TaylorWessing

The current state of the EU regulatory framework on outsourcing in the financial services sector

In recent years, in pursuit of cost reduction and efficiency improvement financial institutions around the globe have been increasingly interested in outsourcing their business activities to other institutions and specialised service providers. From asset management, where delegation of certain functions was a standard practice since decades, to small payment companies relying on specialised regulatory compliance service providers, there is almost no area of the financial services sector nowadays that has remained immune to the ever-increasing use of outsourcing arrangements. Moreover, rapid digitisation of the financial services sector, featured by more frequent use of cloud technology and specialised providers of IT-related services to financial institutions, has just added more complexity into the game which immediately triggered the attention of financial regulators in the European Union.

The current EU regulatory framework on outsourcing is contained in various sector specific pieces of EU legislation like Capital Requirements Directive (CRD IV), the Markets in Financial Instruments Directive (MiFID II), Payment Services Directive 2 (PSD 2), Alternative Investment Funds Managers Directive (AIFMD) etc. However, the requirements stipulated in the aforementioned EU legislation are not harmonized and frequent divergences in national transposition laws at EU Member State level just add more confusion for financial institutions who need to comply with them.

ESA's Guidance Framework

In attempt to bridge these gaps (to a certain extent) the European Supervisory Authorities (ESAs), European Banking Authority (EBA), European Securities and Markets Authority (ESMA and European Insurance and Occupational Pension Authority (EIOPA) have issued guidelines on outsourcing arrangements that stipulate standards and requirements that financial institutions under their respective supervisory remit need to fulfil when entering into outsourcing arrangements.

These include:

- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- ESMA Guidelines on outsourcing to cloud service providers (ESMA50-164-4285)
- EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002)

Whereas the EBA Guidelines apply to all types of outsourcing arrangements that financial institutions under its supervisory remit enter into, the ESMA and EIOPA Guidelines are focused solely on one specific type of outsourcing arrangements that has attracted much of regulatory scrutiny lately, outsourcing to cloud service providers.

	EBA Guidelines	ESMA Guidelines	EIOPA Guidelines
In-Scope Firms	Credit institutions, investment firms subject to CRD IV framework, payment and e-money institutions	AIFMs, UCITS ManCos, investment firms and credit institution providing investment services, CSDs, CCPs, credit rating agencies, operators of trading venues, trade repositories, administrators of critical benchmarks	Insurance and re-insurance undertakings
Scope of application	All types of outsourcing arrangements	Outsourcing arrangements to cloud service providers	Outsourcing arrangements to cloud service providers
Start to apply	30 September 2019	31 July 2021	1 January 2021
Deadline for amendment of existing arrangements	31 December 2021	31 December 2022	31 December 2022

Overview of ESA's Guidance framework on outsourcing

EBA Guidelines on outsourcing arrangements

In February 2019, EBA has published its guidelines on outsourcing arrangements (EBA Guidelines) that apply to credit institutions and investment firms that are subject to CRD IV framework as well as to payment and e-money institutions. The latest EBA Guidelines also integrate the EBA Guidelines on outsourcing to cloud service providers that were published in December 2017. To that end, the EBA Guidelines on outsourcing arrangements apply to all types of outsourcing arrangements that in-scope institutions enter into.

The EBA Guidelines define an outsourcing arrangement as an arrangement of any form between a financial institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the financial institution itself. Intra-group outsourcing arrangements also fall under this definition given that EBA considers that they are not necessarily less risky than outsourcing to third-parties outside the group.

Outsourcing of critical or important functions.

With respect to outsourcing of critical or important functions, the EBA Guidelines stipulate specific requirements that go beyond requirements applicable to other types of outsourcing arrangements. By following the wording of the MiFID II Delegated Regulation (EU) 2017/565, the EBA Guidelines consider a function as critical or important

where the defect or failure in its performance would materially impair financial institutions'

- compliance with applicable regulatory requirements;
- financial performance or soundness and continuity of its main services and activities.

In addition, outsourcing of functions whose performance is subject to authorisation and arrangements, with respect to which certain additional criteria stipulated by the EBA Guidelines are met, are considered as outsourcing of critical or important functions as well. Financial institutions are required to notify their national competent authority in writing and in a timely manner about the planned outsourcing arrangement, where it concerns the outsourcing of a critical or important function.

