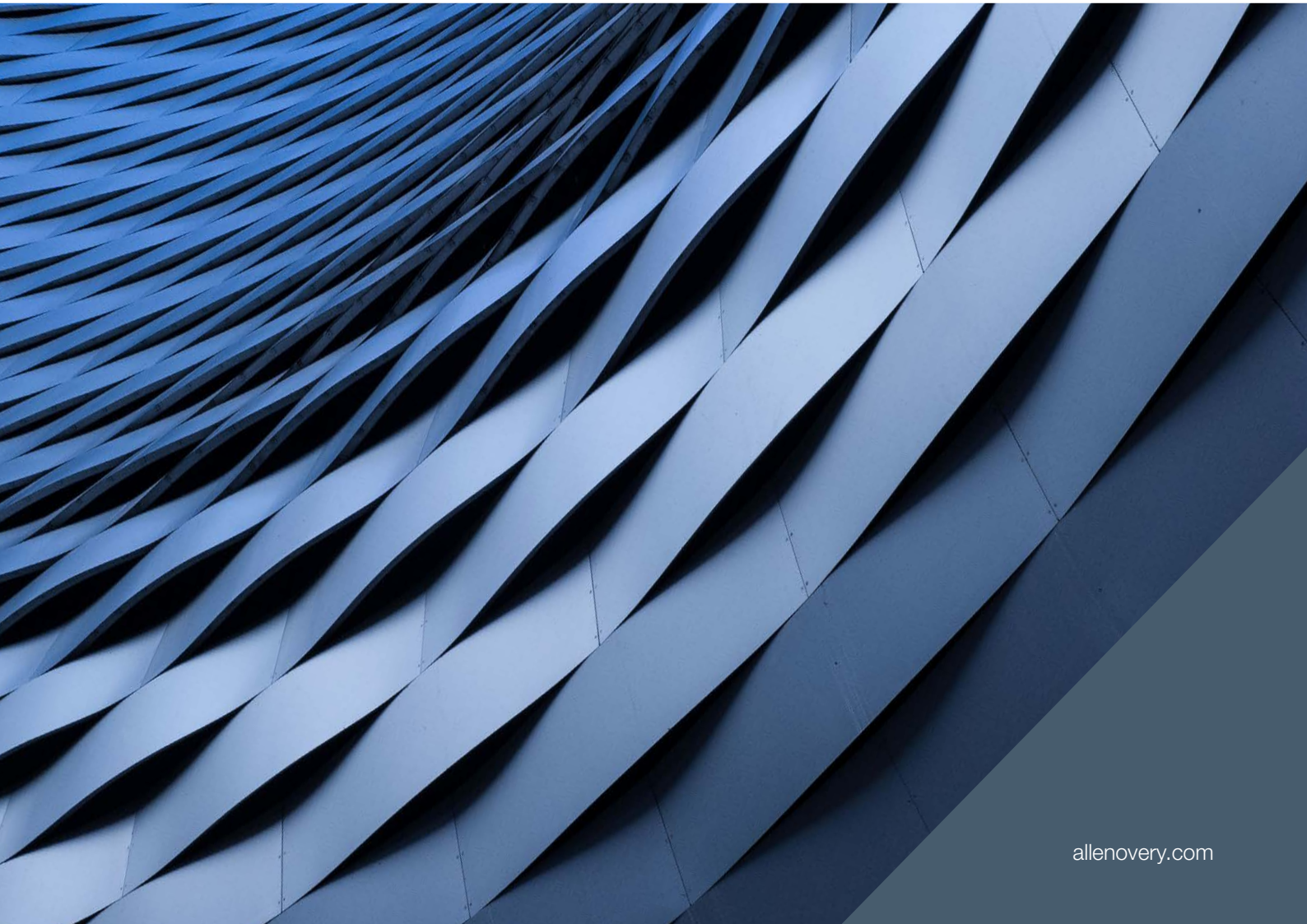


A&O Insight:

# Russian invasion of Ukraine – Implications for commercial parties

The human cost of Russia's invasion of Ukraine is devastating. It is rightly the focus of attention around the globe, including for commercial parties with operations or business relationships with a Ukrainian, Russian or Belarusian nexus. Parties are also having to consider the myriad of other implications.

Here are **twelve key points** we've been considering with our clients when supporting them in responding to the crisis.



