Navigating your way to the cloud

A compliance checklist for financial institutions in France

Version: April 2018

Contents

Introduction: A compliance checklist for financial institutions in France	**Page 3**
Overview of the Regulatory Landscape	**Page 6**
Compliance Checklist	**Page 13**
Part 1: Key Considerations	***Page 14***
Part 2: Contract Checklist	***Page 62***
Further Information	**Back**

Introduction: A compliance checklist for financial institutions in France

Overview

Like all technological advancements, cloud computing provides substantial benefits – but it also creates a complex new environment for financial institutions to navigate. These financial institutions rightly want and expect an unprecedented level of assurance from cloud service providers before they move to the cloud.

Microsoft is committed to providing a trusted set of cloud services to financial institutions in France. Our extensive industry experience, customer understanding, research, and broad partnerships give us a valuable perspective and unique ability to deliver the assurance that our financial institutions customers need.

This checklist is part of Microsoft's commitment to financial institutions in France. We developed it to help financial institutions in France adopt Microsoft cloud services with confidence that they are meeting the applicable regulatory requirements.

What does this checklist contain?

This checklist contains:

1. an **Overview of the Regulatory Landscape**, which introduces the relevant regulatory requirements in France

2. a **Compliance Checklist,** which lists the regulatory issues that need to be addressed and maps Microsoft's cloud services against those issues; and

3. details of where you can find **Further Information**.

Who is this checklist for?

This checklist is aimed at financial institutions in France who want to use Microsoft cloud services. We use the term "financial institutions" to include banks and insurance companies regulated by the French Financial Authority (*Autorité des Marchés Financiers* (**AMF**)) and the French Prudential Authority (*Autorité de Contrôle Prudentiel et de Résolution (***ACPR**)).

What Microsoft cloud services does this checklist apply to?

This checklist applies to Microsoft Office 365, Microsoft Dynamics 365 and Microsoft Azure. You can access relevant information about each of these services at any time via the Microsoft Trust Center:

Office 365:	microsoft.com/en-us/trustcenter/cloudservices/office365
Dynamics 365:	microsoft.com/en-us/trustcenter/cloudservices/dynamics365
Azure:	microsoft.com/en-us/trustcenter/cloudservices/azure

Is it mandatory to complete the checklist?

No. In France, there is no mandatory requirement for financial institutions to complete a checklist to adopt Microsoft cloud services. However, through conversations with our many cloud customers in France, we understand that a checklist approach like this is helpful – first, as a way of understanding the regulatory requirements; second, as a way of learning more about how Microsoft cloud services can help financial institutions meet those regulatory requirements; third, as an internal framework for documenting compliance; and fourth, as a tool to streamline consultations with the regulator(s), if they are required. By reviewing and completing the checklist, financial institutions can adopt Microsoft cloud services with confidence that they are complying with the requirements in France.

The European Banking Authority (**EBA**) also produced high-level guidance for banks on cloud outsourcing in their Final Report on Recommendations on Outsourcing to Cloud Service Providers EBA/REC/2017/03 (**EBA Recommendations**). This guidance takes effect from 1 July 2018 and builds on the general outsourcing guidelines in place published by the Committee of European Banking Supervisors (**CEBS**) in 2006. Microsoft is confident that their cloud services meet the requirements set out in EBA Recommendations.

How should we use the checklist?

1. We suggest you begin by reviewing the Overview of the Regulatory Landscape in the next section. This will provide useful context for the sections that follow.

2. Having done so, we suggest that you review the questions set out in the Compliance Checklist and the information provided as a tool to measure compliance against the regulatory framework. The information in this document is provided to help you conduct your risk assessment. It is not intended to replace, or be a substitute for, the work you must perform in conducting an appropriate risk assessment but rather to aid you in that process. Additionally, there are a variety of resources Microsoft makes available to you to obtain relevant information as part of conducting your risk assessment, as well as maintaining ongoing supervision of our services. The information is accessible via the Service Trust Portal and, in particular, use of the Compliance Manager.

   Microsoft provides extensive information enabling self-service audit and due diligence on performance of risk assessments through the Compliance Manager. This includes extensive

detail on the security controls including implementation details and explanation of how the third party auditors evaluated each control. More specifically, Compliance Manager:

- **Enables customers to conduct risk assessments** of Microsoft cloud services. Combines the detailed information provided by Microsoft to auditors and regulators as part of various third-party audits of Microsoft's cloud services against various standards (such as International Organisation for Standardisation 27001:2013 and ISO 27018:2014) and information that Microsoft compiles internally for its compliance with regulations (such as the EU General Data Protection Regulation or mapping to other required controls) with the customer's own self-assessment of its organisation's compliance with applicable standards and regulations.
- **Provides customers with recommended actions** and detailed guidance to improve controls and capabilities that can help them meet regulatory requirements for areas they are responsible for.
- **Simplifies compliance workflow** and enables customers to assign, track, and record compliance and assessment-related activities, which can help an organisation cross team barriers to achieve their compliance goals. It also provides a secure repository for customers to upload and manage evidence and other artifacts related compliance activities, so that it can produce richly detailed reports in Microsoft Excel that document the compliance activities performed by Microsoft and a customer's organisation, which can be provided to auditors, regulators, and other compliance stakeholders.

3. If you need any additional support or have any questions, Microsoft's expert team is on hand to support you throughout your cloud project, right from the earliest stages of initial stakeholder engagement through to assisting in any required consultation with the regulator(s). You can also access more detailed information online, as set out in the Further Information section.

This document is intended to serve as a guidepost for customers conducting due diligence, including risk assessments, of Microsoft's Online Services. Customers are responsible for conducting appropriate due diligence, and this document does not serve as a substitute for such diligence or for a customer's risk assessment. While this paper focuses principally on Azure Core Services (referred to as "Azure"), Office 365 Services (referred to as "Office 365") and Dynamics 365 Services (referred to as "Dynamics 365"), unless otherwise specified, these principles apply equally to all Online Services as defined and referenced in the Data Processing Terms ("DPT") of Microsoft's Online Services Terms.

Overview of the Regulatory Landscape

Are cloud services permitted?	**Yes.** This means that you can consider Microsoft cloud services for the full range of use-cases across your financial institution.
Who are the relevant regulators and authorities?	The French Financial Authority (*Autorité des Marchés Financiers* (**AMF**)) and the French Prudential Authority (*Autorité de Contrôle Prudentiel et de Résolution (***ACPR**)). The AMF regulates participants and products on French financial markets, including: (i) financial markets and market infrastructures; (ii) listed companies; (iii) financial intermediaries authorised to provide investment services and financial investment advice (credit institutions authorised to provide investment services, investment firms, investment management companies, financial investment advisers, direct marketers) and; (iv) collective investment products invested in financial instruments. The ACPR is responsible for supervising the banking and insurance sectors in France and ensuring the stability of the financial system by: (i) Issuing licences and authorisations as laid down in legislation and regulations. (ii) Conducting ongoing supervision of the financial position and operating conditions of the institutions subject to its supervision, including in particular their compliance with solvency requirements and liquidity maintenance rules. The ACPR ensures that insurance institutions are in a position to honour their commitments to policyholders, members, beneficiaries and reinsured companies at all times, and that they actually honour those commitments in practice. (iii) Ensuring that reporting entities comply with the rules governing the procedures for doing business, whether they are operating by themselves or through subsidiaries, and with the rules governing acquisitions and equity investments. (iv) Supervising the preparation and implementation of

	measures to prevent and resolve banking crises, with a view to safeguarding financial stability, maintaining the continuity of the activities, services and operations of institutions whose failure would have a serious impact on the economy, protecting depositors, and avoiding, or limiting to the greatest possible extent, any recourse to public financial aid. The European Banking Authority (**EBA**). The EBA is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. The EBA recently issued a Final Report on Recommendations on Outsourcing to Cloud Services Providers which provides, for the first time, a comprehensive approach to address outsourcing of cloud computing at an EU-wide level.
What regulations and guidance are relevant?	There are several requirements and guidelines that financial institutions should be aware of when moving to the cloud: 1. Order dated 3 November 2014 relating to the internal control of banking sector, payment services, and investment services undertakings subject to the supervision of the French Prudential Authority (the "**Order**") in French; 2. The AMF General Regulation in French and in English; 3. The Monetary and Financial Code in French; 4. With respect to banking secrecy, Article L. 226-13 of the French Criminal Code, in French; Articles L.511-33, in French and L.531-12, in French of the Monetary and Financial Code (*Code monétaire et financier*). The requirement for professional secrecy prevents financial institutions from disclosing non-public information to a third party unless one of the exemptions described in the Monetary and Financial Code applies; 5. ACPR Guidelines on the risks associated with cloud computing in French and in English; 6. *Loi Informatique et Libertés* No 78-17 dated 6 January 1978, as modified by law n°2004-801 dated 6 August 2004 on information technology, data files and civil liberties (the French Data Protection Act "**French DPA**"), in French and in English, and its implementing Decree No 2005-1309 of 20 October 2005, in French and in English; 7. *Commission Nationale de l'Informatique et des Libertés'* (**CNIL**)

	recommendations for companies planning to use cloud computing services ("**CNIL Cloud Recommendations**"), in French and in English; 8. CNIL's cloud computing practical note: the 7 key steps to guarantee data confidentiality ("**CNIL Cloud Practical Note**"), in French and in English; 9. CNIL's guidelines on the security of personal data ("**CNIL Security Guidelines**"), in French; 10. CNIL's guidelines on the measures for privacy risk treatment ("**CNIL Privacy Risk Measures Guidelines**"), in French and in English; 11. CNIL's guidelines on the methodology for privacy risk management ("**CNIL Privacy Risk Management Guidelines**"), in French and in English; 12. Article 22 of the French Military Programming Act transposed in Articles L.1332-1, L.1332-2 and L.1332-6-1 and R.1332-1 of the Defence code (applicable to financial institutions which are defined as "vitally important operators") and its implementing Decree No 2015-351 dated 27 March 2015 on the security of information systems of vitally important operators (in French only); 13. Committee of European Banking Supervisors' Guidelines on Outsourcing (14 December 2006); 14. EBA's Final Report on Recommendations on Outsourcing to Cloud Service Providers EBA/REC/2017/03 (**EBA Recommendations**) (20 December 2017).
Is regulatory approval required?	The EBA Recommendations set out a regime based on notification of material outsourcing. In certain cases, outsourcing arrangements need to be notified to the AMF or the ACPR. However, it is unlikely that the categories below will apply to a financial services institution's use of Microsoft's cloud services. Categories of financial services institutions having to notify their outsourcing arrangements in case of outsourcing are the following: (i) payment institutions (*établissements de paiement*) and electronic money institutions (*établissements de monnaie électronique)* should notify the ACPR prior to the outsourcing of operational functions of: • payment services; or • issuance and management of electronic money (Article 232 of the Order dated 3 November 2014 relating to the internal control of banking sector,

	payment services, and investment services undertakings subject to the supervision of the ACPR (the "**Order**") (available in French only). (ii) asset management companies (*sociétés de gestion de portefeuille* or "AMC"), should notify the AMF when outsourcing the management of the assets of a non-professional customer, if the outsourced service provider established in a State outside of the European Economic Area: • is not certified (agréé) or registered in its country of origin to provide asset management services on behalf of third parties and is not subject to prudential control; and/or • the regulatory authority of which it depends has not entered into a cooperation agreement with the AMF (Article 313-76 of the AMF General Regulation, in French and in English). • In addition, under AMF Recommendation n°2012-19 (pages 27 and 28) asset management companies should notify their outsourcing agreements to the AMF, as part of their accreditation package, when they intend to outsource their critical tasks and functions as set out in their "activities program". However, this is an optional/voluntary notification regime because AMF Recommendation n°2012-19 is non-binding. No notice period is specified. However, the ACPR and AMF expect relevant financial services institutions to notify them at an early stage, including by communicating with them the outsourcing agreement, before entering into an outsourcing agreement. The ACPR and AMF have enforcement powers in case of failure to give this notice, when mandated by laws and regulations, including, among others, the power to impose a fine of up to EUR 100 million (ACPR: **Article L.621-39 of the Monetary and Financial Code**); or twice the amount of profits generated (AMF: Article L.621-15 of the Monetary and Financial Code). The asset management company should wait 3 months before implementing the outsourcing. In case it does not receive comments from the AMF within 3 months from the notification, the outsourcing can be implemented.
What is a "critical or important provision of services or operational tasks and functions"?	Stricter regulatory rules on outsourcing by financial institutions as listed below will apply if the outsourcing concerns a "critical or important provision of services or operational tasks and functions". This checklist assumes that these rules will apply to Microsoft's online services (in order to show the high level of compliance Microsoft's Online Services are able to achieve). "Critical or important provision of services or operational tasks and functions" are:

	(i) With respect to "asset management companies" ("**AMC**", *sociétés de gestion de portefeuille)*; Article 313-74 of the AMF General Regulation: "if a defect or failure in its performance would materially impair the asset management company's capacity for continuing compliance with the conditions and obligations of its certification or its professional obligations referred to in II of Article L. 621-15 of the Monetary and Financial Code, or its financial performance, or the continuity of its business (e.g. outsourced investment services); and (ii) Article 10 r) of Order dated 3 November 2014 relating to the internal control of banking sector, payment services, and investment services undertakings subject to the supervision of the ACPR (the "**Order**"), which provides a non-limitative list of such services, tasks and functions which **apply to undertakings subject to the Order** (which are identified in Article 1 of the Order), as: • banking services, issuance and management of electronic money services, payment services and investment services; • ancillary services as defined in the Monetary and Financial Code; • services directly allowing the provision of the services referred to in (i) or (ii) above; or • any other functions if a defect or failure in their performance would materially impair the continuing compliance of the relevant regulated entity with the conditions and obligations of its authorisation or its other obligations under the regulatory system, or its financial performance, or the soundness or the continuity of its relevant services and activities. Given the scope of these provisions, financial services institutions should assess on a case-by-case basis for themselves what constitutes a "critical or important provision of services or operational tasks and functions" in the context of their own particular business. Financial services institutions may also discuss with their competent regulator in order to determine if an outsourcing (including IT outsourcing and cloud computing outsourcing) concerns a "critical or important provision of services or operational tasks and functions".
Are transfers of data outside of France permitted?	**Yes, however restrictions apply.** The GDPR, which comes into force on 25 May 2018, allows trans-border dataflows, subject to certain restrictions. More information regarding GDPR compliance can be found here.

