Microsoft Azure Cloud Services: Export Controls of the US, UK, EU and Japan

July 8, 2020

This paper is written by
David Addis
Peter Lichtenbaum
David Lorello
Covington & Burling LLP

With contributions from:
Stevan Vidich, Principal Program Manager Azure Global
Anne Marie Griffin, Director Regulatory Affairs Worldwide Tax & Trade
Satoshi Funayama, Senior Attorney Corporate External & Legal Affairs
Microsoft Corporation

Microsoft Azure Cloud Services: Export Controls of the US, UK, EU and Japan

Revised July 2020

This paper offers a brief overview of United States, United Kingdom, European Union and Japan export control laws and regulations as they may apply to use of Microsoft Azure cloud services and platform, with some general guidance concerning the considerations that Azure customers should bear in mind to assess their obligations under US, UK, EU, and Japan export controls.[1] The Azure platform offers flexible options, capabilities and tools that customers may use to help ensure export-compliance in their use of Azure cloud services.

US export controls are laws and regulations to control the export and transfer of items from the United States or to non-US persons, in the interest of protecting US national security and furthering US foreign policy and other interests. The UK, EU and Japan implement similar export controls. US, UK, EU and Japan export controls apply not only to traditional cross-border shipments of physical goods, but also transfers, uploads or downloads of controlled software and data. That includes transfers, uploads or downloads of software or specific technical data using cloud-based services.

Microsoft Azure is a comprehensive set of robust and flexible cloud services, with a global network of datacenters, for enterprises of all sizes as well as individual developers and IT professionals to build, deploy, and manage applications, to support and integrate enterprise networks, power data analytics and computing, and store data. Microsoft Azure offers the full gamut of cloud service offerings to allow customers to quickly deploy infrastructure and services to meet business needs. *Infrastructure as a Service ("IaaS")* allows customers to provision computing, storage, and networking resources, and deploy and run software, which can include operating systems and applications. *Platform as a Service ("PaaS")* provides customers with a complete development and deployment environment in the cloud, including operating system, middleware, development tools, business intelligence services, database management systems, and allows enterprises to deploy their own application code on the Azure cloud platform. *Software as a Service ("SaaS")* delivers a complete software solution where the service provider manages the hardware and software, and with the appropriate service agreement, will ensure the availability and security of the application and customer data as well. Microsoft Azure also supports on-premises deployments at customer datacenters, and hybrid models that seamlessly integrate cloud-based and on-premises resources.

[1] The United Kingdom withdrew from the European Union on 31 January 2020. However, the UK currently remains subject to EU dual-use export controls legislation under interim measures that are expected to remain in place at least until the end of 2020. We note, in this regard, that as of this writing, the UK is in the process of developing guidance concerning the UK technology export controls regime, which is expected to include a specific discussion on the export controls implications of cloud computing. Microsoft may update this paper, to the extent warranted, based on the UK guidance once it is published.

The Microsoft Azure platform and services by their nature involve storage and processing of customer data on Microsoft's global cloud infrastructure, and transmission of customer data across the Internet to and from Microsoft's cloud infrastructure, within and between Azure datacenters and regions, and between the customer's virtual machines and its end users. The Azure suite of cloud products makes use of physical infrastructure that is located inside and outside of the United States, UK, EU and Japan; and some Azure service operations personnel who have access to customer data subject to export controls of one of those jurisdictions may in some cases be persons who are located in or nationals of a different jurisdiction. Organizations and enterprise customers may therefore need to consider whether and how export controls of the US, UK, EU and Japan may apply to their organization's use of Azure, as explained in more detail in the paper that follows. With appropriate planning, customers can use Azure tools and their own internal procedures to help ensure compliance with these export controls when using the Azure platform.

Customers are wholly responsible for ensuring their own compliance with all applicable laws and regulations. Information provided in this document does not constitute legal advice, and customers should consult their legal advisors for any questions regarding regulatory compliance.

1. Executive Summary

As the first step, customers should consider whether any of the data they want to use or store in the Azure cloud may even be subject to export controls. Export controls are intended to cover specific, non-public technical information required for production or development of a controlled product, and most types of customer data used or stored in the Azure cloud are not the kind of specific technical data that is subject to US, UK, EU or Japanese export controls. Many customers will face little or no export control risks from use of the Azure cloud, because most or all of the customer data in Azure is business or financial information that is simply not controlled for export at all.

Accessing grid and cloud computing services for computational capacity, or storing or processing data in the Azure platform, is not by itself subject to export controls as long the cloud is not used to make available controlled, proprietary technical information or software that is covered by U.S., UK, EU or Japanese export controls.

Moreover, even when technical data is covered by export controls of these jurisdictions, in most cases export licensing is required only for export, reexport or transfer to a small number of countries, primarily those that are subject to US, UK, or EU sanctions. , Microsoft Azure does not have infrastructure to store or process data used for Azure Services in any of these locations.

Where technical data subject to tighter US, UK, EU, or Japan export controls may be involved, Azure offers features that help mitigate the potential risk that customers may inadvertently

violate export controls when uploading or downloading controlled technical data in Azure. For example:

- Azure gives customers visibility and control as to where their customer data is stored, and customers have the ability to restrict the storage of customer data to a single geography, region, or country. For example, with Locally Redundant Storage (LRS), data is stored locally within the users' primary region. With Geo Redundant Storage (GRS), data is also replicated to a secondary region 250+ miles from the primary region but within the same geography.

- Azure gives customers visibility and control to know who can access their data and on what terms, and implements strong measures to protect customers' data from inappropriate access, including limits for Microsoft personnel and subcontractors.

- Azure customers can encrypt data in storage and in transit with robust encryption options to manage and help protect against export control risks. Microsoft Azure offers customers "end-to-end" encryption features that are compliant with FIPS 140-2 standards as prescribed by the US safe harbor rules discussed in this paper.

- Microsoft carries out background checks on all US-based employees who have the potential to access customer data, including checks against export-related lists maintained by the Departments of Commerce, State and Treasury, as well as EU and UK prohibited party lists.

- Specialized Azure solutions and delivery models, including the Azure Government offering, are specifically designed to support ITAR and other highly controlled data categories. Azure Government, hosted in seven dedicated datacenter regions in the United States and operated by screened US persons, provides compliance and security for US government customers as well as qualified US commercial entities in the defense sector.

- Microsoft provides Azure Stack and Azure Stack Edge as key enabling technologies that allow customers to process highly sensitive data using a private or hybrid cloud to ensure that customers have sole operational control over sensitive data.

These features and the ways they can help some customers mitigate export control risk are all described in more detail in the rest of this paper. Accordingly, Azure customers should consider the summary below and carefully monitor the export control requirements for any data that they place into the Azure cloud to ensure compliance with US, UK, EU and/or Japanese export controls.

2. What are export controls?

The export control laws and regulations of the US, UK, and EU and Japan apply not only to traditional exports or transfers of commodities and hardware, but also transfers, uploads or

downloads of software, and transfers or disclosures of defined "technology" and "technical data"—all core features of cloud computing services. These export controls laws derive in part from international export controls arrangements (such as the Wassenaar Arrangement, for example) that seek to harmonize the export controls rules of participating countries; hence, some of the key controls and concepts in the US, UK, EU and Japanese export controls arrangements are similar to one another.

The primary US export controls with the broadest application are the Export Administration Regulations ("**EAR"**), which apply to most commercial items. The EU and UK maintain a similar export regime, which is reflected in the EU Dual Use Regulation and national laws that implement the EU Dual Use Regulation in the various EU Member States and the UK (the latter through transitional legislation implemented in connection with the UK's departure from the EU). Japan also maintains a similar export regime, which is reflected in the Foreign Exchange and Foreign Trade Act, and the relevant orders or regulations made on authority of that Act.

The United States, United Kingdom and EU Member States also have separate and more specialized export control regulations that govern the most sensitive items and technology. For example, the US International Traffic in Arms Regulations ("**ITAR"**) apply to many military, defense and intelligence items and related technical data. Similarly, the UK and EU Member States implement national military export controls regimes that are more restrictive in certain respects than the Dual Use Regulation, and control a range of sensitive military items, including technology and technical data. In Japan, military items are also subject to specific controls under provisions in the Foreign Exchange and Foreign Trade Act, and related orders or regulations.

Key features of the US, UK EU and Japan dual-use and military export controls regulations are summarized below; but note that other US, EU, and UK regulations impose export controls focused on specific industries, including nuclear energy.

