming Interface: a technology allowing communication between different software.
Baremetal cloud	Physical servers dedicated to individual tenants, with high stability and computing performance.
BYOL	Bring Your Own License: a practice allowing SaaS applications to run on cloud environments other than that of the SaaS provider.
Cloud computing	Hosting data and applications in physical servers, accessible through the internet.
Container management	Technology allowing the packing of applications and their dependencies as a single block facilitating future migrations to other environments.
CRM	Customer Relationship Management: a software dedicated to the management of relationships and interactions with customers
ERP	Enterprise Resource Planning: a software dedicated to the management of the companies' main business processes (e.g. procurement, distribution, accounting, human resources).
Hosted private cloud	Private infrastructure hosted and managed by the cloud provider.
Hybrid cloud	The coordination of cloud services across public and private cloud service providers to create another cloud environment.
IaaS	Infrastructure as a Service: cloud computing servicing model based on renting access to storage and computing capacity on physical servers.
IOT	Internet Of Things: physical objects connected to the internet through embedded sensors.
PaaS	Platform as a Service: cloud computing servicing model based on renting access to platforms for software development.
Private cloud	Cloud environments dedicated to one customer / owner with fully isolated access.
Public cloud	Cloud environments within servers owned by cloud provider and shared between different customers / companies.
SaaS	Software as a Service: cloud computing servicing model based on renting access to internet-based application (with underlying platforms and infrastructure).
Virtual Networking	Technology allowing the construction of a complex private infrastructure by connecting multiple private secure networks.
Virtual private server	Virtual servers used for hosting websites and applications with data stored on user-dedicated virtual machines.

Abbreviations and used terminology – Gartner Hype cycle curve (1/2)

