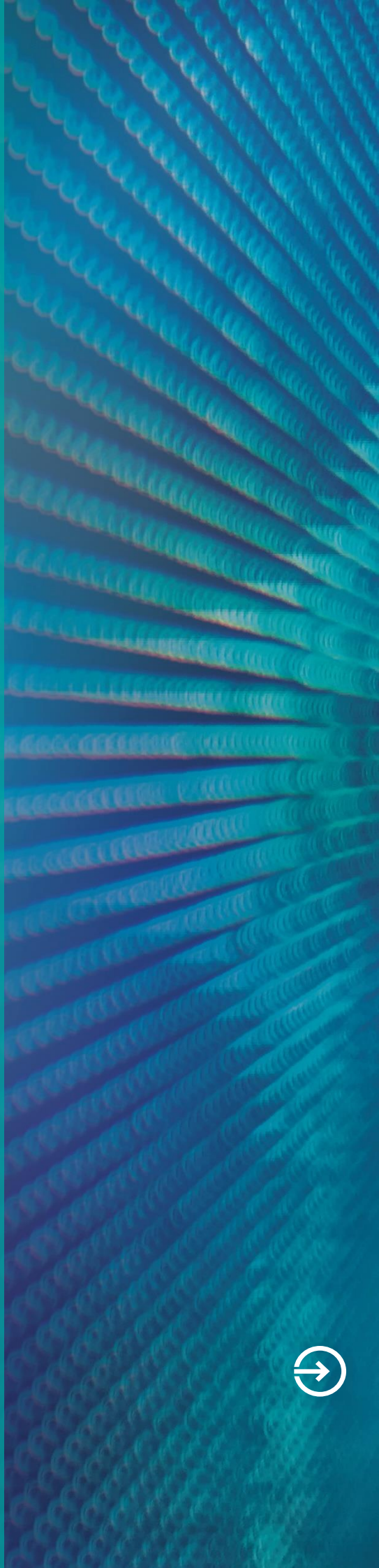
KPMG Law

Outsourcing and third party risk management –

Effective legal decision making to enhance compliance with regulatory expectations



April 2021

kpmg.com/uk

contents

Scope of insights paper 02

Topic 1: Non-outsourced third-party arrangements 03

Topic 2: Intragroup arrangements including third country branches 04

Topic 3: Contract expectations and the role of contract interpretation 05

Topic 4: Legacy contract remediation 06

Topic 5: Contractual clauses that support effective contingency planning and exit planning 07

Topic 6: Data Location 08

Infographic: how the Prudential Regulation Authority expectations have evolved and divergence to the EBA Guidelines on Outsourcing 09

Scope of insights paper

The PRA recently published its final position on outsourcing and third party risk management through PS 7/21 and SS 2/21. This insight paper focusses on those aspects of the PRA's final expectations which require a legal assessment and/or relate more generally to contracts.

For a more end-end overview of the PRA's final expectations, please read KPMG's insight paper called Outsourcing and third party risk management – Building resilience in your supply chain and meeting regulatory expectations.

The PRA also published its final position on operational resilience through a jointly issued policy statement (PS 6/21) with the Financial Conduct Authority and the Bank of England. That final position is closely connected with the PRA's final expectations on outsourcing and third party risk management and you can read KPMG's report on operational resilience called Generating strategic value from operational resilience – industry perspectives here.

For a visual on how the PRA expectations diverge from the EBA Guidelines on Outsourcing please see our Infographic page.

Topic 1: Non-outsourced third-party arrangements

PRA expectations:

"Firms are expected to assess the materiality and risks of all third party arrangements whether constituting 'outsourcing' or otherwise."

For non-outsourced material third party arrangements, firms are not expected to apply the same controls as for outsourcing arrangements but put in place equally robust measures commensurate to the materiality or risk-exposure. Specific requirements of the PRA's final expectations are also applied to this category of non-outsourced material third party arrangement, including risk assessment obligations and notification obligations.

The PRA's primary concern here is to ensure firms assess their relationships with all third parties and apply appropriate governance and controls irrespective of whether the firm would meet the definition of 'outsourcing' or not. This same approach applies to the PRA's Operational Resilience requirements which apply to all third party arrangements.