2.1. The US Export Administration Regulations ("EAR"), EU Dual Use Regulation and Japanese Regulation

The EAR, administered by the US Department of Commerce, impose controls on the export and reexport of most commercial goods, software and technology, including so-called "dual-use" items that can be used both for commercial and military purposes as well as certain defense items. The EAR broadly govern exports from the United States; reexports or retransfers of US-origin items and certain foreign-origin items with more than a *de minimis* portion of US-origin content; and transfers or disclosures to persons from other countries.

In the EU and UK, the Dual Use Regulation imposes controls on the export of dual-use goods, software, and technology, which are in many respects similar to the EAR (the EU/UK and US regimes derive from a number of international treaties and arrangements that the EU, UK, and US, as well as Japan, are all parties to). The Dual Use Regulation is narrower, however, in certain respects than the EAR. For instance, the Dual Use Regulation does not impose restrictions on the in-country transfer of technical data merely on the basis that the recipient is

a national of another country, and the Dual Use Regulation imposes controls on reexports or retransfers from outside of the EU/UK only in limited circumstances (such as, in particular, if the original exports from the EU/UK were made under licensing conditions that restricted the onward transfer of those items absent further approval from the relevant national licensing authority).

In Japan, consistent with multinational agreements, dual-use goods and technologies (including software) are also subject to essentially the same export controls as those of the US and EU. In Japan, transfers of controlled technology to "non-residents" (including a Japanese person who has established residency in a foreign country, as well as a non-Japanese person who resides in a foreign country and a non-Japanese entity in a foreign country) are subject to export controls even if the transfer takes place within Japan.

2.2. The US International Traffic in Arms Regulations ("ITAR") and Military Controls of the EU, UK and Japan

The ITAR, administered by the US Department of State, impose controls on the export, temporary import, reexport and transfer of most military, defense and intelligence items (also known as "defense articles"). "Defense articles," including related software and technical data, that are subject to ITAR controls are defined as any item, software or technical data that are specifically designated or described on the US Munitions List ("USML"), or that provide "equivalent performance capabilities." The USML is intended to cover only items, software or technical data that provide "a critical military or intelligence advantage" that warrants ITAR control.

Like the EAR, the ITAR control not only exports of such items and technical data from the United States, but also reexports and retransfers in foreign countries. Even defense articles, including technical data, made or developed outside the United States may be subject to the ITAR if they contain any amount of ITAR-controlled US-origin content; unlike the EAR, ITAR jurisdiction has no *de minimis* limits.

In the EU, there is no single, EU-wide military export controls regime. Hence, military exports controls operate largely as a function of national laws of each EU Member State, although the EU Member States generally adopt similar approaches to the regulation of military exports, as does the UK. Similar to the ITAR, the UK and EU military export controls regulations focus on goods, software, and technology that are either specifically listed as military items in the EU Member State military lists (which are included as annexes to the regulations), or are otherwise specially designed or configured for a military end use. As with the EU Dual Use Regulation, the EU Member State and UK military export regulations control reexports or retransfers from outside of the EU/UK only in limited circumstances.

In Japan, military items are also subject to specific controls under provisions in the Foreign Exchange and Foreign Trade Act, and related orders or regulations.

2.3. "Technology" / "technical data" subject to export controls

In ordinary usage, "technology" may refer to hardware and software that provide technical solutions. But the EAR and EU Dual Use Regulation define the term "technology" to mean "information" only, distinct from hardware and software. More specifically, the EAR and EU Dual Use Regulation define "technology" subject to export controls as "[i]nformation necessary for the 'development,' 'production,' or 'use'" of a product.[2] "Technology" may take the form of "technical data" in a variety of forms, including blueprints, plans, diagrams, models, formulas, tables, manuals and instructions. Japan defines technology in similar terms; and in addition, "technology" subject to Japanese export control may also take the form of technical support, including technical support includes, for example, technical guidance, skills training, consulting services. Generally speaking, information that is publicly available is generally not subject to export controls in any of these jurisdictions.

Likewise, defense articles that are subject to US ITAR controls include "technical data" recorded or stored in any medium. The ITAR define controlled "technical data" as "information . . . required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification" of defense articles, as well as classified information; information covered by an invention secrecy order; and software "directly related" to defense articles. Again, similar standards exist in the UK and EU military export controls regulations. Japan does not have separate export control regulations that govern sensitive military items but such items are subject to specific export control regulations under the Foreign Exchange and Foreign Trade Act.

2.4. "Export" and "reexport" / "retransfer"

Under US and EU/UK export controls, an "export" includes the actual shipment or transmission of controlled items to another country (although it should be noted that under the EU Dual Use Regulation, exports of most dual-use items are not considered as regulated "exports" when they are made strictly within the EU to other EU Member States). However, exports are not limited to the traditional transportation of physical objects across national boundaries. "Exports" subject to US and EU/UK export controls also include transfers, uploads or downloads of technology/technical data to foreign countries, and transfers, releases or disclosures of technology/technical data or source code to persons or locations in foreign countries.

Similarly, a "reexport" or "retransfer" subject to US export controls includes the actual shipment or transmission of US items, software or technology from one non-US country to another non-US country, or in some cases the transfer of items to an unauthorized end-use or

[2] As a general matter, US regulators have advised that technical information that is only for "operation" of any item is not considered "use" technology for purposes of the EAR unless it also provides information concerning its installation, maintenance, repair, overhaul and refurbishing. In certain narrow circumstances, however, where specified in a particular ECCN and/or where the information may be released to a restricted party on the EAR Entity List, "technology" may include information that is limited to only some, but not all, of those "use" activities (i.e., operation, installation, maintenance, repair, overhaul or refurbishing a product).

end-user. As noted above, the EU and UK export controls regimes do not impose similarly broad reexport or retransfer controls, although in some cases such controls can effectively be imposed at the time items are exported from the UK or EU, as conditions to the initial export licenses. Japan does not generally regulate reexport or retransfer.

The US Commerce Department has confirmed in more than one advisory opinion that merely accessing cloud computing platforms or services for computational capacity is not by itself an "export" or "reexport" that is subject to the EAR. No "export" or "reexport" can occur without some transfer or release of controlled software or controlled technology/technical data. While the EU and UK authorities have not issued similar guidance, many exporters interpret the EU and UK regimes in a manner consistent with the US guidance.

2.5. "Deemed" exports / reexports

The EAR and ITAR also control "deemed" exports and reexports. A deemed export is the release, transfer or disclosure (including oral and visual disclosures) of technology/technical data or source code to a foreign national in the United States. A deemed reexport is a release, transfer or disclosure of US-origin technology/technical data or source code in one foreign country to a national of a different foreign country. Such a deemed export or reexport generally is subject to the same requirements as an export made to the home country or countries of the foreign national.

A "foreign person" or "foreign national" for this purpose is any person or entity that is not a "US person," defined as (1) an individual who is a US citizen, US permanent resident (*i.e.*, green-card holder), or protected individual under the Immigration and Naturalization Act; (2) a corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated under US law; or (3) any federal, state, or local governmental entity in the United States. All other persons are "foreign persons." Importantly, a foreign national working for a US company remains subject to US export controls for potential "deemed exports" even if the foreign national is located and legally employed in the United States under a visa.

The EAR and ITAR generally apply similar principles for deemed exports and reexports, but there are also certain differences. For example, a deemed export of EAR-controlled data or source code is deemed to be made to the foreign person's most recent country of citizenship or permanent residency. The ITAR apply a broader standard than the EAR as to what foreign "nationality" counts for purposed of deemed exports and reexports, however: A release of ITAR-controlled data or software is deemed to be an export or reexport to all countries in which the foreign person has held or holds citizenship or holds permanent residency, not just the most recent.

The "release" of technology or software can occur through visual inspection or electronic exchanges of information in the United States or abroad. The inspection must actually reveal controlled technology or source code to a foreign person. Accordingly, the Commerce

Department has confirmed that the mere ability to access data without actual access, or actual access with limited exposure that is not sustained or complete enough to reveal the controlled technology or source code, would likely not constitute a "release" that results in a deemed export or reexport. Moreover, the State Department has likewise confirmed that "theoretical or potential access to technical data is not a 'release,'" and that a release occurs only "if a foreign person does actually access technical data." In that case, "the person who provided the access is an exporter" of the technical data for purposes of the ITAR.

The UK, EU and EU Member States do not impose "deemed" export or reexport controls. EU, UK or EU Member State licensing would not be required for transfers of restricted items within a given country, merely on the basis of the nationality of the recipient. However, EU/UK parties could potentially face liability if they were to share restricted items within a country with the knowledge that the recipient (irrespective of their nationality) intended to remove those items from the country in question without necessary export licensing.

