COVINGTON

Microsoft Office 365: Export Controls of the US, UK, EU and Japan

August 11, 2020

David Addis
Peter Lichtenbaum
David Lorello
Covington & Burling LLP

With contributions from:
Anne Marie Griffin
Satoshi Funayama
Microsoft Corporation

Microsoft Office 365: Export Controls of the US, UK, EU and Japan

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 Office 365, with some general guidance concerning the considerations that Office 365 customers should bear in mind to assess their obligations under US, UK, and EU export controls.[1] Office 365 offers flexible options, capabilities and tools that customers may use to help ensure export-compliance.

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 software and data. That includes transfers, uploads or downloads of software or specific technical data using cloud-based services.

Office 365 is a cloud-based "Software as a Service" platform that includes the transmission of customer data across the Internet to and from Microsoft's cloud infrastructure and the storage and processing of customer data on Microsoft's cloud infrastructure. The focus of this paper is on Office 365-branded plans or suites intended for organizations (such as Exchange Online and SharePoint Online), rather than consumer Office 365 offerings such as Office 365 Home or Office 365 Personal. The Office 365 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 Office 365 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 Office 365, as explained in more detail in the paper that follows. With appropriate planning, customers can use Office 365 tools and their own internal procedures to help ensure compliance with these export control regimes when using the Office 365 platform.

[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.

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

Most data stored or used in Office 365 is limited to business or financial information that typically is not subject to or restricted by export control laws at all. Export controls cover only specific, non-public technical information for the production or development of a controlled product. For customers with data that meet those criteria and that *is* subject to export controls, Office 365 offers tools and features to help you manage your compliance.

Accessing cloud computing *services* of the Office 365 platform is not by itself subject to export controls as long as no controlled, proprietary technical information or software is released to foreign nationals or restricted jurisdictions or parties.

Even where data is restricted under export controls of the US, UK, EU or Japan, in most cases the restriction is limited to export, reexport or transfer to a small number of countries, primarily those that are subject to US, UK, EU, or Japan economic sanctions. Office 365 does not have infrastructure to store or process data in any such sanctioned locations.

When customers need to manage data that is controlled or restricted, Office 365 offers features that can help mitigate the risk of inadvertently violating export controls. For example:

- **Geolocation control**. For customers in North America, customer data is stored at rest in the United States, which minimizes transfer of controlled technology/technical data outside the United States. Similarly, customers in other regions (called "Geos") also have information about the places their customer data may be stored at rest, as described in the Office 365 Trust Center.

- **Access controls**. Microsoft implements a range of policies and security practices that strictly limit access to customer data by service operations personnel, including built-in controls that grant such personnel the "least privilege" access to the service, "just-in-time" accounts that strictly limit the time for access for a limited amount of time, and controlled access to take specific actions based on a defined role and task. Customer Lockbox is an optional feature that allows the customer to approve or reject access requests to customer content during service operations by Microsoft.

- **Encryption**. Office 365 offers end-to-end encryption features that are compliant with FIPS 140-2 standards as prescribed in US export regulations. These features provide customers with significant technical measures to encrypt data in storage and in transit, and to manage and help protect against US export control risks.

- **Personnel Screening**. 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.

- **Designation of controlled data**. Data Loss Prevention ("DLP"), developed to help organizations protect sensitive information and prevent its inadvertent disclosure, may provide ways for some customers to limit export compliance risk. DLP tools allow customers to conduct searches using key words that may help identify controlled technical data, or tag documents or data when the customer (using its own independent process) has determined the document or data is subject to export controls. DLP tools can also be used to prevent transfer of the designated data, and/or notify individual customers of potential controls before any transfer.

- **Specialized solutions for highly sensitive data**. Microsoft offers specialized Office 365 solutions and delivery models, including the Office 365 GCC High offering, that are designed to support ITAR and other highly-controlled data categories.

- **Hybrid solutions**. Microsoft is ready and able to work with customers to develop a customized "hybrid solution" that uses a mix of servers and resources on the customer's own premises together with cloud-based resources and services.

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. However, it is important to recognize that the nature of the Internet and cloud-based services means these measures cannot eliminate the customers' risk entirely. Accordingly, Office 365 customers should consider the summary below and carefully monitor the export control requirements for any data that they place into the Office 365 cloud to ensure compliance with US, EU, UK and/or Japanese export controls.