Are public cloud services sufficiently secure?	**Yes.** Several financial institutions in France are already using public cloud services. In fact, public cloud typically enables customers to take advantage of the most advanced security capabilities and innovations because public cloud services generally adopt those innovations first and have a much larger pool of threat intelligence data to draw upon. An example of this type of innovation in Microsoft cloud services is Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which provide a very sophisticated model to detect and mitigate previously unknown malware and provide customers with information security protections and analytics information.
Are there any mandatory terms that must be included in the contract with the services provider?	**Yes.** The Order (Article 239) and the AMF General Regulation (Article 313-75) set forth conditions that financial institutions must reflect in contractual requirements with any outsourcing service provider, including the cloud service provider. In Part 2 of the Compliance Checklist, below, we have mapped these against the sections in the Microsoft contractual documents where you will find them addressed.
How do more general French privacy laws apply to the use of cloud services by financial institutions?	The privacy regulator is the *Commission Nationale de l'Informatique et des Libertés"* ("**CNIL**"). Microsoft is committed to protect the privacy of its customers and is constantly working to help strengthen privacy and compliance protections for its customers. Not only does Microsoft have robust and industry leading security practices in place to protect its customers' data and robust data protection clauses included, as standard, in its Online Service Terms, Microsoft has gone further. Notably, Microsoft has taken two important and industry first steps to prove its commitment to privacy. First, in April 2014, the EU's 28 data protection authorities acted through their "Article 29 Working Party" to validate that Microsoft's contractual commitments meet the requirements of the EU's "model clauses". Europe's privacy regulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. For more information on this, follow this link. Second, in February 2015, Microsoft became the first major cloud provider to adopt the world's first international standard for cloud privacy, ISO/IEC 27018. The standard was developed by the International Organisation for Standardisation (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud. The British Standards Institute (BSI) has now

	independently verified that Microsoft is aligned with the standard's code of practice for the protection of Personally Identifiable Information (PII) in the public cloud. For more information on this, follow this link. Additionally, a European privacy law, the General Data Protection Regulation (**GDPR**), is due to take effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organisations that offer goods and services to people in the European Union (EU), or that collect and analyse data tied to EU residents. The GDPR applies no matter where you are located. Microsoft is committed to GDPR compliance across its cloud services and provides GDPR related assurances in its contractual commitments. Microsoft's contractual commitments with regard to the GDPR can be found in Attachment 4 to the Online Services Terms.

Compliance Checklist

How does this Compliance Checklist work?

In the **"Question/requirement"** column, we outline the regulatory requirement that needs to be addressed, based on the underlying requirements.

The questions/requirements in **grey** are not applicable in this market. However, they sometimes apply in other countries. Microsoft has included these additional questions/requiements in this table to demonstrate that Microsoft is also able to comply with them.

In the **"Guidance"** column, we explain how the use of Microsoft cloud services address the requirement. Where applicable, we also provide *guidance* as to where the underlying requirement comes from and other issues you may need to consider.

How should we use the Compliance Checklist?

Every financial institution and every cloud services project is different. We suggest that you tailor and build on the guidance provided to develop your own responses based on your financial institution and its proposed use of cloud services.

Which part(s) do we need to look at?

There are two parts to this Compliance Checklist:

- in **Part 1**, we address the key compliance considerations that apply; and

  in **Part 2**, we list the contractual terms that must be addressed and we indicate where these can be found in Microsoft's contract documents.

Part 1: Key Considerations

Who does this Part 1 apply to?

This Part 1 applies to all deployments of Microsoft cloud services (particularly, Office 365, Dynamics 365 and Azure) by financial institutions in France.

Ref.	Question / requirement	Guidance
A. OVERVIEW ***This section provides a general overview of the Microsoft cloud services.***		
1.	Who is the service provider?	*Undertakings subject to the Order: Article 231 of the Order.* *AMC: Article 313-75 II. 1° of the AMF General Regulation.* *All financial institutions: Recommendation No 5 of the CNIL Cloud Recommendations.* *EBA Recommendations – page 12 (Duty to adequately inform supervisors)* The service provider is the regional licensing entity for, and wholly-owned subsidiary of, Microsoft Corporation, a global provider of information technology devices and services, which is publicly listed in the USA (NASDAQ: MSFT). Microsoft's full company profile is available here: microsoft.com/en-us/investor/ Microsoft's Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx
2.	If the service provider is a listed company, have you reviewed its filings to the relevant authorities (e.g. the relevant stock	*AMC: Articles 313-72, 313-74 I., 313-75 I. 3° of the AMF General Regulation.* *Undertakings subject to the Order: Article 237 c) and d) of the Order.* *All financial institutions: Articles 22, 23, 24, 25 and 31 of the French DPA.*

Ref.	Question / requirement	Guidance
	exchanges or market regulators)? If yes, how is the service provider dealing with the threats and vulnerabilities it has declared in its filings?	Microsoft's filings are available via the Microsoft Investor Relations website. There are no threats or vulnerabilities relevant to the Online Services in such filings.
3.	What cloud services are you using?	Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure
4.	What activities and operations will be outsourced to the service provider? Indicate if the outsourced services are critical to your business or operations.	*Undertakings subject to the Order: Article 10 q) and r) of the Order* *AMC: Article 313-74 of the AMF General Regulation* *Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, page 15, Supervision of the service provider.* *EBA Recommendations – page 12 (Duty to adequately inform supervisors)* This Compliance Checklist is designed for financial institutions using Office 365, Dynamics 365 and/or Azure. Each service is different and there are many different options and configurations available within each service. The response below will need to be tailored depending on how you intend to use Microsoft cloud services. Your Microsoft contact can assist as needed. If using Office 365, services would typically include: • Microsoft Office applications (Outlook, Word, Excel, PowerPoint, OneNote and Access) • Exchange Online

Ref.	Question / requirement	Guidance
		• OneDrive for Business, SharePoint Online, Microsoft Teams, Yammer Enterprise • Skype for Business If using Dynamics 365, services would typically include: • Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Sales and Microsoft Social Engagement • Microsoft Dynamics 365 for Finance and Operations (Enterprise and Business Editions), Microsoft Dynamics 365 for Retail and Microsoft Dynamics 365 for Talent If using Microsoft Azure, services would typically include: • Virtual Machines, App Service, Cloud Services • Virtual Network, Azure DNS, VPN Gateway • File Storage, Disk Storage, Site Recovery • SQL Database, Machine Learning • IoT Hub, IoT Edge • Data Catalog, Data Factory, API Management • Security Center, Key Vault, Multi-Factor Authentication • Azure Blockchain Service
5.	Is the outsourcing arrangement a cloud computing arrangement?	*Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, pages 5 to 7 and 13 (fourth paragraph)* Yes.

Ref.	Question / requirement	Guidance
6.	What type of cloud services would your organisation be using?	*EBA Recommendations - page 13 (Duty to adequately inform supervisors)* If using public cloud: Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenant is isolated from each other tenants as described in section F. (Technical and Operational Risk Q&A) below. If using hybrid cloud: By using Microsoft hybrid cloud, customers can move to multi-tenant cloud at their own pace. Tenants may wish to identify the categories of data that they will store on their own servers using Windows Server virtual machines. All other categories of data will be stored in the multi-tenant cloud. Microsoft Azure, on which most Microsoft business cloud services are built, hosts multiple tenants in a highly-secure way through logical data isolation. Data storage and processing for our tenants is isolated from each other tenant as described in section F. (Technical and Operational Risk Q&A) below.
7.	What data will be processed or stored by the service provider on behalf of the financial institution? Indicate if the data is considered to be sensitive.	*All financial institutions: Articles 2, 6, 8 and 9 of the French DPA.* *All financial institutions: Recommendation No1 of the CNIL Cloud Recommendations.* *EBA Recommendations – page 12 (Duty to adequately inform supervisors)* • *You will need to tailor this section depending on what data you intend to store or process within Microsoft cloud services. The following are common categories of data that our customers choose to store and process in the Microsoft cloud services:*Customer data (including customer name, contact details, account information, payment card data, security credentials and correspondence).

Ref.	Question / requirement	Guidance
		• Employee data (including employee name, contact details, internal and external correspondence by email and other means and personal information relating to their employment with the organisation). • Transaction data (data relating to transactions in which the organisation is involved). • Indices (for example, market feeds). • Other personal and non-personal data relating to the organisation's business operations as a financial institution. Pursuant to the terms of the contract in place with Microsoft, all data is treated with the highest level of security so that you can continue to comply with your legal and regulatory obligations and your commitments to customers. You will only collect and process data that is necessary for your business operations in compliance with all applicable laws and regulation and this applies whether you process the data on your own systems or via a cloud solution.
B. OFFSHORING		
8.	Where are the data center(s) of the service provider located? Indicate the data center(s) in which your organisation's sensitive data would be stored and/or processed.	*AMC: Article 313-76 II of the AMF General Regulation* *Undertakings subject to the Order: Article 240 of the Order* *All financial institutions: Articles 5, 68 and 69 of the French DPA* Microsoft enables customers to select the region that it is provisioned from. Under the OST, Microsoft commits that if a customer provisions its tenant in the United States or EU, Microsoft will store the customer's data at rest in the United States or EU, as applicable. Microsoft is transparent in relation to the location of customer data. Microsoft data centre locations are made public on the Microsoft Trust Center. Customers have the choice to store their data solely at rest within the Europe. Further, Microsoft has now established data centers operating in France. *If using Office 365 and/or Dynamics 365:* These categories of data are described in the interactive data centres map at o365datacentermap.azurewebsites.net

<table>
<tr><th>Ref.</th><th>Question / requirement</th><th>Guidance</th></tr>
<tr><td></td><td></td><td>
If using Azure:

These categories of data are described in the interactive data centres map at: azure.microsoft.com/en-us/regions

The table below will need to be filled in depending on the specific solution that you are taking up.
<table>
<tr><th>No.</th><th>Locations of Data Centre</th><th>Classification of DC: Tier I, II, III or IV</th><th>Storing your organisation’s data (Y/N)</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>9.</td><td>What other risks have been considered in relation to the proposed offshoring arrangement?</td><td>
Undertakings subject to the Order:
- Articles 88, 89, 239 and 240 of the Order
- ACPR Guidelines on the risks associated with cloud computing, pages 14 to 16
AMC: Articles 313-60, 313-75 II 3°, 4°, 5° and 313-76 of the AMF General Regulation
Investment services providers (prestataires de services d’investissement): Article L.533-2 of the Monetary and Financial Code.
All financial institutions:
- Article 34 of the French DPA
- Recommendation No 3 of the CNIL Cloud Recommendations
- CNIL Privacy Risk Measures Guidelines
- CNIL Privacy Risk Management Guidelines
For financial institutions which are defined as “vitally important operators”: Articles L.1332-1, L.1332-2 and L.1332-6-1 and Article R.1332-1 of the Defence code and its implementing decree No 2015-351 dated 27 March 2015 on the security of information systems of vitally important operators
</td></tr>
</table>

Ref.	Question / requirement	Guidance
		EBA Recommendations – page 17 (Location of data and data processing) *The following are risk areas that our customers typically tell us are important.* **a. Political (i.e. cross-border conflict, political unrest etc.)** Our customers know where their data is hosted. The relevant jurisdictions offer stable political environments. **b. Country/socioeconomic** Microsoft's data centres are strategically located around the world, taking into account country and socioeconomic factors. The relevant locations constitute stable socioeconomic environments. **c. Infrastructure/security/terrorism** Microsoft's data centres around the world are secured to the same exacting standards, designed to protect customer data from harm and unauthorised access. This is outlined in more detail at microsoft.com/en-us/trustcenter/security. Data center access is restricted 24 hours per day by job function so that only essential personnel have access. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance and two-factor authentication. The data centers are monitored using motion sensors, video surveillance and security breach alarms **d. Environmental (i.e. earthquakes, typhoons, floods)** Microsoft data centres are built in seismically safe zones. Environmental controls have been implemented to protect the data centres including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation.