Japan by contrast does control certain "deemed" exports (but not deemed reexports). Transfers to "non-residents" (including a Japanese person who has established residency in a foreign country, as well as a non-Japanese person who resides in a foreign country and a non-Japanese entity in a foreign country) are subject to export controls even if the transaction takes place within Japan. But unlike the EAR, under Japanese export controls foreign nationals employed by a Japanese entity in Japan are not generally subject to these deemed export license requirements.

2.6. EAR and ITAR Safe Harbors for "End-to-End Encryption"

The EAR and the ITAR each provide safe harbors for data that is encrypted "end-to-end," and the Commerce Department has advised that the EAR rule is intended to have "a major positive effect on the management and use of many cloud services," and says that it "is consistent with the common practices in both the government and industry, [and] allows for desired or necessary services to be performed within security boundaries." The EAR and ITAR rules generally use the same language with parallel scope and effect; but there are certain differences in the EAR and ITAR safe harbor rules that may be significant for the use of cloud-based services.

Scope of safe harbor. Both the EAR and the ITAR provide that "[s]ending, taking, or storing" controlled EAR technology or software, or ITAR technical data, will not be considered an export, reexport or transfer that is subject to regulation ***provided that*** it meets certain criteria: the technology or software must be (i) limited to information or software that is unclassified (i.e., not a government secret); (ii) secured using "end-to-end encryption" that meets NIST or equivalent standards with at least 128-bit encryption; and (iii) not "intentionally" stored in (or sent to) any one of 25 designated countries.[3] On this last requirement, the EAR and ITAR

[3] The 25 designated countries are currently Russia plus all the countries designated in EAR "Group D:5" and ITAR § 126.1, which are Afghanistan, Belarus, Burma (Myanmar), Central African Republic, China, Congo, Cote d'Ivoire, Cuba,
(continued…)

expressly provide that data "in-transit via the Internet" is not treated as "stored" for purposes of the rule. Thus, for example, encrypted files containing controlled technology temporarily cached on a server outside the approved list of countries while transiting the Internet could still be eligible for this safe harbor.

End-to-end encryption. "End-to-end encryption" means that the data must not be unencrypted (i.e., in clear text) at any point between the originator's "in-country security boundary" and the recipient's "in-country security boundary," and the means of decryption must not be provided to any third-party. The local network within the security boundary – the area in which decrypted/plaintext data can be processed – must be limited to a single country, and may not allow unencrypted data to cross national boundaries. As explained in the preamble to the BIS rule: "A consequence of this requirement is that data eligible for the carve-out must by definition be encrypted before crossing any national boundary and must remain encrypted at all times while being transmitted from one security boundary to another. This principle applies to transmissions within a cloud service infrastructure, where a transmission from one node or cloud infrastructure element to another could qualify for the carve-out provided that it was appropriately encrypted before any data crossed a national border."

For purposes of this end-to-end encryption definition, the originator and recipient can be the same entity. Alternatively, when a customer's encrypted data is uploaded to the cloud, the customer may be the originator while the cloud provider is the recipient (for purposes of this end-to-end encryption rule); when that customer downloads encrypted data from the cloud to its local "security boundary," the cloud provider may be the originator (for purposes of this rule) and the customer is the recipient. In other words, the EAR rule's requirement that "no third party" have the means of decryption is met as long as the means to decrypt are limited to the cloud customer and the cloud provider. Importantly, however, the ITAR rules also explicitly add that the intended recipient must be authorized to receive the ITAR technical data.

Differences between EAR and ITAR safe harbors. The ITAR requirement that the intended recipient of *encrypted* data must be authorized to receive the data in *unencrypted* form highlights the key difference between the EAR and ITAR end-to-end encryption rules. That difference concerns the "means of decryption" or "access information," defined to include decryption keys, network access codes, passwords, or any other information that allows access to encrypted technology, technical data or software. Under the EAR, a release of keys or other access information for encrypted technology requires licensing only if done with "knowledge" that it would result in an unauthorized release of the unencrypted technology. A "release" means inspection that actually "reveals" EAR-controlled technology. Access that does not actually reveal the substance of the technology – including the incidental access by system

---

Cyprus, Eritrea, Haiti, Iran, Iraq, Lebanon, Liberia, Libya, North Korea, Somalia, Sri Lanka, Sudan, Syria, Venezuela, Vietnam and Zimbabwe. Notably, although for many years Hong Kong has been treated for purposes of the EAR as a separate destination from Mainland China, U.S. authorities announced on June 29, 2020 that "We can no longer distinguish between the export of controlled items to Hong Kong or to mainland China…" and the situation remains fluid.

administrators – would not ordinarily be considered a "release" of the technology under the EAR, particularly where there are other work procedures and/or contractual commitments to limit any detailed review. In other words, while system administrators may need access to unencrypted data to perform that job, they generally have no need, and are directed not, to read or view customer data. On that basis, granting access to cloud administrators for the purpose only of system administration does not result in a "release" of technology, since no technology is actually "revealed."

The ITAR apparently impose a stricter regime. The ITAR define "release" of technical data to include any use of access information to cause or enable a foreign person to access, view, or possess unencrypted technical data, or cause technical data outside of the United States to be in unencrypted form – apparently regardless whether the access actually "reveals" any substantive technology to the foreign person. And unless the recipient is already authorized to receive the unencrypted technical data, the ITAR explicitly require licensing or other authorization to provide access information to a foreign person that "can cause or enable access, viewing, or possession" of unencrypted technical data (emphasis added). Thus, unlike the EAR, it appears that some authorization is required before granting foreign persons with access information that would enable them to decrypt ITAR technical data.

2.7. EU and UK interpretations

The EU has not issued any formal rulings that address the impact of EU export controls on cloud-based computing. Guidance from certain EU Member State regulators suggests an approach in the EU that would be similar to the interpretation of the EAR rule summarized above. In particular, some Member State regulators have indicated that when evaluating cloud computing systems, an "export" should be viewed to have occurred only in circumstances where controlled software or technology are rendered *accessible* to persons located outside of the EU Member State in question. Under that reasoning, an export will not have occurred merely on the basis that controlled software or technology were to be stored on a server located overseas. However, EU regulators have indicated that in order for this reasoning to apply, it would need to be assured that the controlled items are encrypted in accordance with adequate encryption standards sufficient to ensure that the data cannot readily be accessed from overseas, and that transfers of controlled software or technology should be made via end-to-end encryption. Some EU regulators have also suggested that transfers should be made via a "private cloud," which is described below. Finally, EU regulators have indicated that transfers of encryption keys likewise should be made in an adequately secure manner.

We note, however, that certain Member States — Germany being one example — have articulated interpretations of the EU Dual Use Regulation that are broader than what has been summarized above, and could call for licensing before at least certain types of controlled technology are exported to cloud services outside of the EU or the Member State in question. In the absence of any formal EU-wide guidance on this subject, it is important to consider how the individual Member States that are relevant to your specific deployment of a cloud service might evaluate the potential application of EU export controls.

From the standpoint of UK export controls, the UK Export Control Joint Unit ("ECJU") is, as of this writing, reported to be considering proposed written guidance on technology export controls, including issues related to use of the cloud. This guidance may address issues relevant to the discussion in this paper. Microsoft intends to examine the final UK guidance once it is published, and may update this paper, to the extent warranted, to address any new perspectives offered in the UK guidance.

2.8. Japan interpretations

In Japan, the Ministry of Economy, Trade and Industry ("METI") has advised that where a user enters into a storage service agreement only to store information on a server for such user's own use, no export license is required even if such user stores controlled technologies; however, a license may be required if a user is aware that a service provider can view, obtain or use stored controlled technologies. The mere ability to view information that is kept on the server does not require licensing, so that if the cloud agreement provides that the service provider can only view the information upon receiving the consent of the user, then no license would ordinarily be required.

Unlike the EAR, METI has not specifically addressed circumstances in which stored or transferred information is encrypted, nor how export controls applies to information in transit. However, the Center for Information on Security Trade Control (a private group) advises that users should take adequate measures to ensure that a service provider or any third party cannot view or obtain stored information, and that encrypting information is considered an effective measure for that purpose.

If a user uses a storage service in order to provide a third party (including a parent company and affiliated companies) with controlled technologies, an export license may be required.

3. Microsoft Azure and the "Cloud"

Microsoft Azure is a comprehensive set of robust and flexible cloud services, with a global network of datacenters, for enterprises of all sizes as well as individual developers and IT professionals to build, deploy, and manage applications, to support and integrate enterprise networks, power data analytics and computing, and for data storage. Microsoft Azure allows customers to quickly deploy infrastructure and services to meet business needs.