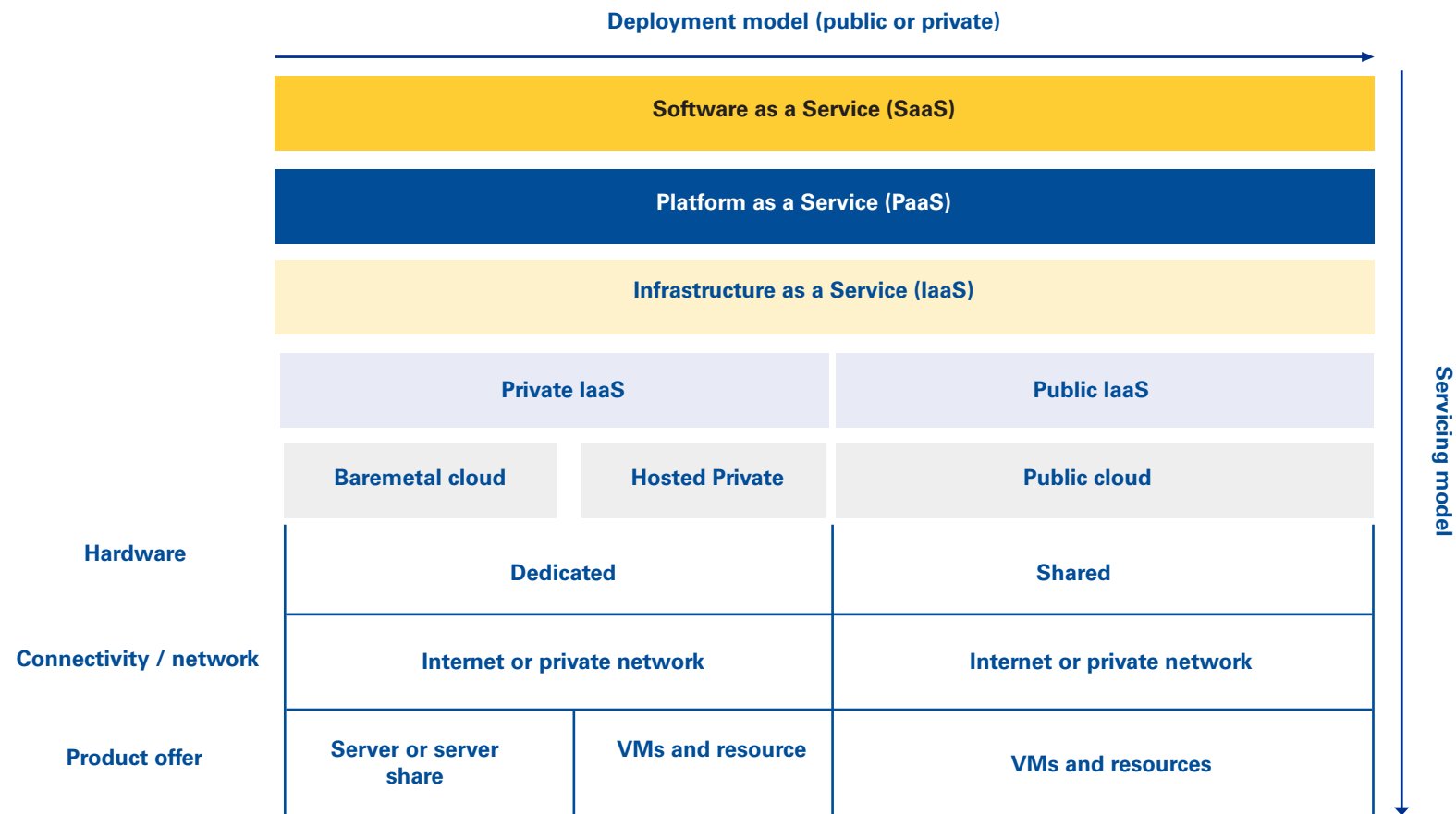
Terminology	Definition
API Gateway	API centralization platform in charge of routing calls to the appropriate microservice with request routing, composition, and protocol translation.
Application PaaS	A set of blockchain software platform services offered in the cloud by a vendor, for subscribers.
Blockchain PaaS	Cloud platform service that offers application development and deployment environments.
Cloud management platforms	Platform that enables organizations to manage private, public, multicloud services and resources.
Cloud marketplaces	Online storefronts through which customers can find and subscribe to cloud service offerings, including IaaS, PaaS and SaaS.
Cloud migration	The process of planning and executing the movements of applications or workloads from on-premises infrastructure to external cloud services, or between different external cloud services.
Cloud Networking	A service offered by service providers to connect disaggregated hybrid IT cloud environments, providing a robust interconnectivity between external cloud data centers and customer's on-premises data centers.
Cloud office	Collection of the most broadly used suites of SaaS-based personal productivity, horizontal collaboration and communication tools (e.g. emails, file sharing, document management and editing).
Cloud Security assessment	Formal security assessments performed by independent evaluators.
Cloud Tethering	An application delivery model in which a device-based application is linked to the provider's cloud service for licensing.
Cloud to Edge Development Support	Describes the extension of cloud providers' programming models and use on edge devices, such as IoT «things».
Cloudbursting	The use of an alternative set of public or private cloud services as a way to augment and handle peaks in IT system requirements at startup or during runtime.
Cloud-testing tools & services	Cloud technology to support testing from or in the cloud (incl. Cloud-based lab management, service virtualization, on-demand-delivered testing tools and device clouds).

Abbreviations and used terminology – Gartner Hype cycle curve (2/2)

Terminology	Definition
Container Management services	API centralization platform in charge of routing calls to the appropriate microservice with request routing, composition, and protocol translation.
Edge Computing	A distributed computing topology where information processing is placed close to the things or people that produce / consume that information.
Expense management	The practice of reviewing and reconciling the charges for services provided by cloud service providers through a monitoring tool.
Hyperscale Computing	A set of architectural patterns for delivering scale-out IT capabilities at massive, industrialized scale.
Immutable Infrastructure	An architectural pattern in which the system and application infrastructure, once instantiated, is never updated in-place.
IOT Platform	A software that enables development, deployment and management of solutions that connect to and capture data from IoT endpoints.
Machine Learning	A discipline that aims to solve business problems utilizing mathematical models that can extract knowledge and pattern from data.
Multicloud	Use of cloud services from multiple public cloud providers for the same purpose.
Private PaaS	A type of PaaS that offers exclusive access to customer organization. Private PaaS may be established on-premises or hosted on a public IaaS by the customer organization (self-managed).
Public Cloud Storage	IaaS that provides block, file and /or object storage services delivered through various protocols.
SaaS Administrative ERP	Administrative ERP focusing on financial management, human capital management HCM and indirect procurement. (Does not include remote hosting, where ownership remains with the customer, or private cloud).
Serverless PaaS	PaaS delivered with serverless characteristics. Serverless is a way of delivering an IT service where the underlying resources are opaque, require no provisioning, and are micropriced.
Software-defined infrastructure	Encompasses a broad set of software-defined infrastructure components (e.g. Software-defined data center SDDC IP, SD edge of edge-based adapters / monitors / gateways / appliances and machines).