KPMG Law point of view:

"Risk assessments using the PRA's updated criteria is now expected over all third party arrangements. Third parties should be viewed with a wider lens than just suppliers. Achieving equivalent legal controls with such third parties will require assessment from a wide group of subject matter experts."

KPMG Law point of view: (cont.)

As part of compliance with the PRA's fundamental rules, firms should have already carried out some form of risk assessment over all of their third party relationships. However the PRA's expectation that firms risk assess using the specific criteria included in the supervisory statement will undoubtedly lead to some retrospective risk assessments. For example, some firms may not have subjected counterparties for services which are directly regulated by the FCA or PRA to the same level of rigour as non-regulated third parties engaged in outsourcing.

The range of these third parties should also not be limited to traditional suppliers. Responding to the above example, the PRA lists counterparties such as providers of clearing, settlement, custody services, and certain services provided by Lloyd's of London as being within scope.

This will be a challenge for firms. To support firms, the PRA's expectations are less prescriptive and enable firms to design and implement fit-for-purpose controls systems reflective of modern business practices. However, because the ambit of third parties is wide and therefore the types and norms of the contracts associated with those third parties will not be consistent, firms will need to take a different approach to legal controls.

An effective tool to deal with this challenge is the use of a contract risk framework. This framework will enable firms to map against the PRA expectations minimum and best practice clauses and other legal controls which should be available in their wider third party contracts. Legal subject matter experts in the particular type of third party contract can then overlay this framework with what is typical for that type of contract and whether alternatives exist to meet the outcomes expected by the PRA.

KPMG Law Tools and Accelerators:

1. Contract risk framework for non-outsourced material third parties

Topic 2: Intragroup arrangements including third country branches

PRA expectations:

"The PRA's expectations should be applied to both intragroup outsourcing and to third country branches in the UK. Firms should only rely on group processes and controls where they are compliant with the PRA's expectations."

The PRA considers that intragroup outsourcing should not be considered inherently less risky than third party outsourcing and firms should apply the PRA's expectations to intragroup as well as third party outsourcing.

Firms can comply with some of the PRA's expectations proportionately however depending on the level of control and influence the firm has over the group entity providing the services. The PRA has provided more detailed guidance than the EBA Outsourcing Guidelines in respect of the application of proportionality to intragroup outsourcing.

As a UK specific additional requirement to the EBA Outsourcing Guidelines, the PRA highlighted the need to treat all UK branches of overseas firms consistently following Brexit, including EU headquartered firms whose EU branches are made subject to the UK outsourcing rules.

KPMG Law point of view:

"Firms who have key dependencies for services on group companies (including UK branches of EEA firms) may need to depart from their group's policies and procedures. Groups with service company entities who sub-outsource services to third parties should include contractual controls to give regulated firms receiving those services effective control."

Although not driven purely by Brexit, the PRA's divergence from the EBA Guidelines in making UK branches of EEA firms subject to outsourcing rules is consistent with EEA countries now being 'third countries' from a UK perspective. The implication is that certain EEA firms will have to apply both EBA Guidelines and, in respect of their UK branches, PRA expectations in respect of material outsourcing agreements.

Intragroup outsourcing arrangements should be reviewed for compliance with the PRA's expectations. If firms do not have effective control and influence over their group service providers, contractual controls should be included to ensure regulated firms are able to demonstrate effective control contractually.

Specifically one area of concern has been ensuring group providers do not show preference for one group entity over another. This is typically dealt with through SMART KPIs (Specific, Measurable, Achievable, Reliant and Timely).

Another area of challenge is for group providers who sub-outsource services to third parties. If the regulated firms are not able to rely on every aspect of their group's processes and control, additional contractual provisions should be included, including the right for the regulated firm to exercise rights directly against the third parties and also ultimately the right to partially terminate those third party arrangements.