3.1. The Cloud

Cloud computing brings together technology solutions in new ways to deliver new efficiencies. The National Institute of Standards and Technology (NIST) defines the key features of cloud computing as customer-directed, on-demand network access to a shared pool of configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The NIST SP 800-145 defines the following cloud deployment models:

- **Public Cloud:** A cloud deployment model where the cloud infrastructure is provisioned for open use by the general public. Azure is an example of a public cloud.

- **Community Cloud:** A cloud deployment model where the cloud infrastructure is provisioned for exclusive use by a specific community of customers from organizations that have shared concerns, e.g., mission, security requirements, policy, and compliance considerations. Azure Government is an example of a community cloud.

- **Private Cloud:** A Private Cloud refers to computing resources used exclusively by a single customer organization, with services and infrastructure maintained on a private network. The Private Cloud is generally hosted "on-premises" — *i.e.*, physically located on the company's on-site datacenter(s) — or in a datacenter of a managed service provider. This might be necessary for certain applications or data that can't be moved to the shared cloud. Private Clouds can be structured to implement a technology stack that is consistent with the Public Cloud. Microsoft Azure Stack is a product that enables organizations to deliver Azure services from their own datacenters. It helps customers build and deploy applications the same way regardless of whether the applications run on Azure public cloud or Azure Stack.

- **Hybrid Cloud:** A cloud deployment model where the cloud infrastructure is comprised of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

Moreover, according to the NIST SP 800-145, cloud computing services can be offered in three different service models, outlined briefly below.

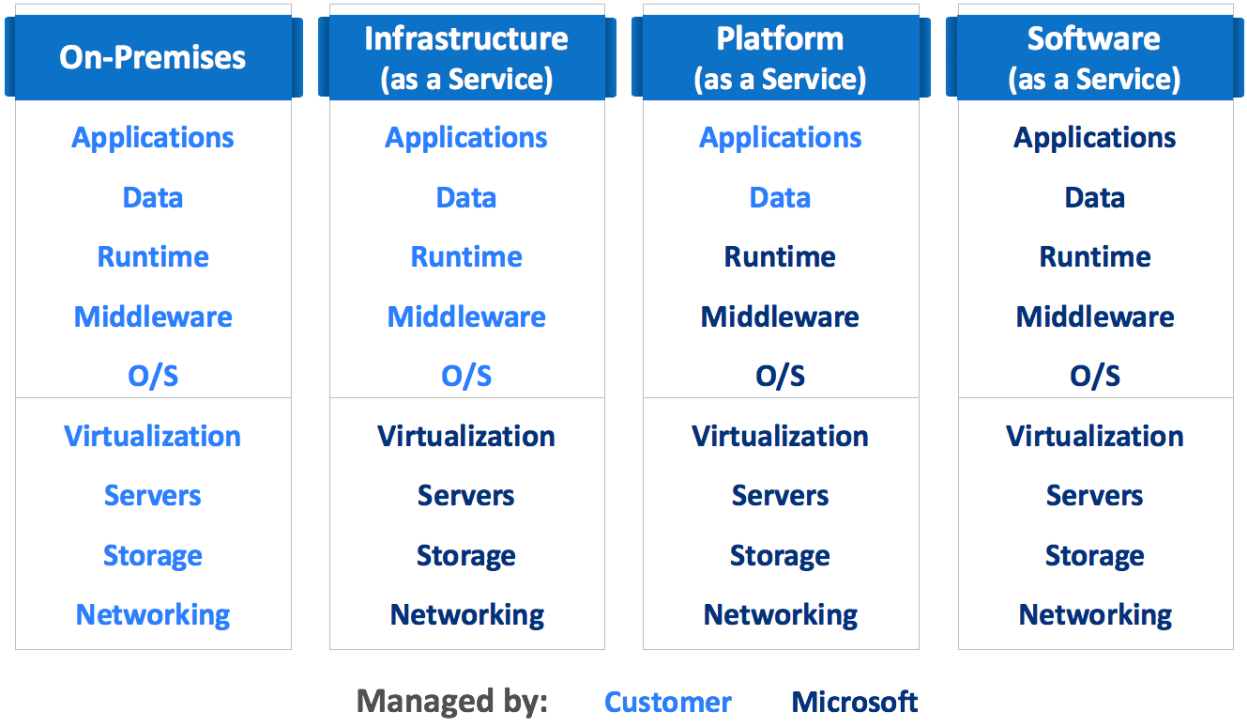
- **Infrastructure as a Service (IaaS):** Infrastructure as a Service abstracts hardware (server, storage, and network infrastructure) into a pool of computing, storage, and connectivity capabilities that are delivered as services for a usage-based (metered) cost. IaaS services allow customers to build and run server-based IT workloads in the cloud, rather than in their on-premises datacenter. IaaS services typically consist of an IT workload that runs on virtual machines that is transparently connected to the customer's on-premises network. IaaS is one of the most common cloud deployment patterns to date. It eliminates the need for capital expense budgets and reduces the time between purchasing and deployment to almost nothing.

- **Platform as a Service (PaaS):** Platform as a Service delivers application execution services, such as application runtime, storage, and integration, for applications written for a pre-specified development framework. In a PaaS deployment model, enterprises focus on deploying their application code into PaaS services. PaaS provides an efficient and agile approach to operate scale-out applications in a predictable and cost-effective

manner. Service levels and operational risks are shared because the customer takes responsibility for the stability, architectural compliance, and overall operations of the application while the provider delivers the platform capability (including the infrastructure and operational functions) at a predictable service level and cost.

- **Software as a Service (SaaS):** Software as a Service delivers business processes and applications, such as Customer Relationship Management (CRM), collaboration, and email, as standardized capabilities for a usage-based cost at an agreed, business-relevant service level. SaaS provides significant efficiencies in cost and delivery in exchange for minimal customization and represents a shift of operational risks from the consumer to the provider. All infrastructure and IT operational functions are abstracted away from the customer. IT departments need only to take care of provisioning users and data and perhaps integrating the application with Single Sign-On.

The chart below shows the shared responsibility concept in the Azure cloud computing platform as customers migrate from an on-premises environment to various Azure cloud service models (IaaS, PaaS, and SaaS):



With on-premises deployment in their own datacenter, customers assume the responsibility for all layers in the stack. As workloads get migrated to the cloud, Microsoft assumes progressively more responsibility depending on the cloud service model. For example, with the IaaS model, Microsoft's responsibility ends at the virtualization (Hypervisor) layer, and customers are responsible for all layers above the virtualization layer, including maintaining the base operating system in guest Virtual Machines. With finished cloud services in the SaaS model

such as Microsoft Office 365 or Dynamics 365, Microsoft assumes responsibility for all layers in the stack; however, customers are still responsible for administering the service, including granting proper access rights to end users.

Many enterprise IT cloud deployments will be based on the **Hybrid Cloud** deployment model. Hybrid clouds combine public and private clouds, using compute or storage resources on both the customer's on-premises network and in the cloud, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options. Hybrid clouds can be a path to migrate an organization to the cloud, or integrate cloud platforms and services with existing on-premises infrastructure as part of the organization's overall IT strategy.

3.2. Microsoft Azure

Microsoft Azure has announced more than 60 defined regions or geolocations across the globe. It currently has data centers in 24 different countries in North and South America, Europe, Asia, and Australia (with multiple defined regions within many of those countries).[4] Azure's global offering has no data centers located in any of the Group D:5 countries identified in Footnote 3 above.[5]

[4] As of the date of this paper, Microsoft Azure stores customer data at multiple datacenters in the United States, and in the following locations: Australia, Canada, Brazil, France, Germany, Hong Kong, India, Ireland, Israel, Italy, Japan, Mexico, the Netherlands, New Zealand, Norway, Poland, Qatar, Singapore, South Africa, South Korea, Spain, Switzerland, the United Arab Emirates, and the United Kingdom.

[5] Microsoft has a partnership with a local cloud provider in China to provide cloud services for customers to use cloud services and store data within China, a Group D:5 country. The partner is Shanghai Blue Cloud Technology Co., Ltd. (21Vianet), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd. and the largest carrier-neutral Internet provider of datacenter, hosting, managed network, and cloud computing infrastructure services in China. Microsoft is the technology provider, licensing its software, technology and solutions to 21Vianet, but does not operate the service. 21Vianet independently operates, provides, and manages the delivery of Microsoft cloud services to China-based customers and China-based users (including in some case China operations of multi-national Azure customers). By licensing Microsoft technologies, 21Vianet can offer Azure and Office 365 services and operate Azure and Office 365 datacenters that keep data within mainland China. 21Vianet also provides subscription and billing services, as well as support. No data of customers outside China is ever stored in China or in 21Vianet data centers, however; and the China Azure offerings are outside the scope of this paper.