## 1. Compliance (and co-ordination)

A critical first step for many has been ensuring compliance with sanctions and other restrictive measures. This is no easy task, not least because sanctions change quickly with little notice and with immediate effect. Multiple overlapping non-identical regimes (eg U.S., UK and EU) may need to be considered. The law can bite extra-territorially: either directly on nationals based outside the jurisdiction or indirectly via exposures to U.S. secondary sanctions risks. There are also licensing regimes to consider – parties must track any general licences and also consider whether to apply for a specific licence. All of this is highly fact dependent, so any analysis in relation to one issue will often not apply to others. And breach of sanctions can of course be a criminal offence.

Those with operations in Russia are also having to consider important changes to Russian laws in response to what has happened, some of which also create criminal offences and are being introduced at speed. A considerable degree of co-ordination and oversight is required to help manage compliance and keep up to date. We have been recommending that clients have a dedicated senior team in place, reporting to management, to take responsibility for assessing and managing the potential impact of what is happening across the different functions in a business, wherever they are based.

## 2. Managing the impact on your workforce

Employers affected by these events must navigate difficult issues in rapidly changing circumstances. This ranges from ensuring the welfare of workers in Ukraine, Russia and elsewhere, to managing the impact of sanctions, changing laws and business disruption for the workforce. Subject to local law requirements, you may need to consider:

- The safety and security of workers in directly affected jurisdictions, including issues around relocation and repatriation where appropriate (noting that most Ukrainian men aged 18 to 60 are currently prohibited from leaving the country).
- Workers' wellbeing and measures to support their mental health, including resources such as employee assistance programmes and adjustments to allow them space or flexibility.
- Compliance with any travel restrictions and any governmental advice around travel.
- Compliance with applicable export controls, for example by preventing access by Russian employees to certain knowledge or technology, where necessary.
- For those who take the decision to withdraw from Russia, to suspend their operations or to take a public stand against the invasion:
  - The direct impact of any restructuring or closure of Russian operations for the workforce, including the need to consider Russian employment laws.
  - How to implement any temporary measures, such as putting workers on unpaid leave, laying them off or changing their employment terms, in a legally compliant manner.
- The impact on Russian workers of proposed Russian legislation targeting foreign businesses taking these steps.
- Ensuring that Russian workers are not involved in any acts or decisions which could be portrayed as them assisting a foreign entity contrary to Russia's interests since this could amount to treason. This could include making a charitable donation to the Ukraine relief effort.
- Whether it is possible to pay staff in Russia in light of banking restrictions (noting the penalties under local legislation for late payment of wages) and whether there are alternative solutions that do not breach sanctions.
- How to communicate in a way that mitigates any risk of criminal liability under recent Russian legislation on "fake news", including by keeping written communications with workers to a minimum where appropriate.
- The support and management of any displaced workers, including compliance with local immigration rules and any contractual, tax and employment law repercussions of their change of workplace.
- How to manage requests made by workers for leave of absence to join the armed forces in Ukraine or Russia in a legally compliant and consistent way.
- Reminding your workforce of your policy on bullying and harassment and ensuring that potential differences of opinion between workers over the crisis are managed consistently with discrimination laws.

### 3. Performing and enforcing contracts

Many parties are also assessing whether sanctions, other restrictive measures or the wider disruption caused by the Russian invasion might affect contractual performance, either directly or indirectly, for example due to issues in the supply chain or the impact of energy price rises. If you are in this position, consider:

- Specific clauses and the steps required to exercise rights under those clauses (and whether those steps are themselves compliant with sanctions). See point 8 below for a discussion of potentially relevant provisions in the funding context.
- Consequences that may arise by operation of law in any relevant jurisdiction, for example the discharge of a contract due to force majeure or frustration, obligations to comply with mandatory laws, local law formalities or reporting obligations, or obligations to document disruption to the supply chain or an inability to perform, for example when asserting force majeure.
- Other factors that could inform your approach, for example market practice, regulatory rules or guidance, or the impact on related agreements.
- The consequences of taking particular steps – are you discharged from your obligations or are they just suspended or amended, and are those consequences

themselves compliant with sanctions?

- Where any disputes will be resolved. Many agreements with a Russian nexus will provide for disputes to be resolved by arbitration, but you may need to assess the risk that the Russian courts will take jurisdiction over your dispute irrespective of an agreement to the contrary. You may also need to assess whether you have assets in Russia (or elsewhere) against which a Russian judgment might be enforced.
- Whether renegotiation of your agreement is necessary, desirable or lawful and, if you do decide to renegotiate, what you need to do to ensure any amendment is effective. You may also need to consider whether any renegotiation gives rise to a clawback risk in any subsequent insolvency.
- If there is more than one route open to you, which one will give you the best outcome legally and commercially and what is the right thing to do in a wider sense?
- Whether sanctions legislation provides protection from being sued or from being liable for non-performance, at least in your home jurisdiction, even if not elsewhere (under so-called “no claims” and/or “no liability” provisions). In practice this protection (and the location of your assets) may significantly influence your decision-making.