Ref.	Question / requirement	Guidance
		e. Legal Customers will have in place a binding negotiated contractual agreement with Microsoft in relation to the outsourced service, giving them direct contractual rights. Customers should also take into account that Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls and that Microsoft offers access and regulator audit rights thereby allowing customers to comply with their regulatory obligations in this respect. The terms are summarised in Part 2.
C. COMPLIANCE WITHIN YOUR ORGANISATION		
10.	Has your management considered the overall business and strategic objectives prior to outsourcing the specific IT operations? Elaborate on the factors considered and the rationale for entering this outsourcing arrangement.	*Undertakings subject to the Order: Article 237 a) of the Order* *AMC : Article 313-75 I of the AMF General Regulation* *Your management would need to have considered the overall business and strategic objectives. Your answer should cover legal/regulatory compliance and customer satisfaction but we would suggest tailoring this with details of:* • *Information about the factors considered for using the Microsoft cloud services;* • *Internal processes that were carried out;* • *Who handled the process and which areas of the business were involved or advised; and* • *Any external consultants or legal counsel involved.* References to some of the key benefits of Microsoft cloud services are described at: • Microsoft Office 365: microsoft.com/en-us/trustcenter/cloudservices/office365 • Microsoft Dynamics 365: microsoft.com/en-us/trustcenter/cloudservices/dynamics365 • Microsoft Azure: microsoft.com/en-us/trustcenter/cloudservices/azure The factors listed below may be used to prepare a business case for the use of Microsoft Online Services:

Ref.	Question / requirement	Guidance
		• Affordability. Microsoft Online Services make enterprise-class technologies available at an affordable price for small and mid-sized companies. • Security. Microsoft Online Services include extensive security to protect customer data. • Availability. Microsoft's data centres provide first-rate disaster recovery capabilities, are fully redundant, and are geographically dispersed to ensure the availability of data, thereby protecting data from natural disasters and other unforeseen complications. Microsoft also provides a financially backed guarantee of 99.9% uptime for most of its Online Services. • IT control and efficiency. Microsoft Online Services perform basic IT management tasks—such as retaining security updates and upgrading back-end systems—that allow company IT employees to focus their energy on more important business priorities. IT staff retain control over user management and service configuration. The continuous nature of Microsoft's Online Services in terms of managing updates, addressing security threats, and providing real-time improvements to the service are unmatched relative to traditional legacy private hosted cloud environments. • User familiarity and productivity. Because programs like Microsoft Office, Outlook, and SharePoint are hosted on the cloud, company employees can access information remotely from a laptop, PC, or Smartphone.
11.	Have you established and applied a set of objective, measurable service provider selection criteria? Do they cover all of the following? • the service provider's	*Undertakings subject to the Order: Article 231 of the Order* *AMC: Article 313-75 II. 1° of the AMF General Regulation* *All financial institutions: Recommendations No 2 and No 5 of the CNIL Cloud Recommendation* **a. Competence.** Microsoft is an industry leader in cloud computing. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. A list of its current certifications is available at microsoft.com/en-us/trustcenter/compliance/complianceofferings. From a

Ref.	Question / requirement	Guidance
	experience and competence (including, in particular, an assessment of its specific financial services industry credentials); • the service provider's track record and reputation; • any outstanding complaints, litigations or disputes involving the service provider in connection with services; • the service provider's staff hiring and screening processes; • the financial strength of the service provider and its parent company(ies) if applicable; and • the ability of the service provider to meet the other	risk assurance perspective, Microsoft's technical and organisational measures are designed to meet the needs of financial institutions globally. Microsoft also makes specific commitments across its Online Services in its Online Services Terms available at https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx. **b. Track-record.** Many of the world's top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe including Asia, North America, Latin America, Europe, Middle East and Africa. Key countries of adoption include, by way of example: the United States, Canada, Hong Kong, Singapore, Australia, Japan, the United Kingdom, France, Germany, Italy, Spain, the Netherlands, Poland, Belgium, Denmark, Norway, Sweden, Czech Republic, Brazil, Luxembourg, Hungary, Mexico, Chile, Peru, Argentina, South Africa, and Israel. Office 365 has grown to have over 100 million users, including some of the world's largest organisations and financial institutions. Azure continues to experience more than 90% growth, and over 80% of the largest financial institutions use or have committed to use Azure services. **c. Specific financial services credentials.** Financial institution customers in leading markets, including in the UK, France, Germany, Australia, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft cloud services meet their respective regulatory requirements. This gives customers confidence that Microsoft can help meet the high burden of financial services regulation and is experienced in meeting these requirements. **d. Financial strength of Microsoft.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalisation. Microsoft has a strong track record of stable profits. Its market capitalisation is in excess of USD $500 billion, making it one of the top three capitalised companies on the planet, Microsoft has been in the top 10 global market capitalised countries since 2000, and, indeed, is the only company in the world to consistently place in the top 10 of global market capitalised firms in the past twenty years. centre Accordingly, customers should have no concerns regarding its financial strength. **e. Business resumption and contingency plan.** Microsoft guarantees 99.9% uptime for most of its Online Services, hosted out of world class data centers, with physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, real-time issue detection and automated response such

Ref.	Question / requirement	Guidance
	requirements set out in this checklist. Please provide details.	that workloads can be moved off any failing infrastructure components with no perceptible impact on the service, 24/7 on-call engineering teams. **f. Security and internal controls, audit, reporting and monitoring.** Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organisations.
12.	Has Board approval been sought prior to signing the outsourcing agreement?	*Undertakings subject to the Order: ACPR Guidelines on the risks associated with Cloud computing, page 13 (2.5. Decision to commit to a cloud computing service).* Ultimate responsibility for effective management of risks lies with the Board and appropriate approval processes should be put in place. Each organisation will of course have its own internal approval processes. Where this does include board sign-off then this will not be an issue. Where it does not, you will need to briefly explain how the sign-off processes work (i.e. how a right of approval has effectively been delegated by the board). Again, details of the relevant decision-makers should be included here.
13.	Did you discuss this checklist with the service provider and ask them to demonstrate how they comply? Were their responses satisfactory? Please provide details.	*AMC: Article 313-75 II 1° of the AMF General Regulation* *All financial institutions: Recommendation No 5 of the CNIL Cloud Recommendations* Customers work closely with the team at Microsoft to ensure that all of the answers to the checklist are satisfactory. Microsoft assists customers in completing the checklist.
14.	What monitoring processes does the financial institution have	*Undertakings subject to the Order: Articles 237 e), 238 b) and 239 a) and g) of the Order.* *AMC: Article 313-75 II 3° of the AMF General Regulation.* *Investment services providers (prestataires de services d'investissement): Article L.533-2 of the Monetary and Financial Code.*

Ref.	Question / requirement	Guidance
	in place to manage the outsourcing and monitor the performance of the service provider? Does your organisation have a process to audit the service provider to assess its compliance with your policies, procedures, security controls and the requirements in this checklist?	*All financial services institutions: Recommendation No 2 of the CNIL Cloud Recommendations.* *Undertakings subject to the Order: Articles 234 b) and 239 f) of the Order.* *AMC: Article 313-75 II 9° of the AMF General Regulation.* *Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, page 9 (weaknesses of cloud computing in the area of control and evidence), page 11, last paragraph, page 15 (Supervision of the service provider).* *All financial services institutions:* *- CNIL Privacy Risk Measures Guidelines.* *- CNIL Privacy Risk Management Guidelines.* *- CNIL Security Guidelines.* *For financial services institutions which are defined as "vitally important operators": Articles L.1332-1, L.1332-2 and L.1332-6-1 and Article R.1332-1 of the Defence code. and its implementing decree No 2015-351 dated 27 March 2015 on the security of information systems of vitally important operators.* *The guidance below sets out certain features of Microsoft cloud services that can make monitoring easier for you. In addition, you may sign up for Premier Support, in which a designated Technical Account Manager serves as a point of contact for day-to-day management of the Microsoft cloud services and your overall relationship with Microsoft.* Microsoft provides access to "service health" dashboards (Office 365 Service Health Dashboard and Azure Status Dashboard) providing real-time and continuous updates on the status of Microsoft's Online Services. This provides your IT administrators with information about the current availability of each service or tool (and history of availability status), details about service disruption or outage and scheduled maintenance times. The information is provided online and via an RSS feed. As part of its certification requirements, Microsoft is required to undergo independent third-party auditing, and it shares with the customer the independent third party audit reports. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft gives them a right to examine, monitor and audit its provision of Microsoft cloud services. Specifically, Microsoft: (i) makes available a written data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Microsoft cloud services and other information that the customer reasonably requests regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on the customer's behalf, of the security of the computers, computing environment and physical data centres that it uses in processing their data (including personal data) for Microsoft cloud services, and provides the audit report

Ref.	Question / requirement	Guidance
		to the customer upon request. Such arrangements should provide the customer with the appropriate level of assessment of Microsoft's ability to facilitate compliance against the customer's policy, procedural, security control and regulatory requirements. The Microsoft Financial Services Amendment further gives the customer the opportunity to participate in the optional financial institution Customer Compliance Program at any time, which enables the customer to have additional monitoring, supervisory and audit rights and additional controls over Microsoft cloud services, such as (a) access to Microsoft personnel for raising questions and escalations relating to Microsoft cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results that leads to subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on the customer's use of Microsoft cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on the customer's use of Microsoft cloud services, (d) access to a summary report of the results of Microsoft's third party penetration testing against Microsoft cloud services (e.g. evidence of data isolation among tenants in the multi-tenanted services); and (e) access to Microsoft's subject matter experts through group events.
15.	Does the financial institution have access to adequate, independent information in order to appropriately monitor the cloud service provider and the effectiveness of its controls?	All customers and potential customers have access to information for monitoring the effectiveness of Microsoft's controls, including through the following online sources: • the information on the Service Trust Portal, and in particular, use of the Compliance Manager provides extensive information enabling self-service audit and due diligence; • a publicly available Trust Center for Microsoft's Online Services that includes non-confidential compliance information; • the Service Trust Platform, which provides confidential materials, such as third-party audit reports, to current customers and potential customers testing Microsoft's Online Services;

Ref.	Question / requirement	Guidance
		• a Financial Services Compliance Program, which provides access to a team of specialists in banking, insurance, asset management, and financial services treasury and remediation services; • the Azure Security Center and Office 365 Advanced Threat Analytics, which enable customers to seamlessly obtain cybersecurity-related information about Online Services deployments; • Office 365 Secure Score, which provides insight into the strength of customers' Office 365 deployment based on the customer's configuration settings compared with recommendations from Microsoft, and Azure Advisor, which enables customers to optimise their Azure resources for high availability, security, performance, and cost; • the Office 365 Service Health Dashboard and Azure Status Dashboard, which broadcast real-time information regarding the status of Microsoft's Online Services; and • Office 365 Advanced Threat Protection and the Azure Web Application Firewall, which protect customer email in real-time from cyberattacks and provide customers with information security protections and analytics information.
D. THE NEED FOR AN APPROPRIATE OUTSOURCING AGREEMENT ***Note: See also Part 2 of this Compliance Checklist for a list of the standard contractual terms that the regulator(s) expects to be included in the outsourcing agreement and how these are addressed by the Microsoft contractual documents.***		
16.	Does the outsourcing agreement include a clause that allows the regulator(s) to access documentation and information relating to	*EBA Recommendations – page 15 (Access and audit rights)* Yes. There are terms in the contract that enable the regulator(s)to carry out inspection or examination of Microsoft's facilities, systems, processes and data relating to the services. As part of the Financial Services Amendment that Microsoft offers to regulated financial services institutions, Microsoft will, upon a regulator's request, provide the regulator a direct right to examine the relevant service, including the ability to conduct an on-premises examination; to meet with Microsoft personnel and Microsoft's external auditors; and to access related information, records, reports and documents. Under the outsourcing

Ref.	Question / requirement	Guidance
	the outsourcing arrangement?	agreement, Microsoft commits that it will not disclose customer data to the regulator except as required by law or at the direction or consent of the customer.
17.	Does the outsourcing agreement provide a guarantee of access to the minimum IT assets required to operate under a disaster scenario?	Yes. The uptime guarantee given by Microsoft applies to all IT assets, not just a minimum number required to operate in a disaster situation. Microsoft guarantees 99.9% of uptime for most of its Online Services. Uptime guarantees are set forth in Microsoft's contracts with its customers, and if service levels are not maintained, customers may be eligible for a credit towards a portion of their monthly service fees. For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.
18.	Is the outsourcing agreement sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in the future to meet changing circumstances?	Yes. The customer can always order additional services if required. The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
19.	In the event of termination, do transitional arrangements address access to, and ownership of, documents, records, software and hardware, and the role of the	Yes. Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service.