In addition, Microsoft offers its Cloud for Government, including Azure Government, a mission-critical cloud operated by screened US persons from US datacenters, as described in more detail below at Section 3.3.[6]

Azure users can take advantage of this global network of datacenters to maintain availability in a cost-effective manner and provide applications close to their user base. Importantly, however, when customers entrust their data to Microsoft Azure, they are not giving up control. Azure gives customers visibility as to where their customer data is stored, and customers have the ability to restrict the storage of its data to a single geography, region, or country. For example, with Locally Redundant Storage (LRS), data is stored locally within the users' primary region. With Geo Redundant Storage (GRS), data is also replicated to a secondary region 250+ miles from the primary region but within the same geography.

The commitments described above relate to storage of data while "at rest." By the nature of cloud computing and the Internet itself, customer data that Microsoft transfers or processes on customers' behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities.

3.2.1. Customer control over access to data

Microsoft's Azure cloud infrastructure is administered, both in the United States and in other locations, by service operations personnel that include nationals of many countries. But customers can know who can access their data and on what terms. Microsoft takes strong measures to protect customers' data from inappropriate access, including limits for Microsoft personnel and subcontractors.

- Microsoft engineers do not have default access to customer data in the cloud and access to customer data is not needed to operate Azure. Moreover, for most support scenarios involving customer troubleshooting tickets, access to customer data is not needed. For those rare instances where resolving customer support requests requires elevated access to customer data, Microsoft engineers can be granted access to customer data under management oversight using temporary credentials via **Just-in-Time (JIT)** privileged access management system. Using the restricted access workflow, access to customer data is carefully controlled, logged, and revoked when it is no longer needed.

- Customer Lockbox for Azure is a service that provides customers with the capability to control how a Microsoft engineer accesses their data. As part of the support workflow, a Microsoft engineer may require elevated access to customer data. Azure Customer Lockbox puts the customer in charge of that decision by enabling the customer to

[6] Microsoft Cloud Germany is another national cloud platform, hosted in German datacenters. Access to customer data is controlled by an independent German Data Trustee operating under German law. T-Systems International GmbH, a subsidiary of Deutsche Telecom, acts as the independent Data Trustee for Microsoft Cloud Germany.

Approve/Deny such elevated requests. Azure Customer Lockbox is an extension of the JIT workflow and comes with full audit logging enabled. It is important to note that Customer Lockbox capability is not required for support cases that do not involve access to customer data. For the majority of support scenarios, access to customer data is not needed and the workflow should not require Customer Lockbox.

- Data encryption with option for customer managed encryption keys ensures that encrypted data is accessible only by entities who are in possession of the key, as described in the next section.

- Customer monitoring of external access to their provisioned Azure resources enables customers to receive security alerts and respond to a wide range of security threats.

Within a customer's Azure subscription, Microsoft provides an approach to allow customers to restrict system access to their own authorized users based on role assignment, role authorization, and permission authorization. Azure Active Directory (AD) is an identity repository and cloud service that provides authentication, authorization, and access control for an organization's users, groups, and objects. Azure AD can be used as a standalone cloud directory or as an integrated solution with existing on-premises Active Directory to enable key enterprise features such as directory synchronization and single sign-on.

Each Azure subscription is associated with an Azure AD tenant. Using Role-Based Access Control (RBAC), users, groups, and applications from that directory can be granted access to resources in the Azure subscription. For example, a storage account can be placed in a resource group to control access to that specific storage account using Azure AD. Azure Storage defines a set of built-in RBAC roles that encompass common permissions used to access blob or queue data. A request to Azure Storage can be authorized using either customer's Azure AD account or the Storage Account Key. In this manner, only specific users can be given the ability to access data in Azure Storage.

3.2.1. Azure tools for encryption, including "end-to-end" encryption

Azure has extensive support to safeguard customer data using data encryption in transit and at rest, as well as data encryption while in use. Azure customers can encrypt data in storage and in transit to align with best practices for protecting data confidentiality and integrity. Customers are able to encrypt communications within Azure Cloud Services and between deployments, between Azure regions, from Azure to on-premises datacenters, and between the customer's virtual machines and its end users. Azure offers robust encryption options, including "end-to-end" encryption features compliant with FIPS 140-2 standards, to allow customers to protect the security and integrity of their data, prevent unauthorized access, and provide additional options to manage and mitigate potential US export control risks. Microsoft uses multiple encryption methods, protocols, and algorithms across its products and services to help provide a secure path for data to travel through the infrastructure, and to help protect the confidentiality of data that is stored within the infrastructure. Microsoft uses some of the

strongest, most secure encryption protocols in the industry to provide a barrier against unauthorized access to your data.

Key management: Azure Key Vault is a multi-tenant secrets management service that uses Hardware Security Modules (HSMs) to store and control access to secrets, encryption keys, and certificates. Key Vault HSMs are FIPS 140-2 Level 2 validated, which includes requirements for physical tamper evidence and role-based authentication. With Azure Key Vault, customers can import or generate encryption keys in HSMs that never leave the HSM boundary to support Bring Your Own Key (BYOK) scenarios. Azure Key Vault can handle requesting and renewing certificates, including Transport Layer Security (TLS) certificates. It provides features for a robust solution for certificate lifecycle management. Importantly, Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents *do not see or extract* customer keys. Accordingly, customers can use the keys created and stored in Azure Key Vault to encrypt their own data stored and transferred in Azure "end-to-end", so that Microsoft Azure administrators and technical support personnel have no access to view the customer data in plaintext (unencrypted) form.

For customers who require single-tenant HSMs, Microsoft provides Azure Dedicated HSM, which has FIPS 140-2 Level 3 validation, as well as Common Criteria EAL4+ certification and conformance with eIDAS requirements. Azure Dedicated HSM is most suitable for scenarios where customers require full administrative control and sole access to their HSM device for administrative purposes. Dedicated HSMs are provisioned directly on customer's virtual network and can also connect to on-premises infrastructure via Virtual Private Network (VPN).

Data encryption in transit: Azure provides many options for encrypting data in transit.

- **Transport Layer Security (TLS)** – Azure uses the Transport Layer Security (TLS) protocol to help protect data when it is traveling between customers and Azure services, leveraging RSA-2048 for key exchange and AES-256 for data encryption. TLS provides strong authentication, message privacy, and integrity. Perfect Forward Secrecy (PFS) protects connections between customer's client systems and Microsoft cloud services by generating a unique session key for every session a customer initiate. PFS protects past sessions against potential future key compromises. This combination makes it more difficult to intercept and access data in transit. Customers can use Azure Application Gateway to configure end-to-end encryption of network traffic and rely on Azure Key Vault integration for TLS termination.

- **Azure Storage transactions** – When interacting with Azure Storage through the Azure portal, all transactions take place over HTTPS. Moreover, customers can configure their storage accounts to accept requests only from secure connections by setting the "secure transfer required" property for the storage account.

- **In-transit encryption for VMs** – Remote sessions to Windows and Linux VMs deployed in Azure can be conducted over protocols that ensure data encryption in transit such as

Remote Desktop Protocol (RDP) initiated from a client computer to Windows and Linux VMs to enable TLS protection for data in transit, and Secure Shell (SSH) for encrypted connections to Linux VMs running in Azure.

- **VPN encryption** – Customers can use Azure VPN Gateway to send encrypted traffic between their VNet and their on-premises infrastructure across the public Internet, e.g., a site-to-site VPN relies on IPSec for transport encryption. Customers can configure Azure VPN Gateway to use custom IPSec/IKE policy with specific cryptographic algorithms and key strengths instead of relying on the default Azure policies.

- **ExpressRoute encryption** – Customers can create private connections between their on-premises infrastructure and Azure by using Azure ExpressRoute with several data encryption options, including MACsec that enables customers to store MACsec encryption keys in Azure Key Vault.

Customers should review Azure best practices for the protection of data in transit to help ensure that all data in transit is encrypted. For key Azure services (e.g., Azure SQL Database), data encryption in transit is enforced by default.