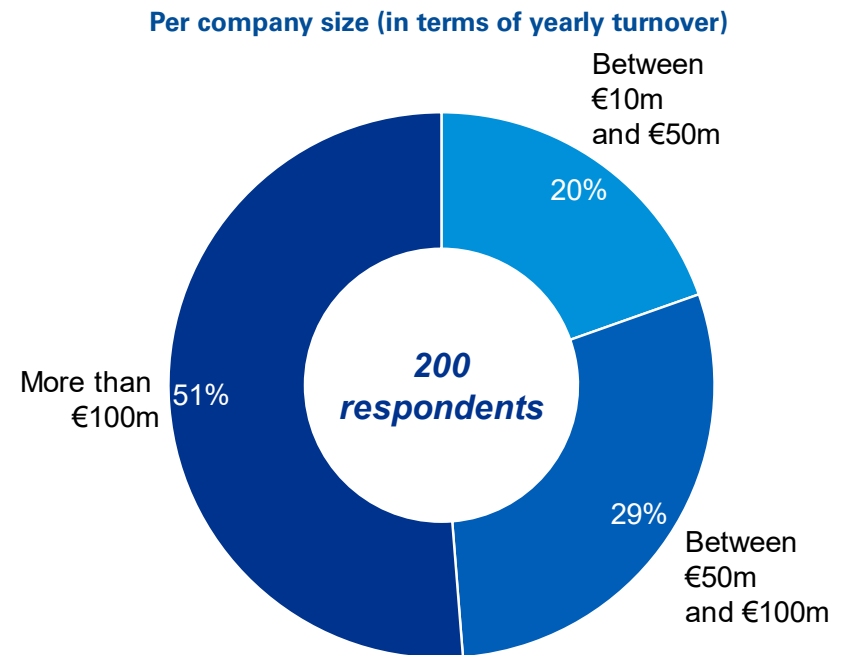
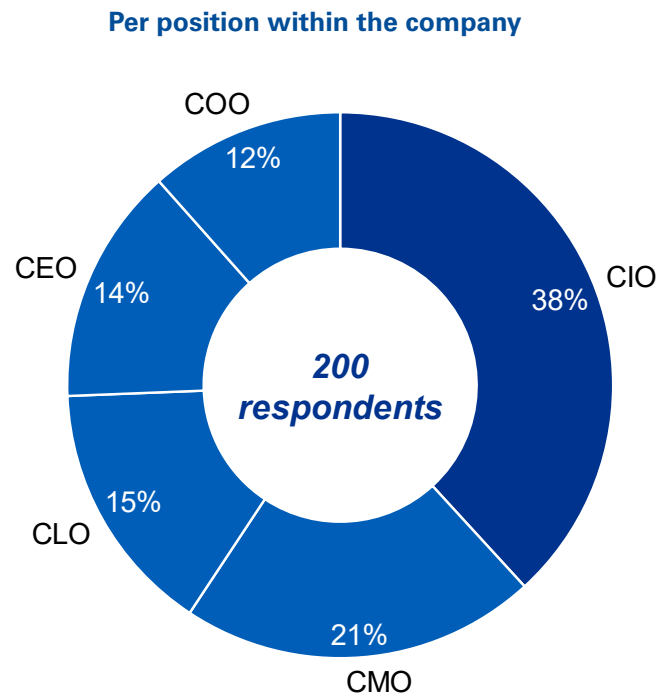
Cloud offers available on the market can be differentiated according to two distinct dimensions, deployment and servicing models

Primary characteristics of the cloud



Through the conducted survey, we collected 200 answers, with a fairly balanced pool of respondents representing several sizes of companies...