2. Office 365 and 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.

Cloud computing services can be offered in several different models: Microsoft Office 365 is an example of "software as a service (SaaS)" that allows the customer to use the provider's applications on cloud infrastructure. Other models for cloud services include "platform as a service (PaaS)," which allows the customer to deploy its own applications onto the provider's cloud infrastructure; and "infrastructure as a service (IaaS)," which allows the customer to deploy and run its own software environment, including both operating systems and applications, on the provider's cloud infrastructure.

Microsoft Office 365 is a cloud-based SaaS platform designed to help meet an organization's needs for robust security, reliability, and customer productivity with a range of software-as-a-service products. Technical descriptions, features and our compliance commitments for the products in the suite are available on Microsoft's website at https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx.

The Office 365 services are offered within specific regions, called "Geos." Information about the location of Office 365 cloud datacenters and data at rest locations is available from Microsoft at http://o365datacentermap.azurewebsites.net/.

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. *See* Microsoft Volume Licensing Online Services Terms June 2020).

Office 365 offers robust encryption options, including "end-to-end" encryption features, 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 and EU/UK export control risks, as described below.

Microsoft's Office 365 cloud infrastructure is administered, both in the United States and in other locations, by service operations personnel that include nationals of many countries. Because Microsoft's cloud infrastructure may be physically located in foreign countries, and may be operated, maintained, and administered by personnel of many nationalities, Office 365 customers should be mindful of the US, UK, EU and Japanese export controls and exceptions outlined in the following sections and their potential obligations to comply with those controls.

Office365 GCC High provides qualifying US customers with an alternative to help that customer manage its own compliance. Office365 GCC High is specifically tailored for US government agencies (including state and local agencies) and commercial companies sponsored to hold controlled, unclassified information. It is designed to address compliance requirements by ensuring that data is stored within the continental United States with compliant infrastructure, and that access to customer content is restricted to screened Microsoft personnel who are US citizens and have passed required background checks. The customer remains responsible to ensure any external party interaction remains compliant.

3. How do export controls apply to Office 365 customers?

The export control laws and regulations that are described in greater detail in Section 4 below apply not only to traditional exports or transfers of commodities and hardware, but also transfers, including electronic or online uploads or downloads, of software and of defined "technology" or technical information. Transfers of software and especially of data that may include defined "technology" subject to export controls are all core features of cloud computing services.

US regulators have 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 applicable export regulations. Likewise, customers with more sensitive data or software subject to separate regulations for defense and military items also have responsibility to ensure compliance with those regulations. The EU, UK and Japan 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.

Because Microsoft's cloud infrastructure may be physically located in multiple countries, and may be operated, maintained, and administered by personnel of different nationalities in a range of locations, Office 365 customers should be mindful of the relevant export controls and exceptions outlined in Section 4 below and their potential obligations to comply with those controls — as well as the robust tools available to manage export control risks.

3.1. Potential sources for export control risks

It is important to recognize that most types of customer data are not considered "technology" or "technical data" as defined in the dual use and military export control regulations of the US, 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 Office 365 cloud may implicate export controls.

First, as discussed above, Microsoft operates datacenters for the Office 365 cloud products in numerous countries around the world, for speed of access, redundancy, and reliability. When Office 365 customers upload data to the Office 365 cloud, there is at least the potential (mitigated by the Geo framework noted above) that the data may be transferred to a server that is physically located in a country other than the country where the customer 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. Likewise, the download of or access to customer data stored in a server 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 export control restrictions may arise from transfers of controlled data to or from servers in more than one location.

Second, US export control regulations apply equally to release or disclosure of controlled technical data to a foreign national in the same way they would apply to the export of that technical data to that person's home country (called a "deemed export," as explained in Section 4.5 below). 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 these US export controls. Microsoft's datacenters and other Office 365 cloud infrastructure are administered by both US and non-US persons (except for Office365 GCC High as noted above). And given the multinational nature of the Office 365 service, the diverse workforce of employees, and the importance of "follow the sun" 24/7 technical support, Office 365 service operations personnel include nationals of many countries.