Ref.	Question / requirement	Guidance
	service provider in transitioning the service?	Ownership of documents, records and other data remain with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft.
E. SUBCONTRACTORS		
20.	Does the service provider use subcontractors?	*All financial institutions: Article 35 of the French DPA.* Microsoft permits the use of subcontractors.
21.	Please provide a list of any subcontractors used by the service provider and confirm that: a) the service provider has controls in place to ensure that its subcontractors agree to equivalent commitments to those that the service provider agrees to; and b) the agreement requires the service provider to take overall responsibility	*Undertakings subject to the Order: Article 237 of the Order.* *AMC: Article 313-75 of the AMF General Regulation.* *All financial institutionsIs: Article 35 of the French DPA.* Microsoft commits that its subcontractors will be permitted to obtain customer data only to deliver the services Microsoft has retained them to provide and will be prohibited from using customer data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST. To ensure subcontractor accountability, Microsoft requires all of its vendors that handle customer personal information to join the Microsoft Supplier Security and Privacy Assurance Program, which is an initiative designed to standardise and strengthen the handling of customer personal information, and to bring vendor business processes and systems into compliance with those of Microsoft. For more information regarding Microsoft's Supplier Security and Privacy Program, see https://www.microsoft.com/en-us/procurement/msp-requirements.aspx.

Ref.	Question / requirement	Guidance
	for the performance of subcontractors.	Microsoft will enter into a written agreement with any subcontractor to which Microsoft transfers customer data that is no less protective than the data processing terms in the customer's contracts with Microsoft (DPT, see OST, page 11). In addition, Microsoft's ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft. Microsoft's ISO 27001 certification provides a layer of additional controls that impose stringent requirements on Microsoft's subcontractors to comply fully with Microsoft's privacy, security, and other commitments to its customers, including requirements for handling sensitive data, background checks, and non-disclosure agreements. Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorising any new subcontractor to access customer data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected cloud computing service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent customer invoices. (DPT, see OST, page 11)
F. TECHNICAL AND OPERATIONAL RISK Q&A ***This section provides some more detailed technical and operational information about Microsoft cloud services which should address many of the technical and operational questions that may arise. If other questions arise, please do not hesitate to get in touch with your Microsoft contact.***		
22.	Are the following physical and environmental controls available at the data center(s)? • Physical access controls such as	*All financial institutions:* - *Articles 34 and 35 of the French DPA* - *CNIL Privacy Risk Measures Guidelines* - *CNIL Security Guidelines* Microsoft has all the stated controls in place.

Ref.	Question / requirement	Guidance
	locked doors, access cards, biometrics access, etc., proper approval sought for visitors to gain access to the data center • Visitors escorted by staff • Records of visitor's activities • Systems and network equipment locked up in cabinet • Uninterruptible power supply • Air conditioning system • Temperature sensor • Fire detector • Smoke detector • Water sprinkler (dry-piped or wet-piped) • FM200 or other fire suppression system • Raised floor • CCTV	
23.	Have you obtained from the service provider a written undertaking to	*Undertakings subject to the Order: Article 239 b) of the Order.* *AMC: Article 313-75 10° of the AMF General Regulation.* *All financial institutions:* *- Article L. 226-13 of the French Criminal Code, Articles L.511-33, and L.531-12 of the Monetary and Financial Code.*

Ref.	Question / requirement	Guidance
	protect and maintain the confidentiality of your sensitive data?	- *Article 35 of the French DPA.* "Confidentiality agreements and non-disclosure agreements" are covered under the ISO/IEC 27001 standard against which Microsoft is certified. MBSA Section 3 deals with confidentiality. Under this section Microsoft commits not to disclose your confidential information (which includes your data) to third parties and to only use your confidential information for the purposes of Microsoft's business relationship with you. Further, Microsoft commits to take reasonable steps to protect your confidential information, to notify you if there is any unauthorised use or disclosure of your confidential information and to cooperate with you to help to regain control of your confidential information and prevent further unauthorised use or disclosure of it. The OST states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment and the OST. Microsoft makes specific commitments with respect to safeguarding your data in the OST. In summary, Microsoft commits that: 1. Your data will only be used to provide the online services to you and your data will not be used for any other purposes, including for advertising or similar commercial purposes. 2. Microsoft will not disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. 3. Microsoft will implement and maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. Technical support personnel are only permitted to have access to customer information when needed.

Ref.	Question / requirement	Guidance
24.	Does the service provider permit audit by the financial institution and/or the regulator(s)?	*Undertakings subject to the Order: Article 239 f) of the Order.* *AMC: Articles 313-75 II 8° and 9° of the AMF General Regulation.* *Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, page 9 (weaknesses of cloud computing in the area of control and evidence), page 11, last paragraph, page 15 (Supervision of the service provider).* *Undertakings subject to the Order: Article 239 h) of the Order.* *Undertakings subject to the Order: Article R 612-26 of the Monetary and Financial Code.* *AMC: Article 313-75 II 8° and 9° of the AMF General Regulation.* *Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, page 15 (Supervision of the service provider).* Yes. Pursuant to the Financial Services Amendment, Microsoft provides the regulator(s) with a direct right to examine the Online Services, including the ability to conduct an on-premise examination, to meet with Microsoft personnel and Microsoft's external auditors, and to access any related information, records, reports and documents, in the event that the regulator(s) requests to examine the Online Services operations in order to meet their supervisory obligations. Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centres that it uses in processing customer data for each Online Service. Customers may also participate in the optional Customer Compliance Program to have additional monitoring, supervisory and audit rights and additional controls over the Online Services. The Customer Compliance Program, which is a for-fee program allows customers to (a) to evaluate the services provided and (b) to review Microsoft's internal control environment. Specifically, this compliance program facilitates our ability to (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.

Ref.	Question / requirement	Guidance
25.	Are the provider's services subject to any third party audit?	Yes. Microsoft's cloud services are subject to regular independent third party audits, including SSAE16 SOC1 Type II, SSAE SOC2 Type II, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27018 as part of Microsoft's certification requirements. Microsoft will also make available the ISO/IEC 27001 audit report.
26.	Has your organisation performed a risk assessment of this outsourcing arrangement, including security risk assessment against the latest security threats? Please elaborate the key risks and threats that have been identified for this outsourcing arrangement and the actions that have been or will be taken to address them.	*Undertakings subject to the Order: Articles 88, 89, 239 of the Order and ACPR Guidelines on the risks associated with cloud computing, pages 14 to 16.* *AMC: Article 313-75 II 3°, 4°, 5° of the AMF General Regulation* *Investment service provider (prestataire de services d'investissement): Article L.533-2 of the Monetary and Financial Code* *All financial services institutions:* - *Article 34 of the French DPA.* - *Recommendation No 3 of the CNIL Cloud Recommendations.* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Privacy Risk Management Guidelines.* *For financial institutions which are defined as "vitally important operators": Articles L.1332-1, L.1332-2 and L.1332-6-1 and Article R.1332-1 of the Defence code and its implementing decree No 2015-351 dated 27 March 2015 on the security of information systems of vitally important operators.* *EBA Recommendations - page 16 (Security of data and systems)* When a financial services customer chooses Microsoft cloud services, we help them to assess the relevant risks and make available a wide range of resources to facilitate the customer's due diligence as available in the Trust Center. You should ensure that you have carried out comprehensive due diligence on the nature, scope and complexity of the outsourcing to identify the key risks and risk mitigation strategies. We have made suggestions regarding common issues below and you will need to expand on our guidance to describe what you see as the key risks and what risk processes you have carried out as part of this project. • identify the role of outsourcing in the overall business strategy and objectives of the institution;

Ref.	Question / requirement	Guidance
		• risk identification; • analysis and quantification of the potential impact and consequences of these risks; • risk mitigation and control strategy; and • ongoing risk monitoring and reporting. If you have any questions when putting together a risk assessment, please do not hesitate to get in touch with your Microsoft contact. The following should be considered in your risk assessment: **1. Data security**: By transferring certain data processing operations to a third party, customers should be aware that they need to ensure that their selected outsourcing partner has in place appropriate and reasonable technical and organisational measures to protect the data. This is necessary both from a financial services regulatory perspective as well as the organisation's compliance with data protection legislation. This should be of utmost importance to customers and therefore they should carry out a robust assessment as part of their selection process. Customers that select Microsoft as an outsourcing partner take heavily into account the fact that it is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centres of even the most sophisticated organisations. Microsoft is ISO/IEC 27001 and ISO/IEC 27018 accredited. The Microsoft cloud services security features (being the product that the organisation will be using) consist of three parts: (a) built-in security features including encryption of data when in transit and at rest; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data. **2. Access and audit**: In addition to ensuring that relevant security and other safeguards are put in place up front, it is essential that the outsourcing arrangement provides for customers to ensure that such standards and commitments and regulatory requirements are adhered to in practice. Customers should be aware that audit and access in order to verify this can be a difficult issue in outsourcing and therefore should make this a high priority requirement as part of their outsourcing. Another

Ref.	Question / requirement	Guidance
		reason for the selection of Microsoft in this case is that it permits regulator audit and inspection of its data centres and in agreed circumstances inspection rights for its financial services customers. **3. Control**: The handing over of a certain amount of day to day responsibility to an outsourcing provider does present certain challenges in relation to control of data. What is essential to customers is that despite the outsourcing they retain control over their own business operations, including control of who can access data and how they can use it. At a contractual level, customer would have dealt with this via their agreement with Microsoft, which provides them with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies. At a practical level, customers select Microsoft cloud services because they provide customers with control over data location, access and authentication and advanced encryption controls. Customers continue to own and retain all rights to their data and their data will not be used for any purpose other than to provide them with the Microsoft cloud services. The following is a summary of the factors that our customers typically tell us are important when addressing the issue of counterparty risk: **g. Competence.** Microsoft is an industry leader in cloud computing. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider. A list of its current certifications is available at https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings. From a risk assurance perspective, Microsoft's technical and organisational measures are designed to meet the needs of financial institutions globally. Microsoft also makes specific commitments across its Online Services in its Online Services Terms available at https://www.microsoft.com/en-sg/Licensing/product-licensing/products.aspx. **h. Track-record.** Many of the world's top companies use Microsoft cloud services. There are various case studies relating to the use of Microsoft cloud services at customers.microsoft.com. Customers have obtained regulatory approvals (when required) and are using Online Services in all regions of the globe including Asia, North America, Latin America, Europe, Middle East and Africa. Key countries of adoption include, by way of example: the United States, Canada, Hong Kong, Singapore, Australia, Japan, the United Kingdom, France, Germany, Italy, Spain, the Netherlands, Poland, Belgium, Denmark, Norway, Sweden, Czech Republic, Brazil, Luxembourg, Hungary, Mexico, Chile, Peru, Argentina, South Africa,

Ref.	Question / requirement	Guidance
		and Israel. Office 365 has grown to have over 100 million users, including some of the world's largest organisations and financial institutions. Azure continues to experience more than 90% growth, and over 80% of the largest financial institutions use or have committed to use Azure services. i. **Specific financial services credentials.** Financial institution customers in leading markets, including in the UK, France, Germany, Australia, Singapore, Canada, the United States and many other countries have performed their due diligence and, working with their regulators, are satisfied that Microsoft cloud services meet their respective regulatory requirements. This gives customers confidence that Microsoft can help meet the high burden of financial services regulation and is experienced in meeting these requirements. j. **Financial strength of Microsoft.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalisation. Microsoft has a strong track record of stable profits. Its market capitalisation is in excess of USD $500 billion, making it one of the top three capitalised companies on the planet, Microsoft has been in the top 10 global market capitalised companies since 2000, and, indeed, is the only company in the world to consistently place in the top 10 of global market capitalised firms in the past twenty years. Its full company profile is available here: microsoft.com/en-us/investor/ and its Annual Reports are available here: microsoft.com/en-us/Investor/annual-reports.aspx. Accordingly, customers should have no concerns regarding its financial strength. We can provide resources and information to our customers to assist them in documenting their assessment.
27.	What security controls are in place to protect the transmission and storage of confidential information such as customer data within the infrastructure of the service provider?	*Undertakings subject to the Order: Article 239 b) of the Order.* *AMC: Articles 313-60 and 313-75 II 10° of the AMF General Regulation.* *All financial institutions: Articles 2, 3 I., 6, 8, 9, 34, 35 of the French DPA.* *All financial institutions: Article 226-17 of the French Criminal Code.* *Credit institutions (établissements de credit) : Article L.611-1 10° of the Monetary and Financial Code.* *Payment services providers (prestataires de services de paiement): L.133-15 and L133-4 of the Monetary and Financial Code.* *All financial institutions: Recommendation No 3 of the CNIL Cloud Recommendations.*