Profile of survey's respondents



Among which



50% of French respondents

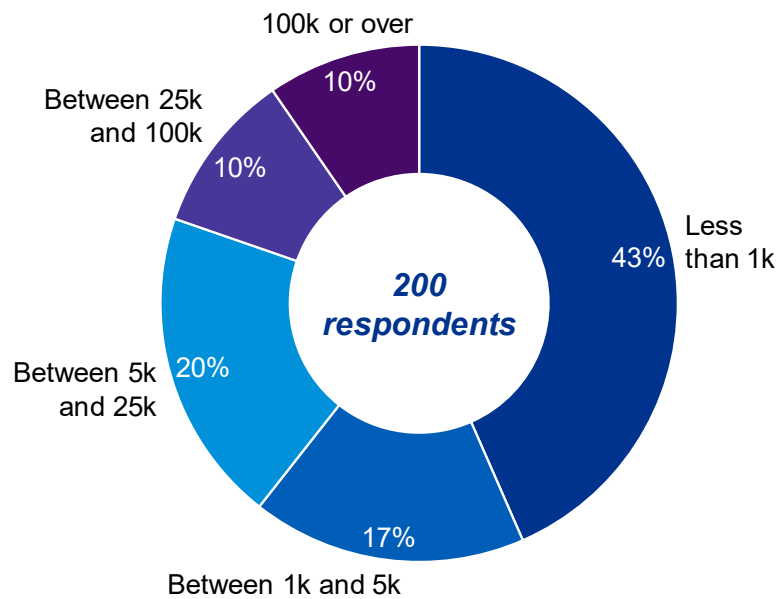


50% of German respondents

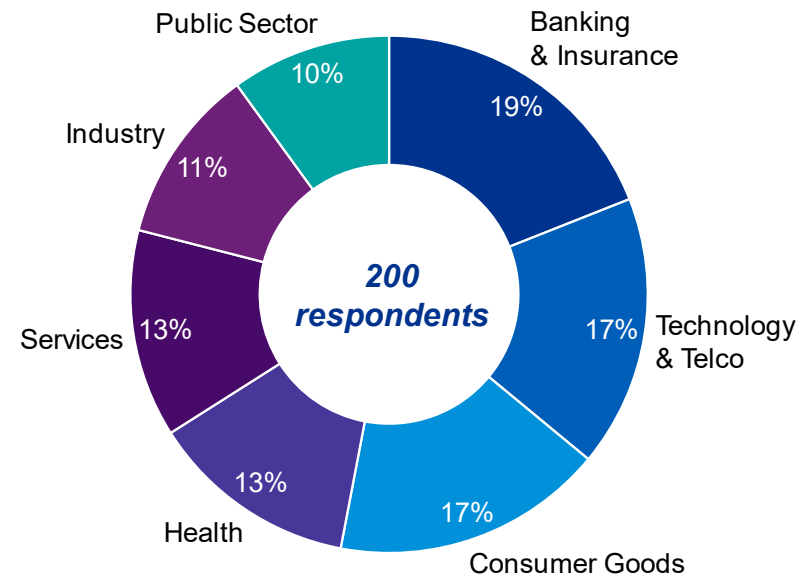
... varying in terms of number of employees, as well as respondents from different activity sectors

Profile of survey's respondents

Per number of employees



Per company's sector of activity

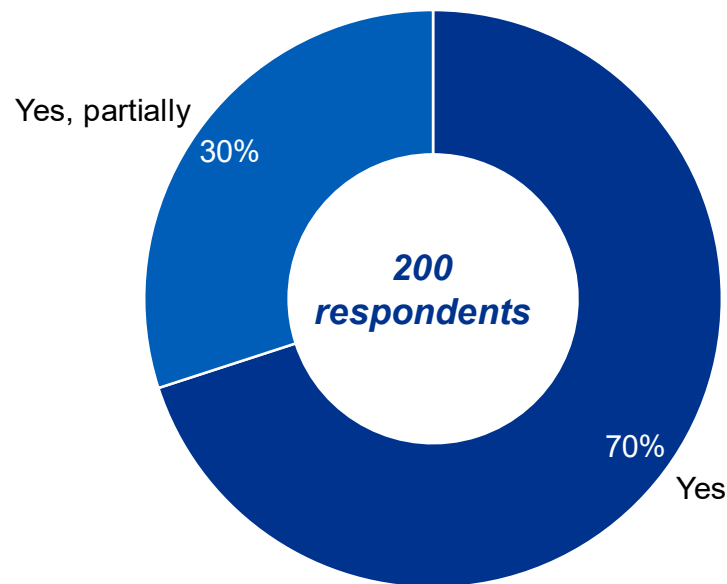


All respondents are involved in the decision-making processes related to cloud computing and the majority of them have a formalized cloud strategy