Data encryption at rest: Azure provides extensive options for data encryption at rest to help customers safeguard their data and meet their compliance needs. This process relies on multiple encryption keys, as well as services such as Azure Key Vault and Azure Active Directory to ensure secure key access and centralized key management. In general, controlling key access and ensuring efficient bulk encryption and decryption of data is accomplished via the following types of encryption keys:

- **Data Encryption Key (DEK)** is a symmetric AES-256 key that is utilized for bulk encryption and decryption of a partition or a block of data. Access to DEKs is needed by the resource provider or application instance that is responsible for encrypting and decrypting a specific block of data. A single resource may have many partitions and many DEKs. When a DEK is replaced with a new key, only the data in its associated block must be re-encrypted with the new key. DEK is encrypted by the *Key Encryption Key (KEK)* and is never stored unencrypted.

- **Key Encryption Key (KEK)** is an asymmetric RSA-2048 key that is optionally provided by the customer. This key is utilized to encrypt the *Data Encryption Key (DEK)* using Azure Key Vault and exists only in Azure Key Vault. KEK is never exposed directly to the resource provider or other services. Access to KEK is controlled by permissions in Azure Key Vault and access to Azure Key Vault must be authenticated through Azure Active Directory. These permissions can be revoked to block access to this key and, by extension, the data that is encrypted using this key as the root of the key chain.

Detailed information about various encryption models, as well as specifics on key management for a wide range of Azure platform services is available in online documentation. The rest of

this section covers encryption implementation for key scenarios, including Storage service encryption, Azure SQL Database Transparent Data Encryption (TDE), and Azure Disk encryption.

- **Storage service encryption (SSE)** – Azure Storage Service Encryption for Data at Rest ensures that data is automatically encrypted before persisting it to Azure Storage and decrypted before retrieval. By default, Microsoft controls the encryption keys and is responsible for key rotation, usage, and access. Keys are stored securely and protected inside a Microsoft key store. This option provides the most convenience for customers given that all Azure Storage services are supported. However, customers can also choose to manage encryption with their own keys by specifying a) customer-managed key in Azure Key Vault for encrypting and decrypting all Blob storage and Azure Files, or b) customer-provided key in Azure Key Vault or another store on customer premises for encrypting and decrypting Blob storage only. Storage service encryption is enabled by default for all new and existing storage accounts and it cannot be disabled. The encryption process leverages two separate keys as described previously: 1) symmetric AES-256 DEK and 2) asymmetric RSA-2048 KEK.

- **Azure SQL Database encryption** – Azure SQL Database provides Transparent Data Encryption (TDE) at rest by default. TDE performs real-time encryption and decryption operations on the data and log files. Database Encryption Key (DEK) is a symmetric key stored in the database boot record for availability during recovery. It is secured via a certificate stored in the master database of the server or an asymmetric key called TDE Protector stored under customer control in Azure Key Vault, which is Azure's cloud-based external key management system. Azure Key Vault supports Bring Your Own Key (BYOK), which enables customers to store TDE Protector in Key Vault and control key management tasks including key rotation, permissions, deleting keys, enabling auditing/reporting on all TDE Protectors, etc. The key can be generated by the Key Vault, imported, or transferred to the Key Vault from an on-premises HSM device. Customers can also use the Always Encrypted feature of Azure SQL Database, which is designed specifically to help protect sensitive data by allowing clients to encrypt data inside client applications and never reveal the encryption keys to the Database Engine. In this manner, Always Encrypted provides separation between those who own the data (and can view it) and those who manage the data (but should have no access).

- **Disk encryption for Virtual Machines** – Azure Storage service encryption encrypts the page blobs that store Azure Virtual Machine disks. Additionally, Azure Disk Encryption (ADE) may optionally be used to encrypt all Azure Windows and Linux IaaS Virtual Machine disks. This encryption includes managed disks. ADE leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks used by an IaaS Virtual Machine. The solution is integrated with Azure Key Vault to help customers control and manage the disk encryption keys. Customers can supply their own encryption keys which are safeguarded in Azure Key Vault to support Bring Your Own Key (BYOK) scenarios. ADE relies on two encryption keys as described previously: 1) symmetric AES-256 DEK used

to encrypt OS and data volumes, and 2) asymmetric RSA-2048 KEK used to encrypt DEK and stored in Azure Key Vault under customer control.

Data encryption in use: Azure Confidential Computing is a set of new data security capabilities that offers encryption of data while in use. This means that data can be processed in the cloud with the assurance that it is always under customer control. Confidential computing ensures that when data is in the clear, which is needed for efficient data processing in memory, the data is protected inside a Trusted Execution Environment (TEE, also known as an enclave). TEE helps ensure that there is no way to view data or the operations from outside the enclave and that only the application designer has access to TEE data; access is denied to everyone else including Azure administrators. Moreover, TEE helps ensure that only authorized code is permitted to access data. If the code is altered or tampered with, the operations are denied, and the environment is disabled.

3.3. Azure Government

In addition, Microsoft offers Azure Government, which is a US government community cloud available to US government customers—from large federal agencies to small town governments — as well as US government defense contractors and qualified US commercial entities. Azure Government is operated by screened US persons.

Azure Government provides additional support for customers with data subject to the ITAR through contractual commitments to customers regarding the location of stored data, as well as limitations on the ability to access such data to US persons. Government and US commercial entities that require ITAR contract commitments are eligible for deployment in Azure Government. Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection and architecture of their applications within their environments. Customers must sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data, so that Microsoft may comply with responsibilities both to its customers and to the US government. The ITAR has specific obligations to report violations, which can provide certain risk mitigation benefits. The Microsoft Enterprise Agreement Amendment enables Microsoft and the customer to work together in reporting such violations.

Customers seeking to host ITAR-regulated data should work with their Microsoft account and licensing teams to learn more, obtain proper agreements, and access relevant system architecture information.

The Azure Government community cloud is available only to U.S. government entities and companies that support the U.S. government. For UK and EU defense sector customers, Microsoft can work with customers to develop hybrid/private cloud solutions (such as Azure Stack and Azure Stack Edge) with on-premises options that will allow those UK and EU customers to ensure that they are able to meet applicable local regulatory requirements (or contractual requirements imposed by local defense authorities).

4. How do export controls apply to Azure customers?

The US Commerce Department has made clear that, when data or software is uploaded to the cloud, or transferred between user nodes, the customer, not the cloud provider, is the "exporter" who has responsibility to ensure that transfers and storage of, and access to, that data or software complies with the EAR. Likewise, customers with ITAR-controlled technical data or software also have responsibility to ensure ITAR compliance. The EU and UK have not, to date, issued comprehensive guidance on this subject; however, informal guidance from UK and EU regulators suggests that the UK, EU and EU Member State export controls regimes should operate in a similar manner. Japanese regulators also suggest that cloud customers with controlled technology have the responsibility to comply with Japan export controls.

Because Microsoft's cloud infrastructure is physically located in multiple countries, and may be operated, maintained, and administered by personnel of different nationalities in a range of locations, Azure customers should be mindful of the relevant export controls and exceptions outlined above and their potential obligations to comply with those controls — as well as the robust tools available to Azure customers to manage export control risks.

4.1. Potential sources for export control risks

To begin with, most types of customer data are not considered "technology" or "technical data" as defined in the EAR, the ITAR, or the dual use and military export control regulations of the EU, UK or Japan. Most business, financial and personal information stored and processed in the cloud has no relationship to design, development, production, manufacture or use (operation, installation, maintenance, repair, refurbishing, and overhaul) of a controlled product, and is simply not subject to export controls at all. Information that is publicly available is also not generally subject to export controls in any of these jurisdictions. Only specific, proprietary (non-public) technical information related to an export-controlled product or process is subject to controls.

For specific proprietary technical data or software that are subject to export control jurisdiction, there are two main ways in which customers' use of the Azure cloud may implicate US, EU and UK and/or Japan export controls.[7]

First, as discussed above, Microsoft operates datacenters for the Azure cloud products in numerous countries around the world, for speed of access, redundancy, and reliability. When Azure customers upload data to the Azure cloud, there is at least the potential (mitigated by the customer's ability to select specific regions or countries) that the data may be transferred to a server that is physically located in a country other than country where the customer

[7] Note that for software distribution via the Azure Marketplace supply chain, the usual export controls for distribution of software to users, whether by remote download or on physical media, would generally apply. The focus of this paper, however, is on the aspects of export control compliance that are specific to the cloud and to users of cloud platforms for computational capacity and processing or storage of customer data, and thus we will not address Azure Marketplace here.

uploads the data from. The transfer of customer data to a cloud server may potentially constitute an export or reexport to the country in which the server is located (subject to the carve-out or safe harbor for "end-to-end" encryption). Likewise, the download of or access to customer data stored in an Azure data center or server in the United States, EU, UK or Japan by a user who is physically located outside the country where the server is located may also represent an export subject to export controls. Similarly, a "reexport" subject to US export controls (or restricted under UK or EU Member State licensing conditions) may arise from transfers of controlled data to or from servers in more than one location.