Ref.	Question / requirement	Guidance
		Microsoft as an outsourcing partner is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centres of even the most sophisticated organisations. Microsoft cloud services were built based on ISO/IEC 27001 and ISO/IEC 27018 standards, a rigorous set of global standards covering physical, logical, process and management controls. The Microsoft cloud services security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data. Microsoft implements the Microsoft Security Development Lifecycle (SDL) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft cloud services. Through design requirements, analysis of attack surface and threat modelling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. Networks within Microsoft's data centres are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data centre. These connections are encrypted using industry-standard transport layer security TLS. The use of TLS establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data centre. Customers can configure TLS between Microsoft cloud services and external servers for both inbound and outbound email. This feature is enabled by default. Microsoft also implements traffic throttling to prevent denial-of-service attacks. It uses the "prevent, detect and mitigate breach" process as a defensive strategy to predict and prevent security breaches before they happen. This involves continuous improvements to built-in security features, including port-scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS detection and prevention and multi-factor authentication for service access. Use of a strong password is enforced as mandatory, and the password must be changed on a regular

Ref.	Question / requirement	Guidance
		basis. From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, “Just-In-Time (JIT) access and elevation” (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and isolation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process. Preventing breach also involves automatically deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. Data is also encrypted. Customer data in Microsoft cloud services exists in two states: • at rest on storage media; and • in transit from a data centre over a network to a customer device. Microsoft offers a range of built-in encryption capabilities to help protect data at rest. • For Office 365, Microsoft follows industry cryptographic standards such as TLS/SSL and AES to protect the confidentiality and integrity of customer data. For data in transit, all customer-facing servers negotiate a secure session by using TLS/SSL with client machines to secure the customer data. For data at rest, 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. Additionally, in some scenarios, Microsoft uses file-level encryption. • For Azure, technological safeguards such as encrypted communications and operational processes help keep customers’ data secure. Microsoft also provides customers the flexibility to implement additional encryption and manage their own keys. For data in transit, Azure uses industry-standard secure transport protocols, such as TLS/SSL, between user devices and Microsoft data centres. For data at rest, Azure offers many encryption options,

Ref.	Question / requirement	Guidance
		such as support for AES-256, giving customers the flexibility to choose the data storage scenario that best meets the customer's needs. Such policies and procedures are available through Microsoft's online resources, including the Trust Center and the Service Trust Platform.
28.	How is the financial institution's data isolated and identified from other sensitive data held by the service provider? Are the outsourced operations using hardware (i.e. servers/network devices) dedicated to the organisation?	*All financial institutions: Articles 2 and 25 I. 5° of the French DPA* *Undertakings subject to the Order: Article 239 b) of the Order.* *AMC: Article 313-75 10° of the AMF General Regulation.* *All financial services institutions:* - *Article L. 226-13 of the French Criminal Code, Articles L.511-33, and L.531-12 of the Monetary and Financial Code.* *Article 35 of the French DPA* *All financial institutions: Recommendation No 4 of the CNIL Cloud Recommendations.* *Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, pages 5, 6 and 7 (Paragraphs 1.1. and 1.2).* Microsoft cloud services are multi-tenant services (that is, data from different customers shares the same hardware resources) but they are designed to host multiple tenants in a highly secure way through data isolation. For all of its Online Services, Microsoft logically isolates customer data from the other data Microsoft holds. Data storage and processing for each tenant is separated through an "Active Directory" structure, which isolates customers using security boundaries ("silos"). The silos safeguard customer data such that the data cannot be accessed or compromised by co-tenants. If using Office 365 dedicated version, customers will have secured a dedicated hosted offering, which means that their data is hosted on hardware dedicated to them.

Ref.	Question / requirement	Guidance
29.	How are the service provider's access logs monitored?	Microsoft provides monitoring and logging technologies to give its customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity. An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems.
30.	What policies does the service provider have in place to monitor employees with access to confidential information?	For certain core services of Office 365 and Azure, personnel (including employees and subcontractors) with access to customer data content are subject to background screening, security training, and access approvals as allowed by applicable law. Background screening takes place before Microsoft authorises the employee to access customer data. To the extent permitted by law, any criminal history involving dishonesty, breach of trust, money laundering, or job-related material misrepresentation, falsification, or omission of fact may disqualify a candidate from employment, or, if the individual has commenced employment, may result in termination of employment at a later day.
31.	How are customers authenticated?	Microsoft cloud services use two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
32.	What are the procedures for	*Undertakings subject to the Order: Article 239 g) of the Order.*

Ref.	Question / requirement	Guidance
	identifying, reporting and responding to suspected security incidents and violations?	*For asset management companies: Article 313-75 II 6° of the AMF General Regulation.* *All financial institutions:* - *Articles 34, 34 prime (only if the service provider is an electronic communications operator, notification requirements to the CNIL apply) and 35 of the French DPA.* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines.* - *CNIL Privacy Risk Management Guidelines.* First, there are robust procedures offered by Microsoft that enable the **prevention** of security incidents and violations arising in the first place and **detection** if they do occur. Specifically: a. Microsoft implements 24 hour monitored physical hardware. Data centre access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. b. Microsoft implements "prevent, detect, and mitigate breach", which is a defensive strategy aimed at predicting and preventing a security breach before it happens. This involves continuous improvements to built-in security features, including port scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS (distributed denial-of-service) detection and prevention, and multi-factor authentication for service access. In addition, Microsoft has anti-malware controls to help avoid malicious software from gaining unauthorised access to customer data. Microsoft implements traffic throttling to prevent denial-of-service attacks, and maintains a set of Security Rules for managed code to help ensure that application cybersecurity threats are detected and mitigated before the code is deployed. c. Microsoft employs some of the world's top experts in cybersecurity, cloud compliance, and financial services regulation. Its Digital Crimes Unit, for example, employs cyber experts, many of whom previously worked for law enforcement, to use the most advanced tools to detect, protect, and respond to cybercriminals. Its Cyber Defense Operations Center brings

Ref.	Question / requirement	Guidance
		together security response experts from across Microsoft to help protect, detect, and respond 24/7 to security threats against Microsoft's infrastructure and Online Services in real-time. General information on cybersecurity can be found here. d. Microsoft conducts a risk assessment for Azure at least annually to identify internal and external threats and associated vulnerabilities in the Azure environment. Information is gathered from numerous data sources within Microsoft through interviews, workshops, documentation review, and analysis of empirical data. The assessment follows a documented process to produce consistent, valid, and comparable results year over year. e. Wherever possible, human intervention is replaced by an automated, tool-based process, including routine functions such as deployment, debugging, diagnostic collection, and restarting services. Microsoft continues to invest in systems automation that helps identify abnormal and suspicious behaviour and respond quickly to mitigate security risk. Microsoft is continuously developing a highly effective system of automated patch deployment that generates and deploys solutions to problems identified by the monitoring systems—all without human intervention. This greatly enhances the security and agility of the service. f. Microsoft allows customers to monitor security threats on their server by providing access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources. g. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. Microsoft conducts a thorough review of all information security incidents. h. Microsoft conducts penetration tests to enable continuous improvement of incident response procedures. These internal tests help Microsoft cloud services security experts create a methodical, repeatable, and optimised stepwise response process and automation. In addition, Microsoft provides customers with the ability to conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing.

Ref.	Question / requirement	Guidance
		Second, if a security incident or violation is detected, Microsoft Customer Service and Support notifies customers by updating the Service Health Dashboard. Customers would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides Recovery Time Objective (RTO) commitments. These differ depending on the applicable Microsoft service and are outlined further below. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: • An incident summary and event timeline. • Broad customer impact and root cause analysis. • Actions being taken for continuous improvement. If the customer is affected by a service incident, Microsoft shares the post-incident review with them. Microsoft's commitment to cybersecurity and data privacy, including restrictions on access to customer data, are set forth in Microsoft's contracts with customers. In summary: • *Logical Isolation*. Microsoft logically isolates customer data from the other data Microsoft holds. This isolation safeguards customers' data such that the data cannot be accessed or compromised by co-tenants. • *24-Hour Monitoring & Review of Information Security Incidents*. Microsoft maintains 24-hour monitoring of its Online Services and records all security breaches. Microsoft conducts a thorough review of all information security incidents. For security breaches resulting in unlawful or unauthorised access to Microsoft's equipment, facilities, or customer data, Microsoft notifies affected parties without unreasonable delay. For more information regarding Microsoft's security incident management, refer to http://aka.ms/SecurityResponsepaper. • *Minimising Service Disruptions—Redundancy*. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, Network Interface Card ("NIC"), power supply, and server levels;

Ref.	Question / requirement	Guidance
		constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. • *Resiliency*. Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. • *Distributed Services*. Microsoft offers distributed component services to limit the scope and impact of any failures of a single component, and directory data is replicated across component services to insulate one service from another in the event of a failure. • *Simplification*. Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. • *Human Backup*. Microsoft's Online Services include automated recovery actions with 24/7 on-call support; a team with diverse skills on call to provide rapid response and resolution; and continuous improvement through learning from the on-call teams. • *Disaster Recovery Tests*. Microsoft conducts disaster recovery tests at least once per year. Customers also have access to the Azure Security Center, Office 365 Advanced Threat Analytics, Azure Status Dashboard, and the Office 365 Service Health Dashboard, among other online resources, which allow customers to monitor security threats on the cloud service provider's server.
33.	How is end-to-end application encryption security implemented to protect PINs and other	*Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, pages 11 and 15.* *All financial institutions:* - *CNIL Privacy Risk Measures Guidelines.*

Ref.	Question / requirement	Guidance
	sensitive data transmitted between terminals and hosts?	- *CNIL Privacy Risk Management Guidelines.* - *CNIL Security Guidelines.* *For financial institutions which are defined as "vitally important operators": Articles L.1332-1, L.1332-2 and L.1332-6-1 and Article R.1332-1 of the Defence code. and its implementing decree No 2015-351 dated 27 March 2015 on the security of information systems of vitally important operators* Microsoft cloud services use industry-standard secure transport protocols for data as it moves through a network—whether between user devices and Microsoft data centres or within data centres themselves. To help protect data at rest, Microsoft offers a range of built-in encryption capabilities. There are three key aspects to Microsoft's encryption: 1. **Secure identity:** Identity (of a user, computer, or both) is a key element in many encryption technologies. For example, in public key (asymmetric) cryptography, a key pair—consisting of a public and a private key—is issued to each user. Because only the owner of the key pair has access to the private key, the use of that key identifies the associated owner as a party to the encryption/decryption process. Microsoft Public Key Infrastructure is based on certificates that verify the identity of users and computers. 2. **Secure infrastructure:** 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 unauthorised access to our data. Proper key management is an essential element in encryption best practices, and Microsoft helps ensure that encryption keys are properly secured. Protocols and technologies examples include: a. Transport Layer Security (TLS), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network. b. Internet Protocol Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it's transferred across the network. c. Office 365 servers using BitLocker to encrypt the disk drives containing log files and customer data at rest at the volume-level. BitLocker encryption is a data protection feature built into Windows to safeguard against

Ref.	Question / requirement	Guidance
		threats caused by lapses in controls (e.g., access control or recycling of hardware) that could lead to someone gaining physical access to disks containing customer data. d. BitLocker deployed with Advanced Encryption Standard (AES) 256-bit encryption on disks containing customer data in Exchange Online, SharePoint Online, and Skype for Business. Advanced Encryption Standard (AES)-256 is the National Institute of Standards and Technology (NIST) specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology. e. BitLocker encryption that uses AES to encrypt entire volumes on Windows server and client machines, which can be used to encrypt Hyper-V virtual machines when a virtual Trusted Platform Module (TPM) is added. BitLocker also encrypts Shielded VMs in Windows Server 2016, to ensure that fabric administrators cannot access the information inside the virtual machine. The Shielded VMs solution includes the Host Guardian Service feature, which is used for virtualization host attestation and encryption key release. f. Office 365 offers service-level encryption in Exchange Online, Skype for Business, SharePoint Online, and OneDrive for Business with two key management options—Microsoft managed and Customer Key. Customer Key is built on service encryption and enables customers to provide and control keys that are used to encrypt their data at rest in Office 365. g. Microsoft Azure Storage Service Encryption encrypts data at rest when it is stored in Azure Blob storage. Azure Disk Encryption encrypts Windows and Linux infrastructure as a service (IaaS) virtual machine disks by using the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the operating system and the data disk. h. Transparent Data Encryption (TDE) encrypts data at rest when it is stored in an Azure SQL database. i. Azure Key Vault helps easily and cost-effectively manage and maintain control of the encryption keys used by cloud apps and services via a FIPS 140-2 certified cloud based hardware security module (HSM). j. Microsoft Online Services also transport and store secure/multipurpose Internet mail extensions (S/MIME) messages and transport and store messages that are encrypted using client-side, third-party encryption solutions such as Pretty Good Privacy (PGP). 3. **Secure apps and data:** The specific controls for each Microsoft cloud service are described in more detail at microsoft.com/en-us/trustcenter/security/encryption.