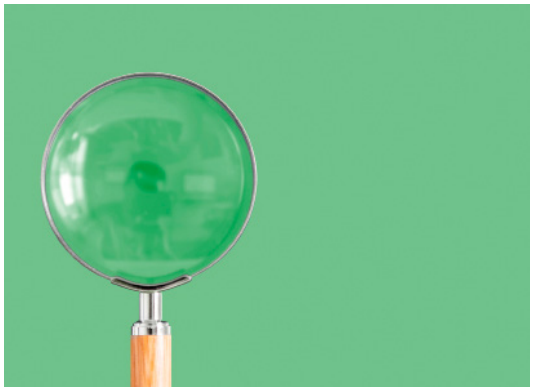
Governance arrangements

Financial institutions are required to implement effective processes and procedures for performance of the preliminary risk assessment, entering into as well as continuous monitoring of outsourcing arrangements. In order to ensure effective management and oversight of all outsourcing arrangements, financial institutions are required to either designate a member of the senior staff or appoint a designated outsourcing oversight function (i.e. outsourcing officer) responsible for this.

As part of internal governance framework on outsourcing, financial institutions are also required to adopt an outsourcing policy, which clearly defines institutions' outsourcing processes and procedures on outsourcing.

Risk analysis and Due Diligence

Prior to entering into an outsourcing arrangement, financial institutions are required to conduct a comprehensive risk analysis of the proposed outsourcing arrangement by taking into account relevant operational risks attached to it (like the risk of improper performance of outsourced functions, concentration and risks attached to sub-outsourcing plans etc.). Further, in order to assess the suitability of the service provider for the performance of the outsourced function financial institutions are required to conduct a due diligence by considering various factors, among other, its business reputation, technical and staff resources, expertise in the specific field etc.



Outsourcing register

Financial institutions are required to establish and regularly maintain an outsourcing register in which all relevant information about all outsourcing arrangements are contained (including date of entry, functions that were outsourced, information about the service provider etc.). In relation to outsourcing arrangements with cloud service providers, the register also needs to contain information about the cloud service and deployment model used as well as relevant information about the type of data and locations used for data storing.

Contractual requirements

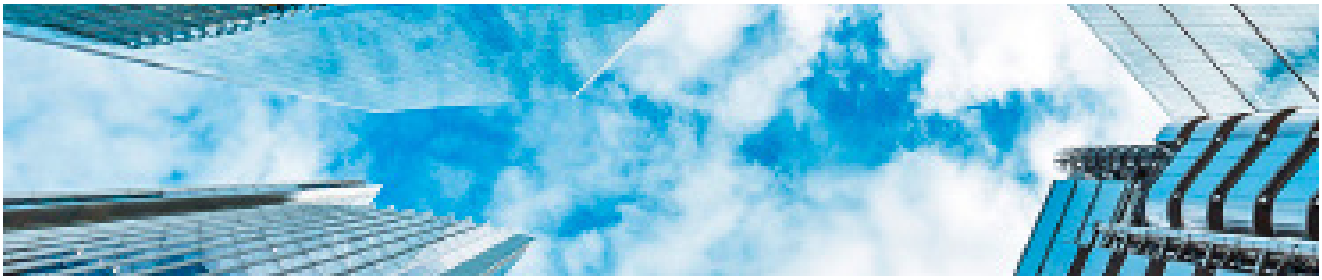
All mutual rights and obligations need to be stipulated in a written outsourcing agreement, which needs to contain relevant provisions, based on which financial institutions can ensure their compliance with applicable regulatory requirements on outsourcing. The outsourcing agreement for outsourcing of critical or important functions needs to contain provisions on reporting obligations of the service provider, the agreed service levels and access rights of the financial institution to documentation and premises of the service provider necessary for efficient monitoring of performance of the outsourced function. Outsourcing agreements shall also explicitly contain provisions on whether and under which conditions the service provider can enter into a sub-outsourcing agreement including the right of the financial institution to object to intended sub-outsourcing or material changes thereof.

Exit strategies and termination rights

In the case of outsourcing of critical or important functions, financial institutions are required to develop strategies that ensure efficient exit from an outsourcing arrangement without undue disruption of business activities or proper provision of services to clients in the case of the termination of an outsourcing agreement or shortcomings in performance of the outsourced function. Properly documented exit strategy needs to outline transition plans pursuant to which the continuity of performance of the outsourced function would be ensured either by its transfer to an alternative service provider or back to the institution.

The outsourcing agreement also needs to contain specific provisions that grant financial institutions a termination right where service provider improperly performs the outsourced function, comes in a breach of applicable laws and regulations or where material changes occur that affect the outsourcing arrangement itself (non-compliant entering into sub-outsourcing arrangement, supervisory intervention etc.).