KPMG Law Tools and Accelerators:

1. Intragroup contract templates compliant with regulatory requirements
2. KPI Framework for intragroup arrangements

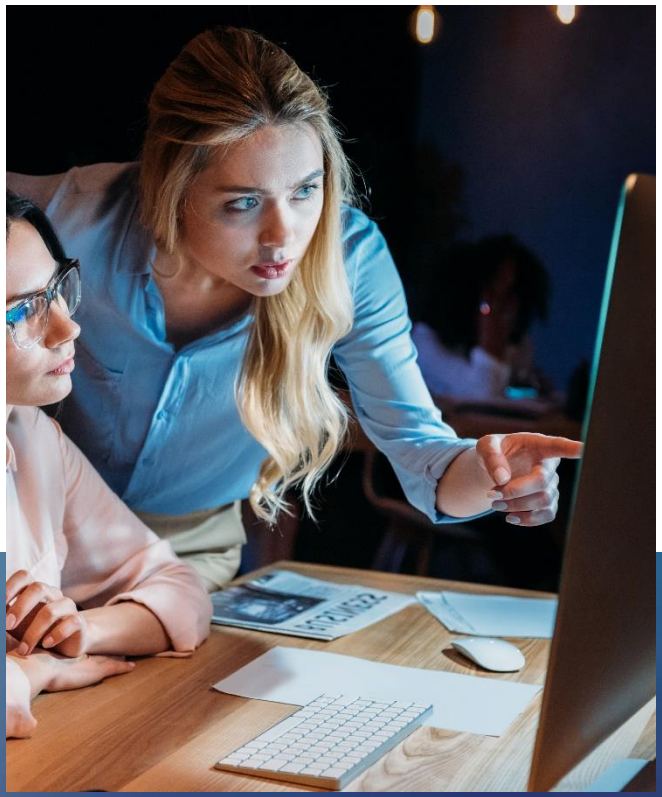
Topic 3: Contract expectations and the role of contract interpretation

PRA expectations:

"The PRA expectations contain minimum contract requirements and various other contract requirements that firms should consider including in their outsourcing agreements."

The PRA expectations are intended to ensure a consistent approach across PRA-regulated firms to all forms of outsourcing and, where indicated, other non-outsourcing third party arrangements entered into by firms.

By providing greater regulatory certainty on these requirements the PRA expects the final expectations will help to ameliorate the imbalance in negotiating power that may exist between smaller firms and dominant third parties. To monitor this the PRA also expects firms to make the PRA aware of any issue where a third party service provider is unable or unwilling to include the specific contractual provisions within the contract.



KPMG Law point of view:

"There is unlikely to ever be a universally accepted set of contractual clauses for outsourcing within financial services. Firms should be able to adopt contract interpretation to achieve commercially acceptable alternatives to contract language which still meet the PRA's expectations."

Given some of the PRA's expectations now also apply to material non-outsourcing third parties, a set of universally accepted contractual clauses for outsourcing within the financial services sector is unlikely to ever emerge.

Negotiating these contractual expectations with relevant third parties will, for certain expectations, still meet resistance where they may lead to uncommercial or operationally disruptive outcomes for them. For example, one of the PRA's expectations is that firms may elect to limit contractual termination rights to situations that, amongst others, "create risks beyond their tolerance". This will necessarily be a subjective assessment for a firm which, if exercised, might put at risk the unamortised investment a relevant third party has made in the relationship.

For these cases, we believe there is room for firms to adopt contract interpretation to meet the outcomes expected by the PRA but still reach a mutually acceptable position with their relevant third parties. In the above example, it should be possible to agree a right to terminate which, if the termination is exercised in circumstances where the third party is not in material breach (a universally accepted termination right), could give rise to some form of termination payment to the relevant third party. There may therefore be commercial trade offs that occur to achieve a compliant position. However we expect the PRA would want firms to consider if there are commercially acceptable alternatives to the language which still meet the PRA's expectations prior to notifying it of providers who are not willing to agree the necessary language.

Topic 4: Legacy Contract Remediation

PRA expectations:

"Legacy outsourcing arrangements entered into before 31 March 2021 should be reviewed and updated to comply with the PRA expectations at the first appropriate contractual renewal or revision point as soon as possible after the 31 March 2022."