These risks may be particularly acute for technical data that is subject to ITAR controls, or to the EU Member State military export controls regulations; for example, the ITAR and similar 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, Office 365 includes features that can help mitigate and manage these potential export control risks, as described in the following section.

3.2. Office 365 features to manage potential export control risks

The Office 365 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. For customers in North America, the Office 365 Geo framework means that customer data as described above is stored in the United States and minimizes transfer of controlled technology/technical data outside the United States. Similarly, customers in Europe and in other Geos also have information to know the places their data may be stored.[2] 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.

End-to-end encryption. In addition, Office 365 offers end-to-end encryption features that can provide customers with significant technical measures to manage and help protect against export control risks, including by taking advantage of US rules described in Section 4.6 regarding "end-to-end encryption," and assessments of the EU/UK export controls framework that lead to an analysis similar to the US rules. Data integrity between the Office 365 security boundary and a customer's security boundary is assured by encryption, and customers have

[2] https://products.office.com/en-us/where-is-your-data-located?geo+all

options in Office 365 to configure forced TLS encryption.[3] All traffic between Office 365 data centers is encrypted.[4] Office 365 deploys BitLocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in SharePoint Online and OneDrive for Business.[5] Emails within a single organization deploying Office 365 are encrypted with TLS, and traffic between an Office 365 customer and a third party deploying Office 365 are likewise encrypted.[6] Office 365 enables several customer-managed options for encrypting traffic between an Office 365 user and third parties, including Office 365 Message Encryption (which may be used to encrypt messages to any external recipient's SMTP address), Information Rights Management / Azure RMS (which encrypts content and applies usage restrictions, often within a single organization), and S/MIME (which is peer-to-peer encryption which no one, even an administrator, can view).[7] Microsoft provides detailed information about cipher suites deployed in Office 365 encryption to support a customer's determination as exporter of whether the cryptographic measures are "equally or more effective" than Federal Information Processing Standards Publication 140-2 (FIPS 140-2).[8]

For some Office 365 services, customer can choose to employ Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) options, using Azure Key Vault, in which Microsoft and its agents do not see or extract customer keys. A cloud-based key protects customer's documents and emails by using a private key for the organization that is managed by Microsoft (the default), or managed by you (the "bring your own key" or BYOK scenario). Accordingly, customers can use the keys to encrypt their own data stored and transferred in Office 365.

Tools and protocols to prevent unauthorized deemed export/reexport. 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. Again, this may not provide complete protection against inadvertent disclosure to the extent that the data does not remain encrypted at all times.

---

[3] See https://technet.microsoft.com/en-us/library/mt163898.aspx.

[4] See https://www.microsoft.com/en-us/TrustCenter/Security/Encryption and https://technet.microsoft.com/en-us/library/dn569286.aspx.

[5] See https://www.microsoft.com/en-us/TrustCenter/Security/Encryption, https://technet.microsoft.com/en-us/library/dn948533.aspx, and https://technet.microsoft.com/en-us/library/dn905447.aspx.

[6] See https://technet.microsoft.com/en-us/library/mt163898.aspx.

[7] See https://technet.microsoft.com/en-us/library/dn948533.aspx.

[8] See https://technet.microsoft.com/en-us/library/dn569286.aspx. See also https://www.microsoft.com/en-us/TrustCenter/Compliance/FIPS and https://www.microsoft.com/en-us/TrustCenter/Compliance/FedRAMP.

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—Office 365 customers' potential risk under US and EU/UK export controls. No Microsoft personnel have standing access to Customer Data stored in the Office 365 services and all access is governed by strict access control policies. Core tenets of these access control policies are Role Based Access Control (RBAC) and Just-in-time Access Controls that grant system administrator personnel the "least privilege" access to the Office 365 service that is necessary to perform specific operations. Microsoft also implements a Lockbox process under which administrators must request access for elevated privileges; if approved, they are given just-in-time accounts with high entropy passwords, access for a limited amount of time, and access to take specific actions based on a defined role.