Ref.	Question / requirement	Guidance
34.	Are there procedures established to securely destroy or remove the data when the need arises (for example, when the contract terminates)?	*Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing, page 14.* *All financial institutions:* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines.* - *Recommendation No 2 of the CNIL Cloud Recommendations.* Yes. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2 compliant. For hard drives that cannot be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft online services utilise approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. In its contracts with customers, Microsoft commits to disabling a customer's account and deleting customer data from the account no more than 180 days after the expiration or termination of the Online Service. "Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standards against which Microsoft is certified.
35.	Are there documented security procedures for safeguarding premises and restricted areas? If yes, provide descriptions of these procedures.	*All financial institutions:* - *Articles 34 and 35 of the French DPA.* - *CNIL Privacy Risk Measures Guidelines.CNIL Security Guidelines.* - *Recommendation No 6 of the CNIL Cloud Recommendations.*

Ref.	Question / requirement	Guidance
		The security procedures for safeguarding hardware, software and security are documented by Microsoft in its Standard Response to Request for Information – Security and Privacy. This confirms how the following aspects of Microsoft's operations safeguard hardware, software and data: a. Compliance b. Data Governance c. Facility d. Human Resources e. Information Security f. Legal g. Operations h. Risk Management i. Release Management j. Resiliency k. Security Architecture Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance and two-factor authentication. The data centres are monitored using motion sensors, video surveillance and security breach alarms.
36.	Are there documented security procedures for safeguarding hardware, software and data in the data centre?	Yes. These are described at length in the Microsoft Trust Center at microsoft.com/trust. For information on: • design and operational security see https://www.microsoft.com/en-us/trustcenter/security/designopsecurity • network security see https://www.microsoft.com/en-us/trustcenter/security/networksecurity • encryption see https://www.microsoft.com/en-us/trustcenter/security/encryption

Ref.	Question / requirement	Guidance
		• threat management see https://www.microsoft.com/en-us/trustcenter/security/threatmanagement identify and access management see https://www.microsoft.com/en-us/trustcenter/security/identity
37.	How are privileged system administration accounts managed? Describe the procedures governing the issuance (including emergency usage), protection, maintenance and destruction of these accounts. Please describe how the privileged accounts are subjected to dual control (e.g. password is split into 2 halves and each given to a different staff for custody).	Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity. Microsoft provides monitoring and logging technologies to give customers maximum visibility into the activity on their cloud-based network, applications, and devices, so they can identify potential security gaps. The Online Services contain features that enable customers to restrict and monitor their employees' access to the services, including the Azure AD Privileged Identify Management system and Multi-Factor Authentication. Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorisation granted or denied, and relevant activity (see Online Services Terms, page 13). An internal, independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. Microsoft provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to

Ref.	Question / requirement	Guidance
		such information, and Azure Monitor, which provides activity logs and diagnostic logs that customers can use to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In emergency situations, a "JIT (as defined above) access and elevation system" is used (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service.
38.	Are the activities of privileged accounts captured (e.g. system audit logs) and reviewed regularly? Indicate the party reviewing the logs and the review frequency.	*All financial institutions:* - *Articles 34, 34 prime (only if the service provider is an electronic communications operator, notification requirements to the CNIL apply) and 35 of the French DPA.* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines.* *CNIL Privacy Risk Management Guidelines* Yes. An internal, independent Microsoft team will audit the log at least once per quarter. More information is available at microsoft.com/en-us/trustcenter/security/auditingandlogging.
39.	Are the audit/activity logs protected against tampering by users with privileged accounts? Describe the safeguards implemented.	*All financial institutions:* - *Articles 34, 34 prime (only if the service provider is an electronic communications operator, notification requirements to the CNIL apply) and 35 of the French DPA.* - *CNIL Privacy Risk Measures Guidelines* - *CNIL Security Guidelines.* - *CNIL Privacy Risk Management Guidelines.* *.* Microsoft logs, or enables customers to log, access and use of information systems containing customer data, registering the access ID, time, authorization granted or denied, and relevant activity (see Online Services Terms, page 13). An internal,

Ref.	Question / requirement	Guidance
		independent Microsoft team audits the log at least once per quarter, and customers have access to such audit logs. In addition, Microsoft periodically reviews access levels to ensure that only users with appropriate business justification have access to appropriate systems. All logs are saved to the log management system which a different team of administrators manages. All logs are automatically transferred from the production systems to the log management system in a secure manner and stored in a tamper-protected way.
40.	Does the service provider have privileged access or remote access to perform system/user administration for the outsourced service? If so, does the service provider have access to your organisation's sensitive data? Please provide details on the controls implemented to mitigate the risks of unauthorised access to sensitive data by the service provider, or other parties	*Undertakings subject to the Order: Article 239 b) of the Order.* *AMC: Article 313-75 10° of the AMF General Regulation.* *All financial institutions:* - *Article L. 226-13 of the French Criminal Code, Articles L.511-33, and L.531-12 of the Monetary and Financial Code.* - *Articles 34 and 35 of the French DPA.* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines.* - *CNIL Privacy Risk Management Guidelines.* Administrators who have rights to applications have no physical access to the production systems. So administrators have to securely access the applications remotely via a controlled, and monitored remote process called lockbox. All operations through this remote access facility are logged. Further, Microsoft applies strict controls over access to customer data. Access to the IT systems that store customer data is strictly controlled via role-based access control (RBAC) and lock box processes. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, required security training, and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements. In addition, the Online Services include built-in approved Windows

Ref.	Question / requirement	Guidance
		PowerShell Scripts, which minimise the access rights needed and the surface area available for misconfiguration. In emergency situations, a "Just-In-Time (JET) access and elevation system" is used (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) for engineer privileges to troubleshoot the service. For more information regarding Microsoft identity and access management, see https://www.microsoft.com/en-us/trustcenter/security/identity.
41.	Does the service provider have a disaster recovery or business continuity plan? Have you considered any dependencies between the plan(s) and those of your financial institution?	*Undertakings subject to the Order: Articles 89, 100, 102, 215, 239 and 253 of the Order.* *AMC: Article 313-56 of the AMF General Regulation.* *All financial institutions:* - *ACPR Guidelines on the risks associated with cloud computing, pages 11, 12 and 15.* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines.* Yes. Microsoft makes every effort to minimise service disruptions, including by implementing physical redundancies at the disk, NIC, power supply, and server levels; constant content replication; robust backup, restoration, and failover capabilities; and real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service. Microsoft also maintains 24/7 on-call engineering teams for assistance. See Financial Services Compliance Program and Premier Support; see also Office 365 Support; Premier Support for Enterprise; and Azure Support Plans. • *Redundancy*. Microsoft maintains physical redundancy at the server, data centre, and service levels; data redundancy with robust failover capabilities; and functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed.

Ref.	Question / requirement	Guidance
		○ For Office 365, Microsoft maintains multiple copies of customer data across data centres for redundancy. ○ For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure GRS replicates certain data between two regions within the same location for enhanced data durability in case of a major data centre disaster. • *Resiliency*. To promote data resiliency, Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. • *Distributed Services*. Microsoft also offers distributed component services like Exchange Online, SharePoint Online, and Lync Online to limit the scope and impact of any failures of a single component. Directory data is also replicated across component services to insulate one service from another in the event of a failure. • *Monitoring*. Microsoft's Online Services include internal monitoring to drive automatic recovery; outside-in monitoring to raise alerts about incidents; and extensive diagnostics for logging, auditing, and granular tracing. • *Simplification*. Microsoft uses standardised hardware to reduce issue isolation complexities. Microsoft also uses fully automated deployment models and a standard built-in management mechanism. • *Human Backup*. Microsoft's Online Services include automated recovery actions with 24/7 on-call support; a team with diverse skills on call to provide rapid response and resolution; and continuous improvement through learning from the on-call teams.

Ref.	Question / requirement	Guidance
		• *Continuous Learning*. If an incident occurs, Microsoft conducts a thorough post-incident review. This post-incident review consists of an analysis of the events that occurred, Microsoft's response, and Microsoft's plan to prevent a similar problem from occurring in the future. Microsoft will share the post-incident review with any organization affected by the service incident. • *Disaster Recovery Tests*. Microsoft conducts disaster recovery tests at least once per year.
42.	Has a business impact analysis been performed?	*All financial services institutions:* *- CNIL Privacy Risk Measures Guidelines.* *- CNIL Security Guidelines.* Financial services institutions are expected to perform a business impact analysis of a disaster situation. Microsoft has tools and resources available to assist and offer Professional Services support as well.
43.	What are the recovery time objectives (RTO) of systems or applications outsourced to the service provider?	Customers can review Microsoft's SLAs and details on its business continuity and failover testing in appropriate whitepapers and policy documents (available at https://servicetrust.microsoft.com/ViewPage/TrustDocuments). Microsoft's core cloud services design principle is for near instant failover and zero data loss.
44.	What are the recovery point objectives (RPO) of systems or applications outsourced to the service provider?	• **Office 365:** Peer replication between data centres ensures that there are always multiple live copies of any data. Standard images and scripts are used to recover lost servers, and replicated data is used to restore customer data. Because of the built-in data resiliency checks and processes, Microsoft maintains backups only of Office 365 information system documentation (including security-related documentation), using built-in replication in SharePoint Online and our internal code repository tool, Source Depot. System documentation is stored in SharePoint Online, and Source Depot contains system and application images. Both SharePoint Online and Source Depot use versioning and

Ref.	Question / requirement	Guidance
		are replicated in near real-time. Information on each Office 365 service available from the Office 365 Trust Center: https://www.microsoft.com/en-us/trustcenter/cloudservices/office365 ○ 45 minutes or less for Microsoft Exchange Online ○ 2 hours or less for SharePoint Online • **Azure:** Backup and resiliency RPO is provided on a service-by-service basis, with information on each Azure service available from the Azure Trust Center: microsoft.com/en-us/trustcenter/cloudservices/azure ○ 1 minute or less for Virtual Storage
45.	What are the data backup and recovery arrangements for your organisation's data that resides with the service provider?	**Redundancy** • Physical redundancy at server, data centre, and service levels. • Data redundancy with robust failover capabilities. • Functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Additionally, Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones", which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational purposes. For example, Azure Globally-Redundant Storage replicates certain data between two regions within the same location for enhanced data durability in case of a major data centre disaster. **Resiliency** • Active/active load balancing. • Automated failover with human backup.

Ref.	Question / requirement	Guidance
		• Recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own. **Distributed Services** • Distributed component services like Exchange Online, SharePoint Online, and Skype for Business Online limit scope and impact of any failures in a component. • Directory data replicated across component services insulates one service from another in any failure events. • Simplified operations and deployment. **Monitoring** • Internal monitoring built to drive automatic recovery. • Outside-in monitoring raises alerts about incidents. • Extensive diagnostics provide logging, auditing, and granular tracing. **Simplification** • Standardised hardware reduces issue isolation complexities. • Fully automated deployment models. • Standard built-in management mechanism.

Ref.	Question / requirement	Guidance
		Human Backup • Automated recovery actions with 24/7 on-call support. • Team with diverse skills on the call provides rapid response and resolution. • Continuous improvement by learning from the on-call teams. **Continuous Learning** • If an incident occurs, Microsoft does a thorough post-incident review every time. • Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. • If the organisation was affected by a service incident, Microsoft shares the post-incident review with the organisation. **Disaster recovery tests** • Microsoft conducts disaster recovery tests at least once per year.
46.	How frequently does the service provider conduct disaster recovery tests?	Microsoft conducts disaster recovery tests at least once per year. By way of background, Microsoft maintains physical redundancy at the server, data center, and service levels; data redundancy with robust failover capabilities; and functional redundancy with offline functionality. Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Microsoft maintains multiple live copies of data at all times. Live data is separated into "fault zones," which ensure continuous access to data. For Office 365, Microsoft maintains multiple copies of customer data across datacenters for redundancy. For Azure, Microsoft may copy customer data between regions within a given location for data redundancy or other operational

Ref.	Question / requirement	Guidance
		purposes. For example, Azure Globally-Redundant Storage ("GRS") replicates certain data between two regions within the same location for enhanced data durability in case of a major datacenter disaster. To promote data resiliency, Microsoft's Online Services offer active load balancing, automated failover and human backup, and recovery testing across failure domains. For example, Azure Traffic Manager provides load balancing between different regions, and the customer can use network virtual appliances in its Azure Virtual Networks for application delivery controllers (ADC/load balancing) functionality. Load balancing is also provided by Power BI Services, the Gateway, and Azure API Management roles. Office 365 services have been designed around specific resiliency principles that are designed to protect data from corruption, to separate data into different fault zones, to monitor data for failing any part of the ACID test, and to allow customers to recover on their own. For more information, refer to Microsoft's white paper "Data Resiliency in Microsoft Office 365," available at https://aka.ms/Office365DR.
G. EXIT STRATEGY		
47.	Is there a contingency plan in the event of the unexpected cessation of the service provider?	*Undertakings subject to the Order: Articles 10 n), 238 b) and 239 c) of the Order.* *AMC: Article 313-75 II, 2°, 4° and 11° of the AMF General Regulation.* Financial institutions should put in place a contingency plan to address the possibility that its current service provider might not be able to continue operations or render the services required.
48.	Do you have the right to terminate the SLA in the event of default, ownership change, insolvency, change of security or serious	*Undertakings subject to the Order: Article 238 b) and c) of the Order.* The SLA is only one part of the contractual arrangement with Microsoft. It is not terminable in itself as a stand-alone document (the remedies available to customers under the SLA are financial). The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the customer may

Ref.	Question / requirement	Guidance
	deterioration of service quality?	contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice.
49.	In the event of contract termination with the service provider, either on expiry or prematurely, are you able to have all IT information and assets promptly removed or destroyed?	*Undertakings subject to the Order:* - *Article 238 c) of the Order.* - *ACPR Guidelines on the risks associated with cloud computing, page 14.* *AMC: Article 313-75 II 7° of the AMF General Regulation.* *All financial institutions:* - *CNIL Privacy Risk Measures Guidelines.* - *CNIL Security Guidelines. Recommendation No 2 of the CNIL Cloud Recommendations.* Upon expiration or termination, the customer can extract its data. As set out in the OST, Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service. Ownership of documents, records and other data remain with the customer and at no point transfer to Microsoft or anyone else, so this does not need to be addressed through transition. Being a cloud services solution, ownership of software and hardware used to provide the service remains with Microsoft. Microsoft uses best practice procedures and a wiping solution that is NIST 800-88, ISO/IEC 27001, ISO/IEC 27018, SOC 1 and SOC 2 compliant. For hard drives that cannot be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained.