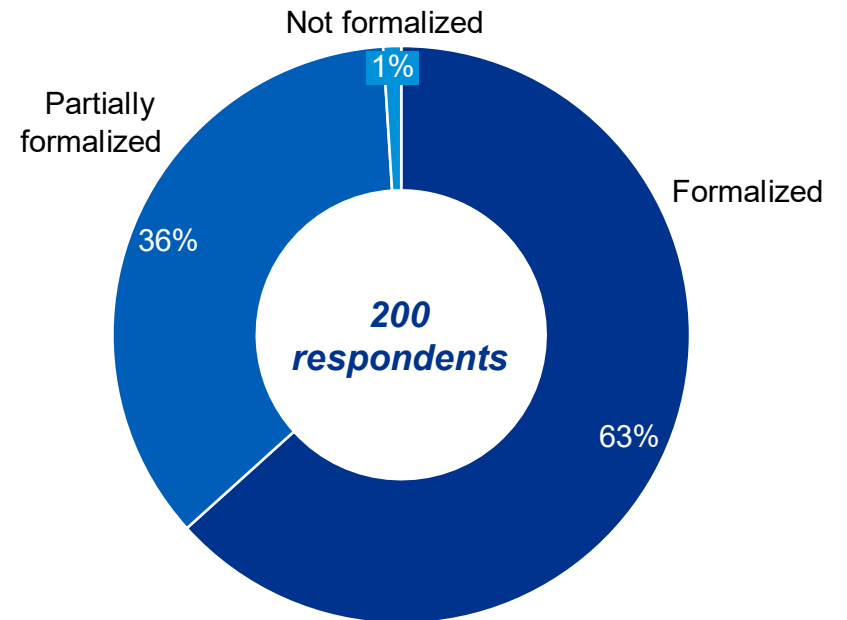
Profile of survey's respondents



Are you involved in the process of making decisions in regard to cloud computing in your organization?



How would you describe your cloud strategy?



6



Appendix -chapitre 2

The GDPR has set-up a regulated “data-trade-zone” inside the European Union, and strongly regulated data processing rules outside the EU



The General Data Protection Regulation (GDPR) determines a particular level of protection for personal data and therefore, enables the free flows of personal data inside and outside the EU



Who is concerned?

Any organization, public or private, regardless of its size, country of establishment and activity

The General Data Protection Regulation

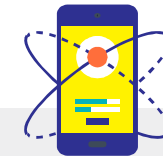
- Generates **more obligations** for the processors and controllers
- Reinforces the **rights of the persons** whose data is processed
- Requires the implementation of **specific technical and organizational measures**



Personal data

Any information relating to an identified or identifiable natural person

Article 4.1 of GDPR : “an identifiable natural person is **one who can be identified, directly or indirectly**, in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”



Data processing

Any operation, or set of operations, relating to personal data

Article 4.2 of GDPR : “‘processing’ means any operation or set of operations which is **performed on personal data** or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

The GDPR provides a consistent framework for personal data protection across the European Union, allowing free internal data flows



- In order to ensure a **consistent and high** level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be **equivalent in all Member States**⁽¹⁾

It is because of the fact that the GDPR is a homogenous regulation in all Member states that this consistent protection can be ensured throughout the Union.

The GDPR provides a consistent framework for personal data protection across the European Union, allowing free internal data flows

Standard guidelines

“ Recital 101 of GDPR ”

Flows of personal data **to and from** countries outside EU and international organization are **necessary for the expansion of international trade and international cooperation**



- The GDPR does not forbid the international flows. However it establish that when controllers or processors make transfers in 3rd countries or to international organization, they must ensure that **“the level of protection of natural persons ensured in the EU by the GDPR is not undermined”**

- In order to ensure a **consistent and high level** of protection of natural persons and to **remove the obstacles to flows** of personal data **outside the Union**, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be **essentially equivalent to that guaranteed within the EU**

The GDPR ensures a **minimum threshold** to be respected, regardless of the origin of the controller or the processor.

3 main sets of tools have been created by the GDPR to facilitate compliance in these situations of outbound data flows

Toolbox

Since **transfers of personal data outside UE is inevitable**, the GDPR has created a toolbox to ensure that such transfers respect the **minimum threshold** established

1 First tool : the adequacy decision

The Commission may decide with **effect for the entire EU** that a 3rd country, a territory or specified sector within a 3rd country or an international organization, **offers an adequate level of data protection** thus providing legal certainty and uniformity throughout the EU as regard the 3rd countries or international organization which is considered to provide such level of protection ⁽¹⁾



2 Second tool : standard contractual clauses

Standard Contractual Clauses (SCCs) adopted by the Commission can be used between controllers and providers in order to **ensure sufficient safeguards** on data protection for the data transferred internationally.