Additionally, Microsoft offers a feature called Customer Lockbox, which is included in the Office 365 Enterprise 5 ("E5") plan and can be purchased as a separate subscription with any other Office 365 Enterprise plan. Customer Lockbox gives customers enhanced control over access by Microsoft support engineers during service operations to customer content in Exchange Online mailboxes and SharePoint Online and OneDrive for Business sites and files. In the rare instances where a Microsoft support engineer requires access to such customer content to troubleshoot and fix an issue regarding those services, Customer Lockbox allows the customer to approve or reject the access request. If the customer approves, then the engineer is able to access such customer content. Each request has an expiration time, and once the issue is resolved, the request is closed and access is revoked.

These limitations that Microsoft places on access by service operations personnel to customer data have the practical effect of reducing Office 365 customers' potential risks under US and EU/UK export controls. And importantly, Customer Lockbox gives customers an opportunity to evaluate what data may be exposed before authorizing access by Microsoft service personnel. Customers should take note, however, that these policies are not likely to completely eliminate all the export control risks. Rather, these are tools that customers can use in combination with internal procedures to help ensure full compliance.

In addition, Data Loss Prevention ("DLP") tools included in some Office 365 plans may provide ways for some customers to limit export compliance risk. These DLP tools were developed to support compliance with privacy and other regulations and to help organizations protect sensitive information from inadvertent disclosure. Where available, DLP tools allow customers to conduct searches using key words that may help identify potentially controlled technical information. Other tools allow customers to tag documents or data, as part of the document properties associated with the document in various Office 365 products, when the customer has determined the document or data is subject to export controls. That does require the customer organization to have a process, as discussed in the next section, to identify and classify controlled technical information.

DLP policies, notifications and policy tips can be customized to notify individual users that a document or data set is potentially controlled for export before it is transferred by email, upload or download; or can be set to prevent transfer without specific authorization.

Office365 GCC High. Qualifying provides qualifying US customers (including in some cases the US affiliates of non-US companies), sponsored to hold controlled, unclassified information, with assurance that sensitive export-controlled content, including defense- and military-related technical data, is stored within the continental United States with compliant infrastructure, and that access to the organization's data and other content is restricted to screened Microsoft personnel who are US citizens and have passed required background checks.

Hybrid cloud. Finally, Microsoft is ready and able to work with customers interested in a customized "hybrid solution" that uses a mix of cloud-based services and resources together with resources that are based on the customers' own premises or on a partner cloud provider's premises. Many customers may find that such hybrid solutions address the export control concerns and potential risks.

4. What are export controls?

The primary US export controls with the broadest application are the Export Administration Regulations ("**EAR"**), administered by the US Department of Commerce. The EU and UK maintain a similar export regime, which his 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 the Member States of the EU also have separate and more specialized export control regulations that govern the most sensitive items and technology. For example, the International Traffic in Arms Regulations ("**ITAR"**), administered by US Department of State, 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.

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.

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.

4.1. 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.

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

The ITAR, administered by 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 the national laws of the UK and 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.

4.3. "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."[9] "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 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

[9] 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).

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.

4.4. "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 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.

4.5. "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 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 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.

4.6. 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 EAR 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 any one of 25 designated countries.[10] On this last requirement, the EAR and ITAR 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

[10] 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, 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.

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.

Office 365. Office 365 can be configured to meet the requirement of US export control regulations that the means of decryption is not provided to any third-party, because the decryption keys or other means of decryption can be limited only to two parties – the customer and Microsoft as Office 365 cloud provider – to comply with the "end-to-end encryption" safe harbor. As explained above, 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 rule; when that customer downloads encrypted data from the Office 365 cloud to its local "security boundary," Microsoft is then the originator and the customer is the recipient.

Consistent with these safe harbor rules, Office 365 customer data is not "intentionally stored" (for purposes of the EAR safe harbor rule) in a non-conforming location. Microsoft discloses information about the location of Office 365 cloud datacenters at http://o365datacentermap.azurewebsites.net.

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 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.

4.7. EU and UK interpretations

The EU has not issued any formal rulings that address the impact of EU export controls on cloud-based computing. However, informal guidance from certain EU Member State regulators suggests an approach in the EU that would be similar to the EAR rules summarized above. In particular, 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 the UK export controls, the UK Export Control Joint Unit ("ECJU") is, as of this writing, considering proposed written guidance on technology export controls, including issues related to use of the cloud. That 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.

4.8. 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.