Part 2: Contract Checklist

What are our contract documents?

Core Microsoft contract documents	Documents incorporated in Microsoft contracts[1]
Microsoft Business and Services Agreement (**MBSA**); Enterprise Agreement (**EA**); and the enabling **Enrollment**, which is likely to be either an Enterprise Enrollment or a Server and Cloud Enrollment.	Online Service Terms (**OST**), incorporating the Data Processing Terms including the EU Model Clauses (**DPT**) and the GDPR Terms that reside in Attachment 4; **Product Terms** Online Services Service Level Agreement (**SLA**).
Amendment provided by Microsoft to add to core contract documents for financial services customers **Financial Services Amendment**	**Supporting documents and information that do not form part of the contract**[2] Materials available from the relevant **Trust Center**

What does this Part 2 cover?

This Part 2 sets out the specific items that must be addressed in the financial services institution's agreement with the service provider and the third column indicates how and where in the Microsoft contractual documents the mandatory requirement is covered.

[1] Available at www.microsoft.com/contracts.
[2] Available at www.microsoft.com/trustcenter.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Undertakings subject to the Order: Articles 238 b) and 239 e) and f) of the Order. **AMC: Articles 313-75 II 4° and 9° of the AMF General Regulation.**	Does the agreement enable the financial services institution to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations?	In order to facilitate your continued and ongoing legal and regulatory compliance needs, and as part of its standard offering to you (i.e. the FSA that automatically applies to regulated financial services institution customers), Microsoft agrees to discuss how to meet new or additional requirements imposed on you should you become subject to Future Applicable Law (as defined in the FSA). Meanwhile, Microsoft enables financial institution customers to retain an appropriate level of control to meet their legal and regulatory obligations. Not only do you have full control and ownership over your data at all times, under the FSA Microsoft (i) makes available to you the written cloud services data security policy that complies with certain control standards and frameworks, along with descriptions of the security controls in place for Azure and other information that you reasonably request regarding Microsoft's security practices and policies; and (ii) causes the performance of audits, on your behalf, of the security of the computers, computing environment and physical data centres that it uses in processing your data (including personal data) for the cloud services, and provides the audit report to you upon request. These arrangements are offered to you in order to provide you with the appropriate level of assessment of Microsoft's ability to facilitate compliance against your policy, procedural, security control and regulatory requirements. You can further elect to participate in the Customer Compliance Program. This program allows you to engage with Microsoft during the term of the outsourcing contract to ensure that you have oversight over the services in order to ensure that the services meet your legal and regulatory obligations. Specifically, it enables you to have additional monitoring, supervisory and audit rights and additional controls over the cloud services, such as (a) access to Microsoft personnel for raising questions and escalations relating to the cloud services, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results and subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on your use of the cloud services, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		business resumption and contingency plans or other circumstances that might have a serious impact on your use of Azure, (d) access to a summary report of the results of Microsoft's third party penetration testing against the cloud services (e.g. evidence of data isolation among tenants), and (e) access to Microsoft's subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of planned developments or reports of significant events will be discussed and you will have a chance to provide structured feedback and/or suggestions regarding the Customer Compliance Program and its desired future evolution. The group events will also give you the opportunity to discuss common issues with other regulated financial institutions and raise them with Microsoft.
Undertakings subject to the Order: Article 238 a) of the Order **AMC: Article 313-75 III of the AMF General Regulation** **All financial institutions: Article 35 of the French DPA**	Has an agreement for each of the items, activities, operations, transactions or areas to be outsourced to the service provider been established?	The agreements with Microsoft comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The online services are ordered under the Enrollment, and the order will set out the online services. The services are described, along with the applicable usage rights, in the Product List and OST. The services are described in more detail in the OST, which includes a list of service functionality. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable initial or renewal term of the Enrollment are fixed for the duration of that term.
Undertakings subject to the Order: Article 239 a) of the Order.	Does the agreement contain provisions regarding performance standards, for example service levels, performance targets, service	All of these aspects of service levels, performance targets, service availability, reliability, stability and upgrade are covered in the SLA. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The SLA is fixed for the initial term of the Enrollment:

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
AMC: Article 313-75 II 1° and 2° of the AMF General Regulation. **Undertakings subject to the Order: ACPR Guidelines on the risks associated with cloud computing.**	availability, reliability, stability and upgrade?	*"We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, then the version of this SLA that is current at the time of renewal will apply for your renewal term."* For information regarding uptime for each Online Service, refer to the Service Level Agreement for Microsoft Online Services.
Undertakings subject to the Order: - **Articles 234, 237 e), 239 f) and 239 h) of the Order.** - **Article R 612-26 of the Monetary and Financial Code.** - **ACPR Guidelines on the risks associated with cloud computing, page 9 (weaknesses of cloud computing in the area of control and evidence), page**	Has your organisation made explicit provisions in the outsourcing contracts to enable it, regulatory bodies and appointed personnel such as auditors to carry out inspection or examination of the service provider's facilities, systems, processes and data relating to the services provided to your organisation?	The DPT specifies the audit and monitoring mechanisms that Microsoft puts in place to verify that the Online Services meet appropriate security and compliance standards. Rigorous third-party audits validate the adherence of Microsoft's Online Services to these strict requirements. Upon request, Microsoft will provide each Microsoft audit report to a customer to verify Microsoft's compliance with the security obligations under the DPT Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx. Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
11, last paragraph, page 15 (Supervision of the service provider). **AMC: Article 313-75 II 8° and 9° of the AMF General Regulation.**		and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and the regulator(s). The "Regulator Right to Examine" sets out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights: 1. **Online Services Information Policy** Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. **Audits of Online Services** On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centres that it uses in processing customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide Customer with each Microsoft Audit Report. 3. **Customer Compliance Program** The customer also has the opportunity to participate in the Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft, including: (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.
Undertakings subject to the Order: Article 239 b) of the Order. **AMC: Article 313-75 10° of the AMF General Regulation.** **All financial institutions: Article L. 226-13 of the French Criminal Code, Articles L.511-33 and L.531-12 of the Monetary and Financial Code.Article 35 of the French DPA.** **EBA Recommendations – page 16 (Security of data and systems)**	Have you obtained from the service provider a written undertaking to protect and maintain the confidentiality of your data?	The OST states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer owns its data that is stored on Microsoft cloud services at all times. The customer also retains the ability to access its customer data at all times, and Microsoft will deal with customer data in accordance with the terms and conditions of the Enrollment and the OST. Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of customer's subscription so that the customer may extract the data. No more than 180 days after expiration or termination of the customer's use of an Online Service, Microsoft will disable the account and delete customer data from the account. Microsoft makes specific commitments with respect to safeguarding your data in the OST. In summary, Microsoft commits that: 1. Your data will only be used to provide the online services to you and your data will not be used for any other purposes, including for advertising or similar commercial purposes. (OST, page 7) 2. Microsoft will not disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. (OST, page 7) 3. Microsoft has implemented and will maintain appropriate technical and organisational measures, internal controls, and information security routines intended to protect your data against accidental, unauthorised or unlawful access, disclosure, alteration, loss, or destruction. (OST, page 36) Technical support personnel are only permitted to have access to customer information when needed. (OST, page 13)

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		The OST states the responsibilities of the contracting parties that ensure the effectiveness of security policies. To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses you for reasonable and third-party validated, out-of-pocket remediation costs you incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and additional, commercially-reasonable, out-of-pocket expenses you incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA. Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (OST).
Undertakings subject to the Order: Article 10 q) of the Order **AMC: Article 313-74 of the AMF General Regulation**	Does the agreement cover the nature and scope of the service to be provided (i.e. scope of the relationship, frequency, content and location of service to be provided)?	The contract with Microsoft comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The online services are ordered under the Enrollment, and the order will set out the online services. The services are described, along with the applicable usage rights, in the Product List and OST. The services are described in more detail in the OST. The SLA contains Microsoft's service level commitment, as well as the remedies for us in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable initial or renewal term of the Enrollment are fixed for the duration of that term. The location of Microsoft's data centers are available on the Trust Center and by participating in the Microsoft Online Services Customer Compliance Program under section 2d of the FSA, we will have access to Microsoft's data center roadmap which will give us advance warning of new data center locations.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Undertakings subject to the Order: Article 239 a) of the Order. **AMC: Article 313-75 II 2° of the AMF General Regulation.**	Does the agreement cover performance monitoring (i.e. includes performance measures and indicators)?	The OST allows customer to have the ability to access and extract customer data, and specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx. In addition, the Financial Services Amendment details the examination and audit rights that are granted to the customer and the regulator(s). The "Regulator Right to Examine" sets out a process which can culminate in the regulator's examination of Microsoft's premises. To enable the customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide the customer with access to information, Microsoft personnel and Microsoft's external auditors. Microsoft will provide the customer with the following rights: 1. **Online Services Information Policy** Microsoft makes each Information Security Policy available to the customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by the customer regarding Microsoft security practices and policies. 2. **Audits of Online Services** On behalf of the customer, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centres that it uses in processing

