ALLEN & OVERY

Consortia for digital innovation

In today's digital economy, rather than doing it alone, many organisations are finding that collaboration is a faster route to driving innovation or building new business models.

Alongside the more common arrangements for M&A, minority investing or strategic alliances, we are increasingly seeing a rise of consortia as a preferred route to bring together parties with a shared vision for redesigning an industry or a process or pushing the boundaries on a new application of technology.

Such consortia often include a number of industry peers, more naturally used to competing in their market. They may also include vertically integrated players, for example from along an industry supply chain. Some consortia will also include research organisations, technical specialists or governmental bodies who also share the common goal of building something new.

There are a number of reasons why consortia are particularly well suited to delivering innovation.

For a start, they offer the chance to pool resources to advance research and potentially develop a commercial offering beyond that which any of the members might be able to foster on their own. This offers more than just cost savings. It may also deliver better access to knowledge, best practice, connections and skills, and also the opportunity to share risk (perhaps even to enable more speculative research efforts).

Consortia by their very nature can be very helpful in building critical mass and momentum for adoption of a new approach, product or technology and can also help to jumpstart industry standardisation. A body of support for a new idea or product can also be a useful factor in early discussions with regulators and help ease the path to regulatory approval.

However, collaboration with others in the market needs to be carefully thought through and comprehensive planning at an early stage is a critical factor to success.

In this article, we step though some of the key areas to consider when planning for the use of consortia for digital transformation projects, focusing on how to add value while mitigating possible risks.

A clear understanding of scope and purpose from the outset

Participants must agree on the objectives and scope of the collaboration. What are the **must haves** for participants? With a large group of parties, early identification and minimisation of **red lines** is also important. A good business plan for the activities of the consortium will be essential. This plan needs to be clear on processes, deliverables, costs and timings, as this will help to manage expectations of members when the project is underway.

We recommend agreeing to these principles and capturing them in a detailed heads of terms before moving into drafting any more detailed documentation. Whereas, some transactions can do without a term sheet, the complexity of consortium arrangements is such that failure to have a clear road map can cause significant issues down the line. In our experience, early participation by lawyers in the planning stage yields considerable advantages in ensuring smooth negotiations. By flushing out key legal and commercial issues early on, the consortium should be able to address potential pitfalls by either recalibrating the membership or amending the scope of the project.

Corporate model

Consider what form the entity will take. Would it be a contractual arrangement or some form of special purpose vehicle (in the UK typically a private limited company)? Explore whether any of the potential members have any specific characteristics or requirements (legal, accountancy or policy) that may limit or, worse, prohibit their participation (for example maximum stake sizes or control rights).

Contribution

Consider how to fund all aspects of the consortium, from management of the entity through to any development and roll out of the eventual output of the business – including both timing of tranches of financial contributions and share of contributions between members. As noted above, a clear business plan with anticipated cash requirements is essential in providing certainty but, where this is not possible, thought will need to be given to the circumstances (if any) in which the consortium can require its members to make additional contributions. If such a provision is included, members may still require caps on their liability to contribute. It is important to consider here how any assets contributed by parties to the consortium will be compensated for and protected (for example, intellectual property). Give consideration as to what will happen should a member default in its contribution obligations. A sliding scale of sanctions (from censure through to suspension of rights or, ultimately, a forced sale) may be considered, depending on the specific commercial requirements of the consortium.

Membership and governance

Consider membership criteria and how to ensure that the right skills and knowledge are represented within the consortium through its membership. Consider how decisions should be taken within the consortium (eg voting rights of members, rights to appoint directors, veto rights, quorum for meetings of consortium members, etc) and who will fill key management roles.

It is also important to agree what **good** participation looks like to mitigate against any disagreements about whether members are **pulling their weight** on the project. In practice, ensuring that incentives for members are aligned will also help achieve this effect. Ensure that a dispute resolution mechanism is agreed upfront and that it allows for swift resolution of disputes. Finally, all of these points will need to be reviewed in light of each consortium member's individual governance and compliance policies (including in relation to anti bribery and corruption prevention).

Exit and new participants

A common challenge in consortium agreements comes down to two key questions: when and how can I exit? Similarly and closely linked to the question of membership criteria, the question of how and in what manner new participants may join is often a point of discussion.

In forming the consortium, careful thought must therefore be given to a wide range of inter-related points, including: subscription mechanics; criteria (if any) for new shareholders; restrictions on transfer of shares; change of control scenarios (including drag and tag rights); walk-away rights; and the consortium's ambitions for IPO or sale. Ultimately, the consortium documents must balance the desire to protect the interests of the members with the need to allow the consortium sufficient flexibility and authority to grow and develop.

Antitrust and merger control

Regulators do take an interest in the information sharing that occurs within consortia and may also have concerns about a consortium's ability to influence industry standards (including pricing). One of the key antitrust considerations is whether information exchange between members is necessary to deliver the purpose of the consortium (and to benefit customers/participants). Information of a commercially-sensitive nature from the consortium members or other competitors should not be the subject of discussion within the consortium and, in addition to setting policy in this regard, certain technical measures may also be relevant (eg firewalls). As well as an appropriate policy for consortium members in this regard, training should be given to members throughout the life of the project.