3 Third tool : binding corporate rules (BCRs)

In case of intragroup transfers of personal data outside EU the binding corporate rules can and must be **established inside the same group** when entities all over the world are involved.

The Privacy Shield was an attempt in 2016 to permit data transfer and data access between the US and the EU... but was invalidated in 2020



2016

The Privacy Shield is a framework, signed by the US and the European Union (adequacy decision), that aims to **protect the fundamental rights of EU online users** whose personal data would be handled by US companies and organizations. It allows controllers and processors to **freely transfer the personal data of EU nationals while respecting their personal rights.**

2020



Privacy Shield Invalidation (Schrems II)

Following a complaint by data protection activist M. SCHREMS, the EU Court of Justice invalidated the Privacy Shield agreement, considering that the US surveillance programs were **not compatible** with the GDPR principles.



The "Foreign Intelligence Surveillance Act" (FISA) and the Executive Order 12333 allow American public authorities to access any personal data that are transferred on U.S. soil



As a consequence of the invalidation of the Privacy Shield, companies transferring personal data to servers outside the EU **no longer have a legal basis** to do so and may be subject to prosecution

Indeed, the Cloud Act now permits a relatively large degree of access by US gov. to personal data, within or outside the US, in contradiction with GDPR



The Clarifying Lawful Overseas Use of Data (Cloud) Act US federal law requiring providers of electronic communication services or remote computing services to disclose personal user data to U.S. government, whether the information is located within or outside the US



Who is concerned?

All suppliers subject to U.S. law i.e. an entity doing business in the US, such as:

- **US companies**
- Foreign-based entities with **U.S. subsidiaries**



Conditions for data disclosure

Authorities can only compel service providers to provide data by complying with the strict legal provisions of a **warrant issued by a U.S. court**

Number of government requests received for user information (2019)



81,785 requests across all of Google, with **282** targeting enterprises, **152** data produced for requests relating to G Suite Enterprise Cloud customers and 0 for requests relating to Google Cloud Platform Enterprise customer

As a result of this invalidation of the Privacy Shield, the GDPR's toolbox also became obsolete, raising key questions for American and EU companies

An ineffective GDPR's toolbox



The SCHREMS II Case put in **reconsideration** the whole toolbox created by the GDPR to the extent that it is no longer possible, regardless of the tool, to ensure an adequate level of protection for personal data transferred to the USA.



National legislation prevails on any of the tools offered by the GDPR since the other means to ensure an adequate level of protection of personal data transferred outside the EU are contractual tools

New questions arise from the toolbox reconsideration

- When you are an **American hosting** company you could only process EU personal data on the basis of an adequacy decision (Safe Harbor then Privacy Shield). What happened if such adequacy decision is cancelled?
- If you are a hosting company, **established in EU but affiliates and controlled by an American company**, what happened when the adequacy decision upon which the personal data were processed is cancelled?

Considering the invalidation of the Privacy Shield, the European Data Protection Board (EDPB) has proposed a new toolbox, along 6 key steps

EDPB1 new toolbox



Considering the invalidation of the Privacy Shield, the European Data Protection Board has proposed a **new toolbox** **ROADMAP of ACCOUNTABILITY** : which implies **6 steps to follow** in order for exporters to assess third countries and identify appropriate supplementary measures where needed



The EDPB also listed **different authorized and prohibited uses-cases** to help companies identified where they stand regarding their processing of personal data

- 3 types of possible measures :**
- Technical measures
 - Contractual measures
 - Organizational measures

Note : (1). European Data Protection Board
Source: KPMG Avocats

EDPB remedies to the Privacy Shield invalidation in a number of use cases involving personal data



Authorized Use-Cases

- ✓ Use Case 1: data storage for backup and other purposes that do not require access to data in the clear
- ✓ Use Case 2: Transfer of pseudonymized data
- ✓ Use Case 3: Encrypted data merely transiting to third countries

✓ Use Case 4: Protected recipient

✓ Use Case 5: Split or multi-party processing

Implies to contractually provide for security technical measures around personal data transfers

The EDPB refers to a data exporter transferring personal data to a data importer to a third country specifically protected by that country's law for example for the purpose of jointly provide medical treatment for a patient or legal service to a client.