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		customer data for each Online Service. Pursuant to the terms in the OST, Microsoft will provide customer with each Microsoft Audit Report. **3. Customer Compliance Program** The customer also has the opportunity to participate in the Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft. This program allows you to engage with Microsoft during the term of the outsourcing contract to ensure that you have oversight over the services in order to ensure that the services meet your legal and regulatory obligations. Specifically, it enables you to have additional monitoring, supervisory and audit rights and additional controls over Azure, such as (a) access to Microsoft personnel for raising questions and escalations relating to Azure, (b) invitation to participate in a webcast hosted by Microsoft to discuss audit results and subsequent access to detailed information regarding planned remediation of any deficiencies identified by the audit, (c) receipt of communication from Microsoft on (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on your use of Azure, (2) Microsoft's risk-threat evaluations, and (3) significant changes to Microsoft's business resumption and contingency plans or other circumstances that might have a serious impact on your use of Azure, (d) access to a summary report of the results of Microsoft's third party penetration testing against Azure (e.g. evidence of data isolation among tenants), and (e) access to Microsoft's subject matter experts through group events such as webcasts or in-person meetings (including an annual summit event) where roadmaps of planned developments or reports of significant events will be discussed and you will have a chance to provide structured feedback and/or suggestions regarding the Customer Compliance Program and its desired future evolution. The group events will also give you the opportunity to discuss common issues with other regulated financial institutions and raise them with Microsoft.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Undertakings subject to the Order: Article 239 g) of the Order. **For AMC: Article 313-75 II 6° of the AMF General Regulation.**	Does the agreement cover reporting requirements (i.e., type, content and frequency of reporting, whether the performance is met and reporting of incidents or events that may affect the service)?	Microsoft will notify the customer if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (see OST). The DPT specifies the audit and monitoring mechanisms that Microsoft puts in place to verify that the Online Services meet appropriate security and compliance standards. Rigorous third-party audits validate the adherence of Microsoft's Online Services to these strict requirements. Upon request, Microsoft will provide each Microsoft audit report to a customer to verify Microsoft's compliance with the security obligations under the DPT Microsoft also conducts regular penetration testing to increase the level of detection and protection throughout the Microsoft cloud. Microsoft makes available to customers penetration testing and other audits of its cybersecurity practices, and customers also may conduct their own penetration testing of the services. This is done in accordance with Microsoft's rules of engagement, which do not require Microsoft's permission in advance of such testing. For more information regarding penetration testing, see https://technet.microsoft.com/en-us/mt784683.aspx. Microsoft makes available certain tools through the Service Trust Platform to enable customers to conduct their own virtual audits of the Online Services. Microsoft also provides customers with information to reconstruct financial transactions and develop audit trail information through two primary sources: Azure Active Directory reporting, which is a repository of audit logs and other information that can be retrieved to determine who has accessed customer transaction information and the actions they have taken with respect to such information, and Azure Monitor, which provides activity logs and diagnostic logs that can be used to determine the "what, who, and when" with respect to changes to customer cloud information and to obtain information about the operation of the Online Services, respectively.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		The customer also has the opportunity to participate in the Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to audit Microsoft. This program allows you to engage with Microsoft during the term of the outsourcing contract to ensure that you have oversight over the services in order to ensure that the services meet your legal and regulatory obligations.
All financial institutions: Article 35 of the French DPA. **EBA Recommendations – page 17 (Chain oursourcing)**	Does the agreement cover sub-contracting (i.e. restrictions on sub-contracting and clauses governing confidentiality of data)?	Microsoft commits that its subcontractors will be permitted to obtain customer data only to deliver the services Microsoft has retained them to provide and will be prohibited from using customer data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST (OST, page 9). To ensure subcontractor accountability, Microsoft requires all of its vendors that handle customer personal information to join the Microsoft Supplier Security and Privacy Assurance Program, which is an initiative designed to standardise and strengthen the handling of customer personal information, and to bring vendor business processes and systems into compliance with those of Microsoft. For more information regarding Microsoft's Supplier Security and Privacy Program, see https://www.microsoft.com/en-us/procurement/msp-requirements.aspx. Microsoft will enter into a written agreement with any subcontractor to which Microsoft transfers customer data that is no less protective than the data processing terms in the customer's contracts with Microsoft (DPT, see OST, page 11). In addition, Microsoft's ISO/IEC 27018 certification requires Microsoft to ensure that its subcontractors are subject to the same security controls as Microsoft. Microsoft's ISO 27001 certification provides a layer of additional controls that impose stringent requirements on Microsoft's subcontractors to comply fully with Microsoft's privacy, security, and other commitments to its customers, including requirements for handling sensitive data, background checks, and non-disclosure agreements. Microsoft provides a website that lists subcontractors authorised to access customer data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		authorising any new subcontractor to access Customer Data, Microsoft will update the website and provide the customer with a mechanism to obtain notice of that update. If the customer does not approve of a new subcontractor, then the customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected cloud computing service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent customer invoices. (DPT, see OST, page 11) In this way the confidentiality of customer data is protected when Microsoft uses subcontractors because Microsoft commits that its subcontractors "*will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose*".
Undertakings subject to the Order: Articles 10 n), 238 b) and 239 c) of the Order **AMC: Article 313-75 II, 2°, 4° and 11° of the AMF General Regulation** **EBA Recommendations – pages 16 and 18**	Does the agreement cover business resumption and contingency requirements?	Business Continuity Management forms part of the scope of the accreditation that Microsoft retains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (DPT, see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's industry standards compliance commitments and Microsoft's annual third party compliance audit. Business Continuity Plans (BCPs) are documented and reviewed at least annually, and the BCPs provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Microsoft also maintains emergency and contingency plans for the facilities in which Microsoft information systems that process customer data are located. Microsoft's redundant storage and its

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		procedures for recovering data are designed to attempt to reconstruct customer data in its original or last-replicated state from before the time it was lost or destroyed. Data Recovery Procedures • On an ongoing basis, but in no case less frequently than once a week (unless no customer data has been updated during that period), Microsoft maintains multiple copies of customer data from which customer data can be recovered. • Microsoft stores copies of customer data and data recovery procedures in a different place from where the primary computer equipment processing the customer data is located. • Microsoft has specific procedures in place governing access to copies of customer data. • Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services , which are reviewed every twelve months. Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
	Does the agreement cover default termination and early exit by all parties? Does the financial institution have the right to terminate the agreement in the event of default including change of ownership, insolvency or where there is a breach of	Microsoft agreements are usually subject to terms of 12-36 months, which may be extended at the customer's election. They also include rights to terminate early for cause and without cause. Micosoft's Financial Services Amendment provides for business contiuity and exit provisions, including rights for the customer to obtain exit assistance at market rates from Microsoft Consulting Services. Customers should work with Microsoft to build such business continuity and exit plans. Microsoft's flexibility in offering hybrid solutions further facilitate transition from cloud to on-premise solutions more seamlessly.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
	security or confidentiality or demonstrable deterioration in the ability of the service provider to perform the service as contracted?	
Undertakings subject to the Order: Articles 238 c) of the Order. **AMC: Article 313-75 II 7° of the AMF General Regulation.**	Does the financial institution have the right to interrupt/terminate the outsourcing agreement where necessary without detriment to the continuity and quality of its provision of services to clients?	The customer may terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the Customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice Microsoft will retain customer data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data. Microsoft will disable the account and delete customer data from the account no more than 180 days after expiration or termination of customer's use of an Online Service.
Undertakings subject to the Order: Articles 238 b) of the Order **AMC: Article 313-75 II 4° of the AMF General Regulation** **EBA Recommendations –**	Does the financial services institution have the right to take measures if it appears that the service provider may not be carrying out the functions effectively and in compliance with applicable	First, Microsoft is contractually obliged to comply with all applicable laws (MBSA, section 4a). In the event, that Microsoft was not carrying out the functions in compliance with applicable laws and regulatory requirements, customers could raise this point with us as a contractual issue. A customer that has elected to participate in the Customer Compliance Program under the OST has access to the services and the ability to monitor and scrutinise performance. Under this program, customers can raise issues directly and immediately with Microsoft where corrective measures are

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
page 16 (Security of data and systems)	laws and regulatory requirements?	required, including if the functions are not being carried out effectively or in compliance with applicable laws and regulatory requirements. The customer may also terminate an Online Service at the express direction of a regulator with reasonable notice. Additionally, to ensure regulatory compliance, Microsoft and the Customer may contemplate adding additional products or services, or if these are unable to satisfy the customer's new regulatory requirements, the customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice. Additionally, in order to facilitate your continued and ongoing legal and regulatory compliance needs, and as part of its standard offering to you (i.e. the FSA that automatically applies to regulated financial services institution customers), Microsoft agrees to discuss how to meet new or additional requirements imposed on you should you become subject to Future Applicable Law (as defined in the FSA).
Undertakings subject to the Order: Articles 239 b) of the Order **AMC: Article 313-75 II 10° of the AMF General Regulation** **All financial institutions: Article 35 of the French DPA**	Does the agreement cover confidentiality and security (i.e. roles and responsibility, liability for losses in the event of breach of confidentiality)?	The OST states the responsibilities of the contracting parties that ensure the effectiveness of security policies. To the extent that a security incident results from Microsoft's failure to comply with its contractual obligations, and subject to the applicable limitations of liability, Microsoft reimburses you for reasonable and third-party validated, out-of-pocket remediation costs you incurred in connection with the security incident, including actual costs of court- or governmental body-imposed payments, fines or penalties for a Microsoft-caused security incident and additional, commercially-reasonable, out-of-pocket expenses you incurred to manage or remedy the Microsoft-caused security incident (FSA, Section 3). Applicable limitation of liability provisions can be found in the MBSA. Microsoft further agrees to notify you if it becomes aware of any security incident, and to take reasonable steps to mitigate the effects and minimise the damage resulting from the security incident (OST).

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
Undertakings subject to the Order: Articles 239 f) of the Order. **AMC: Article 313-75 II 9° of the AMF General Regulation.** **EBA Recommendations pages 14 and 15**	Does the agreement cover effective access bv the financial services institution, or the persons in charge of auditing its accounts or the competent authority to data related to the outsourced activities?	Customers have a contractual right to access their data at all times and their data will only be used to provide the Online Services and will not be used for any other purposes, including for advertising or similar commercial purposes (see OST, page 7). In terms of access to your data by a competent authority, section 2a of the FSA details the examination and influence rights that are granted to regulators. The process can culminate in the regulator's examination of Microsoft's services, records, reports and premises. This examination and inspection right has been validated by a variety of regulators across the world, including those in Singapore, Australia and Europe as being sufficient to meet the regulatory needs in those markets, and as such, we are satisfied the rights we have agreed are sufficient to meet our regulatory obligations. In terms of a regulatory request to access data, Microsoft will not disclose customer data to law enforcement unless it is legally obliged to do so, and only after not being able to redirect the request to the customer.
Undertakings subject to the Order: Article 239 c) of the Order. **AMC: Article 313-75 II 11° of the AMF General Regulation**	Does the agreement cover contingency plan in case of serious difficulty affecting the continuity of service; or alternatively, the financial services institution's own contingency plan takes account of the fact that the service provider may be prevented from carrying out its services.	Business Continuity Management forms part of the scope of the accreditation that Microsoft retains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (DPT, see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's industry standards compliance commitments and Microsoft's annual third party compliance audit. In addition, customers also have the following rights to be able to obtain their data in the event that they need to activate their own contingency plans: (i) contractual right to access their data at all times; and (ii) Microsoft will retain customer data stored in the Online Service in a limited function account for

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		90 days after expiration or termination of the customer's subscription so that the customer may extract the data. Separately, customers are also required to consider their own contingency plans, in the event that the service provider is no longer able to carry out the services.
Undertakings subject to the Order: Article 239 d) of the Order	Does the agreement provide that prior consent of the financial institution is required for material modification of the services by the service provider?	Yes. The terms of the contract with Microsoft are fixed for the duration of that term (see the introductory wording to the OST). When customers renew the contract or purchase a new subscription to an Online Service, the then-current OST will apply and will not change during their subscription for that Online Service.
Undertakings subject to the Order: Article 237 e) of the Order **AMC: Article 313-75 II 5° of the AMF General Regulation**	Does the agreement cover the right of the financial institution to retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing and to supervise those functions and manage those risks?	The agreement gives customers a number of rights which allow them to retain the necessary expertise to supervise the outsourced functions effectively and manage the risks associated with the outsourcing and to supervise and manage those risks, including: 1. Under the FSA, section 2c, if the customer requests, Microsoft will provide copies of its audit reports so that customers can verify Microsoft's compliance with its obligations. 2. Microsoft will notify customers if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (see OST). 3. Microsoft also offers a Customer Compliance Program which facilitates the customer's ability to audit Microsoft. This program allows you to engage with Microsoft during the term of the

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
		outsourcing contract to ensure that you have oversight over the services in order to ensure that the services meet your legal and regulatory obligations
Undertakings subject to the Order: Articles 237 a), b), c) and d) of the Order. **AMC: Article 313-75 I 1°, 2° and 3° of the AMF General Regulation**	Has the financial institution ensured that the agreement with the service provider does not contain clauses which: - create a delegation by the executive body of its responsibility; - alter the relationship and obligations of the financial institution towards its clients; - undermines the conditions with which the financial institution must comply in order to be authorised, and to remain so; - removes or modifies the other conditions subject to which the financial	The agreement with Microsoft does not contain any such clauses.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
	institution's authorisation was granted.	
EBA Recommendations – page 17 (Location of data and data processing)	Is agreement tailored to address additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when outsourcing to a service provider outside of your jurisdiction?	The DPT provides commitments on the location at which Microsoft will store customer data at rest (see OST, page 11). Microsoft cloud services offer data-location transparency so that the organisations and regulators are informed of the jurisdiction(s) in which data is hosted. The data centres are strategically located around the world taking into account country and socioeconomic factors. Microsoft's data centre locations are selected to offer stable socioeconomic environments. The OST contains general commitments around data location. Microsoft commits that customer data transfers out of the EU will be governed by the EU Model Clauses set out in the OST to represent a high standard of care in relation to data transfers. Also, as noted in the OST: "Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the Data Processing Terms". Microsoft also makes GDPR specific commitments (Attachment 4, OST) to all customers effective May 25, 2018.
	Does the agreement cover dispute resolution (i.e. a protocol for resolving disputes and continuation of contracted service during disputes), a choice of law provision, and a jurisdictional choice that provides for adjudication of disputes	In the event that a financial institution and Microsoft have a dispute, the choice-of-law and dispute resolution provisions would be clearly described in the agreement between Microsoft and the financial institution. MBSA clauses 10(g) and 10(h) contains terms that describe how a dispute under the contract is to be conducted.

Reference	Requirement	How and where is this dealt with in Microsoft's contract?
	between the parties in a specific forum?	

Further Information

- **Trust Center: microsoft.com/trust**
- **Service Trust Portal: aka.ms/trustportal**
- **Customer Stories: customers.microsoft.com**
- **Online Services Terms: microsoft.com/contracts**
- **Service Level Agreements: microsoft.com/contracts**
- **SAFE Handbook: aka.ms/safehandbook**
- **A Cloud for Global Good | Microsoft: news.microsoft.com/cloudforgood/**