The EBA Guidelines have come into force on 30 September 2019 and all outsourcing arrangements entered into or amended on or after this date need to be structured in accordance with new requirements. Financial institutions have until 31 December 2021 to make necessary amendments to existing outsourcing arrangements entered into before 30 September 2019.



ESMA Guidelines on outsourcing to cloud service providers

On 10 May 2021, the European Securities and Markets Authority (ESMA) has published its final Guidelines on outsourcing to cloud service providers (ESMA Guidelines) which aim to provide guidance to financial institutions and supervisory authorities with respect to steps that are to be followed in relation to ever increasing use of cloud outsourcing.

Scope

The ESMA Guidelines apply to a wide range of firms including among others Alternative Investment Fund Managers (AIFMs), UCITS Management Companies, investment firms and credit institutions (in part in which they provide investment services), operators of trading venues, CSDs, credit rating agencies etc.

In contrast to the EBA Guidelines, the ESMA Guidelines are limited in scope by applying solely to outsourcing to cloud service providers. Therefore, new ESMA Guidelines do not affect directly standard outsourcing arrangements that do not include the provision of cloud services like the outsourcing of compliance or risk management function or common delegation agreements of AIFMs and UCITS management companies with external portfolio managers that are common in the industry. Such outsourcing arrangements will remain subject to applicable sector specific requirements on outsourcing (like requirements contained in the MiFID II Delegated Regulation (EU) 2017/565, AIFMD Delegated Regulation (EU) 231/2013 etc.).

Cloud outsourcing arrangement

The definition of a "cloud outsourcing arrangement" under the ESMA Guidelines covers arrangements in any form (including delegation arrangements) between a regulated firm and a provider of services based on cloud computing (cloud service provider, "CSP"), by which the CSP performs a function that would otherwise be undertaken by the firm itself. Further, the ESMA Guidelines equally apply to arrangements between a regulated firm and a third-party that itself relies on a CSP to perform its functions in which case all references to CSPs are to be read as referring to such third-party.

ESMA Guidelines

In its Guidelines, ESMA generally follows the same principles that EBA has stipulated in its Guidelines on outsourcing arrangements, by requiring financial institutions under its supervision who enter into outsourcing arrangements with cloud service providers to:

- Implement effective governance arrangements based on an outsourcing policy which is in line with internal standards and processes on information and communication technology, information security and risk management;
- Designate a member of the senior staff or establish a permanent cloud outsourcing oversight function responsible for effective oversight and management of outsourcing arrangements;
- Determine whether the arrangement includes the outsourcing of a critical or important function;
- Conduct a risk analysis of each proposed outsourcing arrangement by taking into account all relevant risks attached to it (including ICT risks, risks related to planned cloud service and the deployment model, data transfers etc.);
- Conduct a due diligence on the service provider by taking into account its business reputation, resources, organisational structure as well as its ability to properly comply with information security and data protection standards;
- Maintain an outsourcing register which needs to contain all relevant information about each outsourcing arrangement with cloud service provider, including information on the type of cloud services and deployment models, specific type of data used and locations where data will be stored;
- Prepare exit strategies in the case of outsourcing of critical or important functions that enable smooth transition in the case of the termination of an outsourcing agreement;
- Stipulate specific contractual provisions in outsourcing agreements that describe the outsourced function, type of cloud service and deployment models used, the access and inspection rights of the financial institution, termination rights and the transition mechanism related to the above-mentioned exit strategy etc.
- Notify their competent authority in writing and in a timely manner of planned outsourcing arrangement that concerns a critical or important function.

Focus on information security

In addition to the above-mentioned requirements that follow the principles from EBA Guidelines, the ESMA Guidelines put an additional accent on information security by requiring financial institutions to set information security requirements in their internal policies and procedures as well as to stipulate relevant provisions thereto in cloud outsourcing agreements. In the case of outsourcing of critical or important functions, financial institutions are required to ensure that:

- Clear allocation of information security roles and responsibilities between them and CSP exist (including in relation to threat detection, incident management and patch management);
- The strong authentication mechanisms and access controls are in place to prevent unauthorised access to data;
- The relevant encryption technologies are used, where necessary, for data in transit, data in memory, data at rest and data back-ups;
- Appropriate levels of network availability and network segregation are considered;
- The effective business continuity and disaster recovery controls are in place;
- Risk based approach to data storage and data processing locations is used;

Last but not least, financial institution need to ensure that CSPs comply with internationally recognised information security standards and have appropriate information security controls in place.