Second, access by service operations personnel who are foreign nationals to customer data on a cloud server could potentially lead to a "deemed export" or "deemed reexport" subject to US export controls. Microsoft's datacenters and other Azure cloud infrastructure are administered by both US and non-US persons. And given the multinational nature of the Azure service, the diverse workforce of employees, and the importance of "follow the sun" 24x7 technical support, Azure service operations personnel include nationals of many countries.

The risks summarized here may be particularly acute for technical data that is subject to ITAR controls, or to the UK EU Member State military export controls regulations; for example, the ITAR and similar UK/EU military export controls generally impose stricter licensing and compliance requirements for most destinations and nationalities, with fewer safe harbors or other accommodations for the cloud.

Nevertheless, Azure includes features that can help mitigate and manage these potential export control risks, as described in the following section.

4.2. Azure features to manage potential export control risks

The Azure cloud services are structured in ways that help to manage and significantly mitigate the potential risks that customers face under US, UK, EU and/or Japanese export controls.

Ability to control data location. A customer has visibility as to where its data is stored, and robust tools to restrict the storage of its data to a single geography, region, or country. A customer may therefore ensure that its data is stored in the United States or EU/UK and minimize transfer of controlled technology/technical data outside the United States or EU/UK. Similarly, customers in other regions also have information and ability to select the places their data may be stored. But as noted, given the nature of the Internet, when data is processed or in transit, there is no assurance that customer data will not be transferred to and processed in any location in which Microsoft or its affiliates or subcontractors maintain facilities.

Control over access to data. Customers can know and control who can access their data and on what terms. Microsoft technical support personnel do not need and do not have default access to customer data. For those rare instances where resolving customer support requests requires elevated access to customer data, customers have ability to grant Microsoft personnel temporary access customer data, under management oversight, using temporary **Just-in-Time (JIT)** credentials and Customer Lockbox; access is then revoked when it is no longer needed.

End-to-end encryption. In addition, Azure offers end-to-end encryption features that can provide customers with significant technical measures to manage and help protect against. export control risks, by taking advantage of the US EAR rule regarding "end-to-end encryption," and assessments of the EU/UK export controls framework that lead to an analysis similar to the US EAR rule. Using the tools and options outlined in Section 3.2 above, including Key Vault and Customer Managed Key (CMK) options, Azure customers can encrypt data at rest and in transit with a variety of robust encryption options, including "end-to-end" encryption features compliant with FIPS 140-2 or equivalent standards as prescribed by the EAR and ITAR rules. As a result, data integrity between the Azure datacenter security boundary and a customer's on-premises security boundary is assured by end-to-end encryption, mitigating against potential export control risks.

Customer data is not "intentionally stored" in a non-conforming location, consistent with the EAR and ITAR rules..

Azure can be configured to meet the EAR requirement that the means of decryption is not provided to any third-party: The decryption keys or other means of decryption can be limited only to two parties—the customer and Microsoft as Azure cloud provider — to comply with the EAR "end-to-end encryption" safe harbor. As explained above, under that rule, when a customer's encrypted data is uploaded to the cloud, the customer is the "originator" while the cloud provider is the "recipient" for purposes of the EAR rule; when that customer downloads encrypted data from the Azure cloud to its local "security boundary," Microsoft is then the originator and the customer is the recipient.

In addition, to comply with the requirements of the ITAR "end to end" encryption rule, Azure Key Vault also gives customers the ability to generate and manage their own encryption keys in FIPS 140-2 validated Hardware Security Modules (to which Microsoft does not have access) and determine who is authorized to use them. Customers can use the keys created and stored in Azure Key Vault to encrypt their own data stored and transferred in Azure "end-to-end", so that Microsoft Azure administrators and technical support personnel have no access to view the customer data in plaintext (unencrypted) form.

Tools and protocols to prevent unauthorized deemed export/reexport. Apart from the EAR "end-to-end encryption" safe harbor for physical storage locations, the use of encryption also helps protect against a potential *deemed* export (or deemed reexport), because even if a non-US person has access to the encrypted data, nothing is actually revealed to non-US person who cannot read or understand the data while it is encrypted and thus there is no "release" of any controlled data. Azure offers a wide range of encryption capabilities and solutions, flexibility to choose among encryption options, and robust tools for managing encryption.

In Japan there are no clear indications in METI's documents with respect to the case where information is encrypted. However, according to the Self-Management Guidelines issued by CISTEC, users should take measures to ensure that a service provider or any third party cannot

view or obtain stored information, and encrypting information is considered an effective measure.

Microsoft also implements a range of policies and security practices that strictly limit access by service operations personnel to customer data and thereby reduce—but not eliminate—Azure customers' potential risk under US, EU/UK and Japan export controls. As noted, Microsoft engineers do not have default access to customer data in the cloud. Instead, they are granted access, under management oversight, only when necessary. Using the restricted access workflow, access to Customer Data is carefully controlled, logged, and revoked when it is no longer needed. For example, access to Customer Data may be required to resolve customer-initiated troubleshooting requests. Evidence that procedures have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes is available from the Azure SOC 2 Type 2 attestation report produced by an independent third-party auditing firm.

These limitations that Microsoft places on access by service operations personnel to customer data have the practical effect of reducing Azure customers' potential risks under US, EU/UK and Japan export controls. Moreover, EAR rules allow service operations employees of cloud service providers to have access (in the rare cases that might be necessary) to data stored in foreign data centers without triggering a "deemed reexport" license requirement, provided that certain screening and other compliance measures are met.

Hybrid cloud. Microsoft provides Azure Stack and Azure Stack Edge as key enabling technologies that allow customers to process highly sensitive data using a private or hybrid cloud to ensure that customers have sole operational control over sensitive data.

Azure Stack is an integrated system of software and validated hardware that customers can purchase from Microsoft hardware partners, deploy in their own data center, and then operate entirely on their own or with the help from a managed service provider. With Azure Stack, the customer is always fully in control of access to their data. Azure and Azure Stack can help customers unlock new hybrid use cases for customer-facing and internal line of business application, including edge and disconnected scenarios, cloud applications intended to meet data sovereignty and custom compliance requirements, and cloud applications deployed on-premises in customer data center.

Azure Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. It enables customers to pre-process data at the edge and also move data to Azure efficiently. Azure Stack Edge uses advanced Field-Programmable Gate Array (FPGA) hardware natively integrated into the appliance to run Machine Learning algorithms at the edge efficiently. The size and portability allow customers to run Azure Stack Edge as close to users, apps, and data as needed.

5. What should I do to comply with export controls when using Azure?

Under the EAR, and under analyses of the EU, UK and Japanese export controls regimes that lead to similar assessments as the EAR guidance described above, when data is uploaded to a cloud server, such as the Azure cloud, the customer who is owner of the data—not the cloud services provider, such as Microsoft—should be considered the exporter. For that reason, the owner of the data—*i.e.*, the Azure customer—should understand the US, EU/UK and Japan export control implications of transferring data to the Azure cloud. In particular, Azure customers should consider, as discussed below, (1) whether the data is technology or technical data that is subject to the US, UK, EU, or Japanese export regulations at all, and if so, (2) how the data is classified for export control purposes, (3) where the data will physically be stored and processed, (4) the nationalities of service operations personnel who may have access to the data, and (5) whether an export license is required.

It is important to note that leveraging cloud technology need not be an all-or-nothing proposition: Many customers may find through their data classification and risk analysis that the lion's share of their data may be processed in the cloud with a small subset retained in a hybrid environment or a fully "on premises" environment.

5.1. Determine whether the data is "technology" or "technical data"

As highlighted above, most data stored or shared on Azure is not "technology" or "technical data" within the meaning of applicable export control regulations. Customers who have no "technology" or "technical data," as defined in these export control regulations, to store or use in Azure generally should not need to do anything further for export compliance.

5.2. Determine whether the data are controlled by the ITAR or other jurisdictions' military trade controls

Customers who hold or work with technical data potentially controlled by the ITAR or EU/UK military trade controls should already have in place robust procedures to identify and properly classify such technical data to ensure compliance. Microsoft offers several Azure options for customers to choose depending on their risk assessment and particular needs for ITAR-controlled data, data controlled under the EU or UK military trade controls, or other specialized export control obligations.