Firms are no longer required to comply with, or inform the PRA if they miss, the timelines for reviewing material outsourcing arrangements as previously outlined in the EBA Outsourcing Guidelines. The implementation date has now moved to 31 March 2022. Outsourcing arrangements entered into or after 31 March 2021 should adopt the PRA requirements by 31 March 2022. Legacy outsourcing arrangements entered into before 31 March 2021 should be reviewed and updated to comply with the PRA requirements at the first appropriate contractual renewal or revision point as soon as possible after the 31 March 2022.

KPMG Law point of view:

"Firms (even smaller firms) will have a multitude of outsourcing arrangements. To ensure consistency of review and remediation, firms should adopt a programmatic approach to this expectation."

Reviewing and amending legacy outsourcing and third party arrangements can be a time consuming and resource intensive task. Firms should adopt a methodology which achieves consistency of results to make the effort count.

Aspects of this type of methodology we have worked with our clients on include:

- Prioritising contracts for review based on their renewal dates;
- A scoring system for contract reviews that ranks compliance with the PRA expectations on a weighted, qualitative basis;
- A standardised set of remediation actions linked to the final weighted score ensuring that standardised remediation steps are followed across the firm's contract portfolio; and
- Implementation of remediation steps by firm's supplier managers (or equivalent), to allow for open and constructive dialogue with third parties.

Remediation plans should include interim actions that supplier managers (or equivalent) can take in the short-term to close any compliance gaps.

Whilst the PRA's final expectation provides firms with timing latitude for updating legacy outsourcing arrangements, firms should not delay commencing the review of contracts which are due for renewal in the short-term.

KPMG Law Tools and Accelerators:

1. Contract Risk Framework for material outsourced third parties
2. Contract risk scoring & remediation plan methodology
3. Technology assisted contract reviews using KPMG's proprietary Ignite CCM tool
4. Contract templates for material outsourcing compliant with regulatory requirements
5. Risk-based clause library
6. Workflow tool using KPMG Law's Cloud Legal platform

Topic 5: Contractual clauses that support effective contingency planning and exit planning

PRA expectation:

"For each material outsourcing arrangement, firms should develop, maintain, and test a business continuity plan and document an exit strategy, which should cover both stressed exit and managed exits."

The PRA expects firms to develop their business continuity and exit plans, particularly for stressed exits during the pre-outsourcing phase.

The PRA's position on business continuity and exit planning is designed to complement existing guidance on Operational Resilience and Operational Continuity in resolution (OCIR). The PRA is primarily focused on the ability of firms to continue delivering important business services which are provided or supported by third parties, in line with identified impact tolerances.

KPMG Law point of view:

"For the successful execution of business continuity and exit plans there is a high dependency on firms having control over the operational assets that are necessary for the continuation of those services."

KPMG Law point of view: (cont.)

Examples of operational assets include data, intellectual property and process manuals. Firms should have a clear understanding of their operational assets and whether those assets are under the firm's ownership or direct control, or whether they are provided as a service by a third party. If it is the latter, firms should have the contractual controls necessary to ensure ongoing access to them. This could include provisions relating to software escrow, data ownership and the maintenance of a database of process manuals.

As identified above, firms must ensure that, prior to a contractual agreement becoming effective, they have evaluated the actions involved in delivering an effective stressed exit. The outcome of this evaluation should then be used to formulate the firm's exit plan, which in turn should be capable of enforcement under the contractual agreement. The PRA's approach effectively frontloads firms' contingency and exit planning requirements, putting a greater focus on pre-contractual due diligence.

To satisfy the PRA's requirements, the contractual agreement should impose direct obligations on the third party to maintain, comply with, review, update and test plans for business continuity, disaster recovery and exits. In order to increase their efficacy, these obligations should specify the frequency of review and testing of plans and the consequences of any deficiencies being identified, for example the need to update and re-test the plans in order to address those deficiencies.

It is important to note that contractual provisions such as those outlined above do not operate in a vacuum and should therefore be supplemented by robust, additional obligations relating to matters such as record keeping, audit and reporting obligations.

KPMG Law Tools and Accelerators:

1. Exit obligations matrix and template exit plans

Topic 6: Data Location

PRA expectation:

"The PRA expects firms to adopt a "risk based" approach to where their data is stored using GDPR-compliant mechanisms."