5. What should I do to comply with export controls when using Office 365?

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 Office 365 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 Office 365 customer—should understand the US and EU/UK export control implications of transferring data to the Office 365 cloud. In particular, Office 365 customers should consider, as discussed below, (1) whether the data is technology or technical data that is subject to US, UK, EU or Japanese export control regulation 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 Office 365 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 Office 365 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, UK, EU or Japanese military trade controls should already have in place robust procedures to identify and

properly classify such technical data to ensure compliance. Microsoft offers several Office 365 options for customers to choose depending on their risk assessment and particular needs with these military trade controls, or other specialized export control obligations, including Office 365 solutions and delivery models designed to support ITAR and other controlled data categories. One of those options is the Office365 GCC High offering available to qualified government entities as well as to non-governmental entities who handle data subject to government regulations and requirements, subject to validation of eligibility. Another option includes alternative Office 365 delivery models across the Microsoft partner ecosystem, including the hybrid solutions noted above.

Please contact your Microsoft representative to discuss available Office 365 solutions and delivery models designed to support ITAR 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 Office 365, the next step is to determine the appropriate Export Control Classification Number ("ECCN") or EU export 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, and is generally not classified as controlled technology in Japan either. 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 on its website, and by the Japanese government here.)

5.4. Take steps to comply with the EAR and EU Dual Use Regulation

For technology subject to the EAR or the EU Dual Use 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 EAR 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 Office 365 cloud, as Office 365 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 ECCNs that are controlled for reasons other than "AT," or items that fall within EU Dual Use List classifications, the Office 365 customer can consider whether the relevant ECCN/EU classification has a licensing requirement for export to one or more of the Office 365 server location(s) for the relevant Office 365 product(s) and Geo being used. As noted above, for example, for customers in North America, the Geo framework means that customer data is stored in the United States; and customers in other Geos also have information to know the places their data may be stored.

1. End-to-end encryption solutions. Customers should evaluate whether the end-to-end encryption features available for Office 365 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 provides information about Office 365 encryption to enable the customer to confirm it meets the specified NIST/FIPS 140-2 standard, or provides cryptographic measures that are "equally or more effective" than those standards; (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 Office 365 plans and the way it uses Office 365 to keep data encrypted between the customer's "security boundary" in a given country and the Office 365 data center "security boundary" (or between different Office 365 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) HYOK and BYOK options for some services give customers the ability to manage.

2. License Exceptions / General Licenses. Alternatively, or in addition, if the relevant export classification does have a licensing requirement for one or more Office 365 locations designated for the relevant Office 365 product(s) and Geo 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 also 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. Office 365 locations in the Geo do not require licensing. If the relevant export classification does not have any specific licensing requirement for any Office 365 server location designated for the relevant Office 365 product(s) and Geo being used, then export controls typically should not prevent a customer from allowing that data to be stored in or downloaded to those Office 365 locations. In light of (1) the Geo framework and Microsoft commitments to store Office 365 in the United States or in particular, known locations; (2) the end-to-end encryption deployed and configurable in Office 365 to help customers limit and control where unencrypted data is "in the clear" between in-country security boundaries; and (3) the features such as Just-in-time Access Controls and Customer Lockbox (an optional feature in some plans) 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 Office 365 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 not to place or use that data in the Office 365 cloud, and to explore other possible service delivery models. Customers may consider working with Microsoft to develop a customized "hybrid solution," with some resources "on-premises" for export-controlled data, and cloud-based resources and services for other data.

5. Office365 GCC High. Alternatively, some US customers may consider whether Microsoft's ITAR-compliant Office365 GCC High offering mentioned above may be a good solution for this technology that is subject to a higher level of EAR controls.

6. Conclusion

Not all data are subject to the export controls of the US, EU, UK or Japan, and Office 365 offers important features and tools to help customers manage export-control risks. Customers should carefully assess how their use of the Office 365 cloud may implicate export controls of these jurisdictions and determine whether any of the data they want to use or store in the Office 365 cloud may be subject to export controls, and if so, what controls apply. Where technical data subject to tighter export controls may be involved, Office 365 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 Office 365. With appropriate planning, customers can use Office 365 tools and their own internal procedures to help ensure

full compliance with US, EU, UK and Japanese export controls when using the Office 365 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 OFFICE 365 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 OFFICE 365.