Timeline

The ESMA Guidelines are starting to apply as of 31 July 2021 and all outsourcing arrangements of in-scope firms with cloud service providers entered into or amended on or after this date will need to be structured in compliance with new requirements. Until 31 December 2022, all outsourcing agreements with cloud service providers concluded before 31 July 2021 need to be brought in line with new ESMA Guidelines.

EIOPA Guidelines on cloud outsourcing arrangements

Published in February 2020, the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA Guidelines) set out minimum requirements that insurance and re-insurance undertakings are required to comply with when entering into outsourcing arrangements with cloud service providers by following predominantly the principles contained in the aforementioned EBA and ESMA Guidelines.

Scope

Despite referring to the definition of "outsourcing" stipulated under Solvency II, the EIOPA Guidelines are limited in scope in the same way as the ESMA Guidelines by applying solely to outsourcing to cloud service providers. The EIOPA Guidelines apply to insurance and re-insurance undertakings both at undertaking at group level.

Guidelines

In its Guidelines, EIOPA has followed the principles stipulated by EBA Guidelines by requiring insurance and re-insurance undertakings to comply with:

- Governance requirements (especially to establish an outsourcing strategy, outsourcing policy, oversight function and perform continuous monitoring of outsourcing arrangements)
- Due diligence requirements (for the purposes of ensuring suitability of cloud service provider);
- Requirements on risk analysis (with respect to each proposed outsourcing arrangement under due consideration of relevant risks attached to it)
- Contractual requirements (clauses enabling insurance and re-insurance undertakings to comply with applicable requirements on outsourcing in the same way as described in previous chapters)
- Requirements on exit strategies and termination rights (in the same way as other financial institutions under EBA and ESMA Guidelines)

Insurance and re-insurance undertakings are required to differentiate between outsourcing of critical or important functions (previously known as material outsourcing under Draft Guidelines) other outsourcing arrangements in the same way as other financial institutions subject to EBA and ESMA Guidelines mentioned before.

Timeline

The EIOPA Guidelines have started to apply as of 1 January 2021 and all outsourcing arrangments entered into or amended on or after this date need to be structured in compliance with them. Insurance and re-insurance undertakings have until 31 December 2022 to bring existing outsourcing arrangements in line with new requirements.

Outlook

It is unquestionable that the ESA's Guidance framework on outsourcing has provided a valuable set of standards and requirements that financial institutions can follow when ensuring compliance with applicable requirements on outsourcing they may be a subject to under applicable sector specific pieces of EU and national legislation. However, there are small divergences between ESA's Guidelines and such lack of full alignment causes significant challenges for regulated financial institutions. Furthermore, given that the ESMA and EIOPA Guidelines apply solely to outsourcing to cloud service providers, there is a great number of standard outsourcing arrangements that will still need to be structured in accordance with high-level regulatory requirements on outsourcing stipulated by applicable EU legislation that frequently falls short of providing clear guidance for financial institutions.

Nevertheless, the process of harmonization of rules on outsourcing and operational resilience of financial institutions in general seems to be far from over. As part of its Digital Finance Package published on 24 September 2020, the EU Commission has published a proposal for Regulation on digital operational resilience for the financial sector (commonly known as Digital Operational Resilience Act, "DORA") that aims to harmonize EU regulatory requirements on digital operational resilience in financial services. In the same vein, beside requirements on management of ICT risks, DORA aims to bring certain requirements on outsourcing arrangements, onto a legislative footing.

Despite the fact that DORA may harmonize a number of questions related to outsourcing arrangements until it becomes operational (which from today's point of view is hard to expect before 2023) financial institutions will have to ensure compliance with requirements on outsourcing in accordance with the ESA's Guidelines and applicable sector specific pieces of EU and national legislation.

Help is at hand

If you have any questions please get in touch with:

Dr. Verena Ritter-Döring
Partner, Lawyer
+49 69 97130 0
v.ritter-doering@taylorwessing.com

Charlotte Dreisigacker
Associate, Lawyer
+49 69 97130 0
c.dreisigacker@taylorwessing.com

Miroslav Djuric, LL.M.
Professional Support Lawyer, Advokat
+49 69 97130 0
m.djuric@taylorwessing.com

© Taylor Wessing 2021

This publication is not intended to constitute legal advice. Taylor Wessing entities operate under one brand but are legally distinct, either being or affiliated to a member of Taylor Wessing Verein. Taylor Wessing Verein does not itself provide services. Further information can be found on our regulatory page at taylorwessing.com/en/legal/regulatory-information.