The PRA acknowledges the increase in the use of cloud technologies by firms as a means of improving their operational resilience through dispersing data across various jurisdictions and locations. However, the PRA expects firms to adopt a "risk-based" approach when ascertaining where data is stored, balancing the advantages offered by cloud computing as part of a firm's operational resilience planning against any data privacy risks that may arise.

Firms should be aware of any jurisdictions that fall outside their agreed risk tolerance and ensure that discussions take place to mitigate these risks as part of the pre-outsourcing phase. Any contractual arrangement should contain adequate data protection measures and firms should put in place the required GDPR-compliant mechanisms.

KPMG Law point of view:

"The PRA's expectation in this area and the European Data Protection Board's ("EDPD's") guidance following the Schrems II case are broadly complementary. There is an opportunity for firms to streamline their compliance with this expectation with their GDPR compliance activities generally by building on existing frameworks and processes."

However, the EDPB guidance mandates that entities have to undertake risk assessments relating to international data transfers both retrospectively and going forward. This differs to the PRA's stance that adoption of the requirements for legacy arrangements does not have to be retrospectively implemented but can be adopted at the next revision or renewal date. Firms should therefore follow the ICO and EDPB guidance when it comes to data localisation and not necessarily wait until March 2022 to implement the required controls.

KPMG Law point of view: (cont.)

The PRA also expects firms to consider "legal risks stemming from conflicting or less developed relevant legal or regulatory requirements" which indicates the need to undertake a broader analysis to cover regulations across a range of areas including data protection but also financial regulatory, and cybersecurity, amongst others.

Firms may wish to prepare a framework for conducting assessments of third countries' legislation covering both PRA and EDPB requirements. This should avoid duplication of work.

The expectation that firms must have robust controls in place for data-in-transit throws up practical difficulties for firms. In practice, firms may find it very difficult to keep control over their data flows due to the fact that they usually have a large number of operations and territories in which they handle information. This PRA requirement may lead to many firms being required to revisit their data mapping exercises.

We also note that third party cloud service providers may engage in "splitting" information into small portions - a common security measure – with the result that a firm's data may be physically stored in different locations in an automated way. This will make it more difficult for firms to identify where the information is physically located, and therefore knowing where a firm's data is "in transit" will be particularly challenging. Firms may have to renegotiate their outsourcing or third party arrangements to ensure they retain visibility over the service provider's automated processes in order to evidence controls over data "in transit".

A firm's record of processing ("ROPA") should therefore be updated to reflect the PRA expectation as to controls relating to data-in-transit (alongside the other PRA expectations pertaining to data security). By implementing the more prescriptive PRA requirements under a firm's ROPA, a firm can streamline its internal processes to comply with both the PRA expectations and GDPR obligations.

KPMG Law Tools and Accelerators:

1. Data transfer impact assessment tool

Infographic: How the PRA expectations diverge from the EBA Guidelines on Outsourcing

Key: **Notes of Divergence:** **PRA expectation compared to EBA Guidelines on Outsourcing**

More requirements **Fewer requirements**

Non-outsourced third party arrangements

Firms are expected to assess relationships with services providers and apply appropriate governance and controls irrespective of whether the third party is providing "outsourced" services or not

Intragroup arrangements including third country branches

The PRA requirements contain more detailed guidance than the EBA Outsourcing Guidelines in applying the proportionality assessment to intragroup outsourcing. The PRA requirements also bring third country branches into the scope of its supervisory statement

Contract expectation and the role of contract interpretation

The PRA requirements contain more prescriptive minimum contract requirements than are contained in the EBA Outsourcing Guidelines that firms should consider when drafting agreements

Legacy contract remediation

Firms are no longer required to comply with the timelines for reviewing material outsourcing arrangements as outlined in the EBA Outsourcing Guidelines

Contingency and exit planning

Firms are to have considered their exit plans for stressed exits before a contract is signed

Data location

Additional obligations on firms to implement required technical and operational measures, including data-in-transit

Usman Wahid

Partner & Solicitor– KPMG Law

M: +44 (0)20 7694 3316

E: usman.wahid@kpmg.co.uk

Christopher Overton

Senior Manager & Solicitor – KPMG Law

M: +44 (0)20 3078 3734

E: christopher.overton@kpmg.co.uk

kpmg.com/uk