Azure Government. One of those options is Azure Government, which is available to US government entities at all levels as well as to qualified US commercial entities who handle data subject to the ITAR or other strict government regulations and requirements. US-based customers seeking to host ITAR-regulated data have the option, if they qualify, to use the Azure Government cloud to ensure ITAR compliance. Azure Government is hosted in seven datacenter regions limited exclusively to Azure Government customers and operated by screened US persons. It offers additional contractual commitments regarding the location of stored data, as well as limitations on the ability to access such data subject to the ITAR.

Microsoft provides these assurances for the infrastructure and operational components of these government cloud services, but customers are ultimately responsible for the protection

and architecture of their applications within their environments. Customers must sign additional agreements formally notifying Microsoft of their intention to store ITAR-controlled data, so that Microsoft may comply with responsibilities both to its customers and to the US government.

Azure Key Vault and end-to-end encryption tools. Customers have the ability to generate and/or bring their own encryption keys, and manage those keys, using the Azure Key Vault service. Azure customers can use these tools to encrypt data in storage and in transit "end-to-end," with assurance that customer data is not "intentionally stored" in a non-conforming location. Customers should carefully evaluate whether and how these tools can be used to ensure that the customer's use of Azure complies with the ITAR.

Hybrid cloud. Another option includes private and hybrid cloud solutions noted above. Customers may be able to restrict ITAR- or EU/UK military-controlled data to on-premises resources and leverage cloud resources for less-sensitive data. Please contact your Microsoft representative to discuss available Azure solutions and delivery models designed to support ITAR, EU/UK military, and other controlled data categories.

5.3. Classify the data that may be controlled technology under the EAR or other dual use export control regulations

If it appears that specific proprietary technology or technical data potentially subject to the EAR or EU Dual Use Regulation may be uploaded, stored, processed or used in Azure, the next step is to determine the appropriate Export Control Classification Number ("ECCN") or EU export controls classification for that technology or technical data. The ECCN export classification will determine the level of export controls applied to that technology. Data that meets the definition of "technology" under the EAR (specific information for development, production or use) but that is not described or covered by the criteria for any specific ECCN are given the default designation "EAR99." Under the EU Dual Use Regulation, such technology falls outside of the EU dual use classifications. More information concerning the export classification process is provided at the US Commerce Department's website. Similar resources are available on the websites of export controls regulators in the UK, EU Member States, and Japan. (See, for instance, the information published by the UK Government and by the Japanese government).

5.4. Take steps to comply with the EAR and other export control regulations

For technology subject to the EAR, the EU Dual Use Regulation or Japanese regulation, the relevant export controls classification, and the reasons for export control that apply to that classification, determine the next steps.

EAR99 or "AT" controlled ECCNs. If the ECCN indicates controls only for anti-terrorism reasons, indicated with the designation "AT," or if the technology is classified in the default EAR99 category, the EAR would not require licensing for export or reexport except to such sanctioned countries as Cuba, Iran, North Korea, Sudan, Syria and the Crimea region now claimed by

Russia. Such data may be placed in or used in the Azure cloud, as Azure does not have infrastructure in these locations.

The great majority of technical data falls within these EAR99 or AT-controlled categories, and many customers may find that they have little or no technical data that is subject to more stringent controls.

Under the EU Dual Use Regulation, technology that does not fall within any classifications in the EU Dual Use List (Annex I to the Dual Use Regulation) would generally not require an export license, except to the extent the exports are intended for a military end-use in a country subject to an EU arms embargo, exports to certain EU-sanctioned countries or parties, or exports that are known or suspected to be intended for activities in relation to weapons of mass destruction. Likewise, in Japan, an export license is not required with respect to technology that is not classified as controlled technology under Japanese regulation, except in the event that the exporter had knowledge about the risk of technology being used in the development, manufacture, use or storage of weapons of mass destruction, or in the development, manufacture, or use of conventional weapons, or when a notice is received from METI indicating that a license is needed.

Other Export Classifications. For the relatively smaller proportion of technology that falls within US ECCNs that are controlled for reasons other than "AT," or items that fall within EU Dual Use List classifications, the Azure customer can consider whether the relevant ECCN/EU classification has a licensing requirement for export to one or more of the Azure server location(s) for the relevant Azure product(s) and Geo being used.

1. End-to-end encryption solutions. As with ITAR compliance discussed above, customers should evaluate whether the end-to-end encryption features available for Azure are the most appropriate tools to manage these export control risks. As discussed above, it should often be possible to develop a plan to deploy end-to-end encryption that conforms to the requirements of the EAR carve-out or safe harbor: (1) Microsoft Azure offers encryption tools that comply with the specified FIPS 140-2 standard, and cryptographic measures that are "equally or more effective" than those standards, to satisfy the EAR rule; (2) customers can ensure that customer data is not "intentionally" stored in a prohibited location, because Microsoft does not have data centers for permanent storage in any one of the 25 prohibited locations; (3) the customer can structure its Azure plans and the way it uses Azure to keep data encrypted between the customer's "security boundary" in a given country and the Azure data center "security boundary" (or between different Azure data centers); (4) the means of decryption will be limited to two parties -- the customer and Microsoft -- and not available to any third-party; and (5) Azure Key Vault gives customers the ability to manage keys so that no Microsoft personnel have access at all.

2. License Exceptions / General Licenses. Alternatively, or in addition, if the relevant export classification does have a licensing requirement for one or more Azure regions being used, customers may want to consider whether any License Exception or General License is

available to authorize export without a specific license. The EAR and EU/UK dual use regimes all set forth a number of License Exceptions or General Licenses that permit eligible parties to carry out a defined category or type of export transactions, subject to specified criteria and conditions, without a specific license that would otherwise be required based on the export classification and reason for control. Japanese export control regulations also provide certain exceptions to licensing requirements.

3. Customer ability to select Azure regions and locations that do not require licensing. Customers have the ability to select where their data is stored, so that customers in North America are able to limit data storage to data centers in the United States. If the relevant export classification does not have any specific licensing requirement for any Azure server location designated for the relevant Azure product(s) and region/country being used, then US and EU/UK export controls generally should not prevent a customer from allowing that data to be stored in or downloaded to those Azure locations. In light of (1) the regional and country-specific datacenters and Microsoft commitments to store Azure in datacenters as directed by the customer; (2) the end-to-end encryption deployed and configurable in Azure to help customers limit and control where unencrypted data is "in the clear" between in-country security boundaries; and (3) the features such as Always Encrypted and other tools and protocols that minimize access to customer data by foreign-national service operations personnel, some customers may conclude that these are reasonable compliance measures and that putting such data in the Azure cloud involves a low risk of export control violations, enforcement actions or penalties.

4. Hybrid models. If the customer chooses not to rely on these measures to mitigate export control risk, and the export classification and reason for control for some technical data indicate that a specific license is required, then it would be prudent to explore other possible service delivery models. Azure and Azure Stack can help customers unlock new hybrid use cases with on-premises hosted workloads for export-controlled data, and cloud-based workloads for other data.

5. Azure Government. Alternatively, some US customers may consider whether they may qualify for Microsoft's ITAR-compliant Azure Government offering, and whether that may be a good solution not only for ITAR-controlled technical data, but also for technology that is subject to the highest levels of EAR controls.

6. Conclusion

Not all data are subject to the export controls of the US, EU, UK or Japan, and Microsoft Azure offers important features and tools to help customers manage export-control risks. Customers should carefully assess how their use of the Azure cloud may implicate export controls of these jurisdictions and determine whether any of the data they want to use or store in the Azure cloud may be subject to export controls, and if so, what controls apply. Where technical data subject to tighter export controls may be involved, Azure is configured to offer features that help mitigate the potential risk that customers may inadvertently violate export controls when

uploading or downloading controlled technical data in Azure. With appropriate planning, customers can use Azure tools and their own internal procedures to help ensure full compliance with US, EU, UK and Japanese export controls when using the Azure platform.

* * *

DISCLAIMER: IN THIS PAPER, NEITHER COVINGTON & BURLING LLP NOR MICROSOFT IS PROVIDING LEGAL ADVICE AND THE VIEWS EXPRESSED HEREIN ARE FOR INFORMATIONAL PURPOSES ONLY. THIS PAPER WAS DEVELOPED TO HELP CUSTOMERS UNDERSTAND CAPABILITIES OF AZURE TO MANAGE EXPORT CONTROL COMPLIANCE AND RISKS. READERS ARE ADVISED TO CONSULT WITH BOTH TECHNICAL AND LEGAL ADVISERS IN ASSESSING COMPLIANCE WITH US EXPORT CONTROL LAWS AND REGULATIONS AS APPLICABLE TO THEIR PARTICULAR USE OF AZURE.