Upfront consideration will also need to be given to merger control. In the event that filings will need to be made to antitrust authorities, consideration needs to be given to the impact of this process on the overall transaction timetable including whether a split sign and close may be required.

Intellectual property

The IP issues involved in forming and operating (and ultimately terminating) a consortium are much more numerous than would typically apply to a straightforward investment, or on a merger or acquisition. The pitfalls are also more insidious. Potential collaborators consistently cite the potential loss of background IP rights as a major risk in such structures.

Different issues arise at different stages in the lifecycle of a consortium or indeed other collaborations:

– At the pre-contract stage of any collaboration, confidentiality concerns will often be paramount, if potential collaborators share information for the purposes of evaluating and structuring a deal. Due diligence on IP issues is increasingly thorough. Structural aspects, often driven by tax and competition considerations, will also be important.

– At the formation stage, the parties will need to consider the assignment and licensing of existing rights for the purposes of the collaboration between the parties, including the terms of transfer and the value of their respective IP contributions as a component of the commercial terms.

– During the life of the collaboration, key issues include obligations to make future contributions of existing and future background rights, the ownership and exploitation of "foreground" rights (ie rights arising from the collaboration between the parties) and the maintenance and protection of foreground rights. For IP-rich businesses, rigorous IP protection and governance is essential. A well-developed and consistently applied policy supported by a strong contractual framework are essential foundations.

– On termination, the parties will benefit from having considered and catered for both unexpected and expected termination events in advance, particularly to ensure that neither party is blocked from continuing its business outside the collaboration, although it is difficult to anticipate every scenario and a certain amount is likely to be left to be agreed at the point of termination

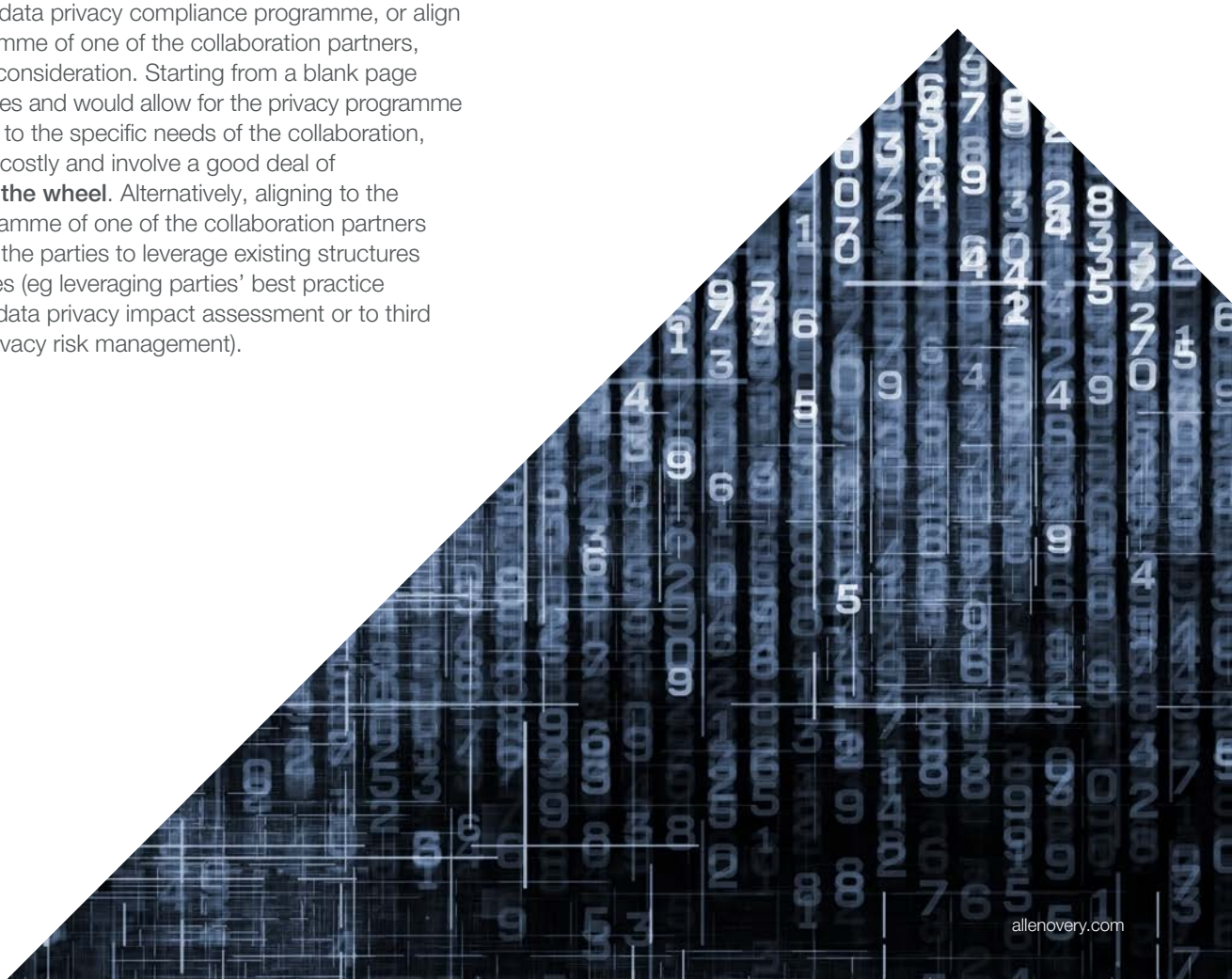
Data

To the extent that personal data is processed as part of the substantive activities or offering of the consortium, the parties may wish to consider:

– A key requirement under General Data Protection Regulation (GDPR) is to practise **privacy by design**. To this end, the establishment of any collaboration should involve some consideration of data privacy issues at the design and structuring phase. Clearly, the amount of time to dedicate to this should be flexed, on a case-by-case basis, to adopt a proportionate approach which is appropriate to the extent of data processing, the importance of that data processing to the business model and to the level of risk involved. Matters that it would be valuable to consider at the outset include what scope of use of personal data is contemplated – by considering this at the outset, privacy notices and other privacy compliance measures can be tailored to ensure data is collected in a manner that gives the collaboration sufficient flexibility to use that data for its business purposes.

– Any business involving processing of personal data should have some form of data privacy compliance programme, comprising policies, processes, governance, training and other tools. Whether the collaboration will operate under an independent data privacy compliance programme, or align to the programme of one of the collaboration partners, will be a key consideration. Starting from a blank page has advantages and would allow for the privacy programme to be tailored to the specific needs of the collaboration, but could be costly and involve a good deal of **re-inventing the wheel**. Alternatively, aligning to the privacy programme of one of the collaboration partners could enable the parties to leverage existing structures and processes (eg leveraging parties' best practice approach to data privacy impact assessment or to third party data privacy risk management).

Personal and non-personal data is increasingly recognised as a valuable asset of any collaboration. Accordingly, increasingly it is addressed as an asset class as part of the commercial agreement, alongside intellectual property rights and other assets. The commercial agreement between the parties should address similar issues to those considered with intellectual property rights, including who **owns** the rights (if any) in data, who has the right to exploit that data and how those rights might be affected by events (eg termination events), who is responsible for maintaining that data and who is responsible for enforcing rights against third parties and defending actions brought by third parties. There are additional data privacy-specific considerations as well, such as allocating which party or parties will be responsible for dealings with data subjects, data protection authorities and other third parties, which party will be responsible for meeting statutory requirements (eg to report data breaches), and how liability should be allocated between the parties in the event of enforcement action or claims.



Taxation

Tax considerations for a collaboration begin with the choice of entity for the collaboration: whether to choose a tax opaque entity (typically a company) or a tax transparent one (typically a partnership). This will need to be considered in light of the parties' tax objectives in respect of the collaboration.

At the outset, parties will need to decide how they want to fund the collaboration, and assess how any arrangements around investor equity and loans will interact with the investors' individual tax profiles. It will be important to ensure that future profits can be extracted without tax leakage.

The provision of assets and services between the investors and the collaboration entity, in terms of both initial contributions of assets and ongoing supplies such as IP licensing and management services, can also have tax consequences which will need to be taken into account.

Depending on the jurisdictions involved, it may be possible to achieve some tax profit/loss sharing between investors and the collaboration entity, which can add value for all parties.

In the tech space, another potential tax positive is that the activity of the collaboration may attract valuable tax incentives for R&D. It is important to think from the beginning about whether any conditions for these incentives would be satisfied, and ensure that they are not unnecessarily failed!

The tech industry is, however, subject to increasing attention from tax authorities because of the geographical mobility of its profits, and the digitalisation of the global economy has become the focal point of discussions around international tax reform. Some jurisdictions are already introducing new taxes intended to capture these profits, such as taxes on offshore receipts from locally exploited intangibles, and digital services taxes. The picture here is live and changing, and will need to be kept under review by the collaboration on an ongoing basis.

Regulatory changes

The regulatory landscape for technology companies has shifted considerably over the last few years and, if policy proposals discussed by governments around the world are anything to go by, this is a trend which is set to continue. Layer on to that the increased geopolitical tensions which face certain technologies (such as machine learning and communication networks) and it is clear that a clear and robust approach on regulatory risk is essential to any consortium wishing to engage in innovative tech. An early understanding of the current regulatory landscape, the direction of travel by policy makers, and the potential impact of both on the underlying technology or business of the consortium can therefore be an important strategic differentiator for the project. In areas where the future regulatory landscape is truly uncertain (for example, artificial intelligence), instructing political consultants or lobbyists may also be relevant.

Key contacts

Will Samengo-Turner
Partner – London
Tel +44 20 3088 4415
william.samengo-turner@allenovery.com

Philip Mansfield
Partner – London
Tel +44 20 3088 4414
philip.mansfield@allenovery.com

Tim Harrop
Counsel – London
Tel +44 20 3088 3983
tim.harrop@allenovery.com

Nigel Parker
Partner – London
Tel +44 203 088 3136
nigel.parker@allenovery.com

UK
CS2012_CDD-62359