Such use-case is authorized if, among others, the law of the third country exempts a resident data importer from potentially infringing access to data held by that recipient for the given purpose (professional secrecy) and that technical measures are taken to ensure such privileged information (cryptographic keys, passwords etc.)





The EDPB refers to a data exporter wishing to process personal data jointly with two or more independent processors located in different jurisdiction without disclosing the content of the data to them. Prior to the transmission, the data exporter splits the data in such way that no part an individual processor receive suffices to reconstruct the personal data in whole or in part.

Such use-case is authorized if, among others, the data exporter processes personal data in such a manner that it is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information and each of the pieces is transferred to a separate processor located in a different jurisdiction



Yet two of the most common use cases appear still prohibited despite the EPDB's efforts to mitigate consequences of the Privacy Shield invalidation

Prohibited Use-Cases

-  Use Case 6: transfer to cloud services providers or other processors which require access to data in the clear
-  Use Case 7: Remote access to data for business purposes



We can clearly see that the remedy of the EDPB is partial since the most current uses cases are the one prohibited

The EDPB refers to a data exporter using a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

 Such case is prohibited since the cloud service provider or other processors need access to the data in the clear in order to execute the task assigned and if the recipients' third country grants power to public authorities to access the transferred data in a way that goes beyond what is necessary and proportionate in a democratic society



The EDPB refers to a data exporter making personal data available to entities in a third country to be used for shared business purposes. That can be a controller or processor established on the territory of a EU Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertaking or a group engaged in a joint economic activity.

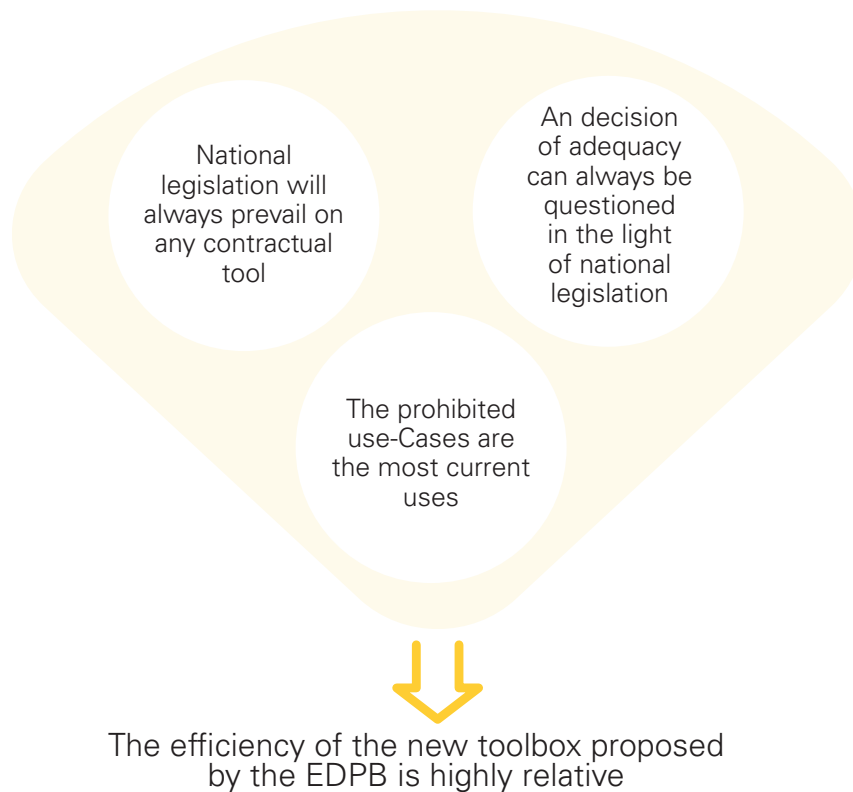
 Such case is prohibited since the data exporter allows the importer direct access of data of its own choice by transferring it directly through use of a communication service for the importer to use such data in the clear for its own purposes, particularly if the importer's third country grants power to public authorities to access the transferred data in a way that goes beyond what is necessary and proportionate in a democratic society



In both scenarios, even transport encryption and data-at-rest encryption together cannot constitute a supplementary measure that ensure an essentially equivalent level of protection for personal data

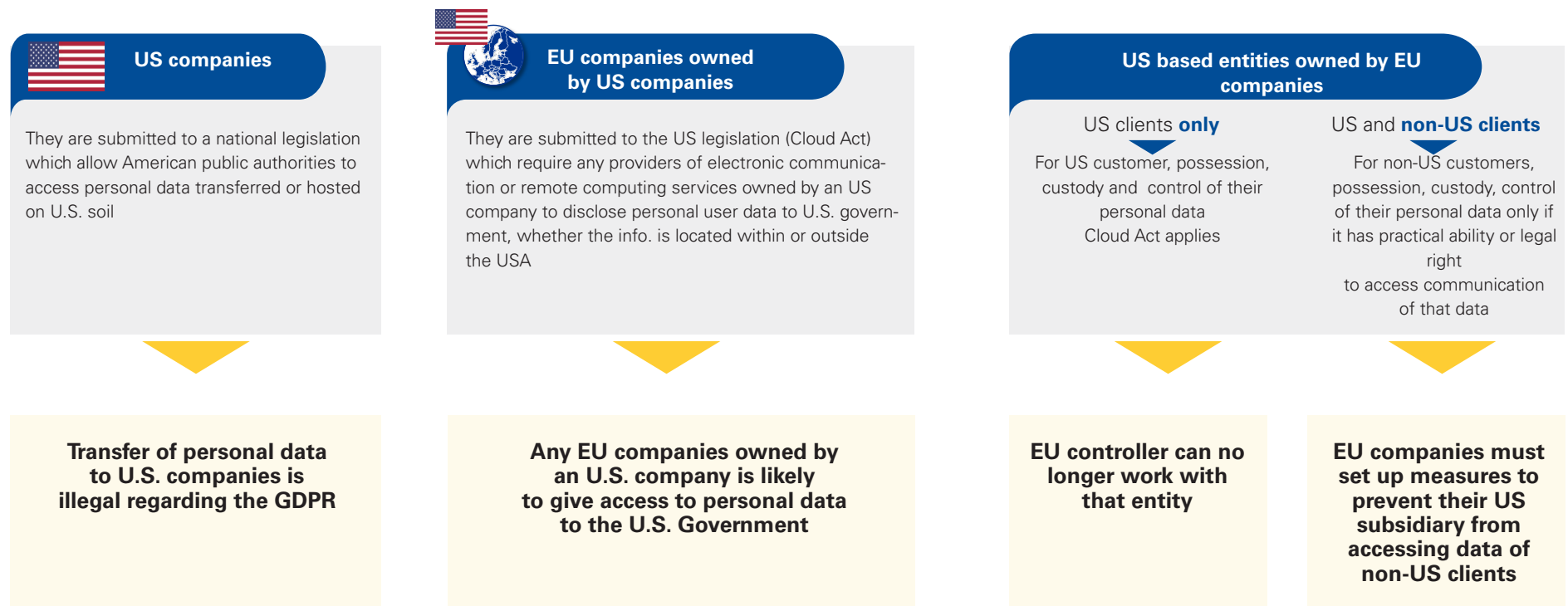
In conclusion, the success of the EDPB's remedy efforts – through its toolbox – appears largely relative, as the prohibited use cases are the most common ones

Efficiency of the EDPB remedies?



- This means that the problematic of the reconsideration of the initial toolbox established by the GDPR is applicable to **all transfers of personal data outside of EU**, not only towards the USA but also to other third countries like the UK for example after the Brexit.

As a conclusion, EU companies subject to the GDPR, as controllers, can no longer work with U.S. companies or European companies owned by U.S. companies



• **EU companies subject to the GDPR, as controllers, can no longer work with US companies, EU companies owned by U.S. companies, or US based entities owned by EU companies with US clients only**, to the extent that U.S. legislation breaks with the GDPR principle of adequate protection, whether the information is located within or outside the USA



Jean-Charles Ferreri

Partner

KPMG Global Strategy Group

Tel: +33 (0)6 60 07 08 99
jferreri@kpmg.fr



Bertrand Grau

Partner

KPMG Global Strategy Group

Tel: +33 (1) 55 68 25 10
bertrandgrau@kpmg.fr



Sébastien Ropartz

Partner

KPMG Technology Transformation

Tel: +33 (1) 55 68 38 83
sropartz@kpmg.fr



Patrick Amouzou

Partner

KPMG Avocats

Tel: +33 (1) 55 68 51 19
pamouzou@kpmgavocats.fr