### 4. Operational and supply chain risks

Some of our clients are also having to consider wider operational impacts. For example:

- For those who take the decision to withdraw from Russia or suspend or alter their operations:
  - How to manage the process of halting “business as usual” activities, where necessary. This may involve selling operations, suspending them temporarily, or winding them up.
  - Security implications for premises and assets if activities are halted and staff are no longer available on the ground.
  - Local law implications of taking particular steps, including corporate and directors’ responsibilities and liabilities (at both an entity and controlling shareholder level), compliance with tax and other administrative laws and risks from any prohibition on repatriation of assets.
  - Risks arising from loss of control over, or lack of use of, intellectual property rights (for example trade marks or trade secrets).
  - Whether to appoint additional or alternative directors and/or issue powers of attorney to allow particular individuals to act on behalf of a Russian company, with a view to mitigating risks for specific individuals.

- Environmental, social and governance (ESG) compliance, including in relation to human rights issues.
- How to manage the new EU, UK and U.S. export controls on Russia, which could have a significant impact on existing supply chains, since many exports are now prohibited. The provision of certain services to Russian persons is also now prohibited. There are also restrictions on certain money transfers and foreign currency payments under sanctions laws and Russian counter-measures. Additionally, the withdrawal of “most-favoured-nation” status from Russia by a number of jurisdictions could result in a considerable additional cost being imposed on imports from Russia. Supply chains may need to be re-assessed in this light.
- How to provide information (for example to authorities) or obtain accurate translations (for example of legislation or statements) or signatures where business as usual operations have been disrupted.
- Managing reputational issues and responses to stakeholder queries or press enquiries, bearing in mind that the use of certain phrases is a criminal offence in Russia.



## 5. Sector specific issues

In some sectors, including aviation, consumer and retail, telecoms, maritime, energy and natural resources, real estate, critical infrastructure, commodity trading,

fund management and financial services, there have been very specific issues to consider. Please do get in touch if you would like to discuss these.

## 6. Corporate issues

Both the invasion itself and the financial sanctions imposed in response are having a significant impact on financial markets and companies. In addition to the other points raised elsewhere, companies will need to:

- Determine the risks and impact of these events and the resulting sanctions on the company's business.
- Ensure compliance with directors' duties in circumstances where many directors are having to navigate potentially conflicting obligations and take exceptionally difficult decisions.
- Comply with rules on donations.

- Consider the impact of market volatility on pension schemes.

In addition, listed companies will also need to consider carefully:

- Any formal disclosure and announcement obligations and any need to keep the market updated (including making a holding announcement where more time is needed to better assess the impact of events).
- Any need to confirm the impact of sanctions on the company's ownership or control.
- How to respond to investor scrutiny and demands.

## 7. Intellectual Property (IP)

Russia has exercised a compulsory licensing regime of intellectual property rights to try to mitigate the economic effect of international sanctions. This means that patent and industrial design owners from territories that have sanctioned Russia are not entitled to compensation for the unauthorised use of their intellectual property. There is also a new law that will remove or restrict IP protection for certain goods (most likely to be medicines and software but it could be broader). This is expected to cover all the main IP rights (trade marks, patents and copyright).

There may be little that intellectual property owners can do at this stage to protect their rights in Russia. However, it will be important to keep a close eye on what is happening and to document decisions and events with a view to taking action in the longer term where appropriate, for example via claims for breach of international intellectual property agreements or investment treaty claims for expropriation of assets.

At the moment it is still theoretically possible to apply for and renew trade marks in Russia provided any steps taken comply with sanctions rules.

## 8. Funding

Where a borrower is (or may become) a sanctioned entity, lenders may have to consider:

- Payments – can the agent or the lenders accept payment from a sanctioned borrower? Where the borrower is not sanctioned, can it access payment systems (eg SWIFT) if its bank account is held at a sanctioned bank that is no longer permitted to use SWIFT?
- Capital and exchange controls – can a non-sanctioned Russian borrower pay in the contractual currency in light of Russian capital or exchange controls and/or redenomination laws?
- Drawstop – does the imposition of sanctions trigger a legal and/or contractual basis for lenders to refuse to lend to a sanctioned entity? Is the analysis different where the borrower is Russian (or Russian owned/controlled) and could become a sanctioned entity if territory-wide sanctions are imposed on Russia?
- Events of default – is there an event of default and, if so, are any of the remedies available to lenders? In the case of secured deals, where is the security located?
- Jurisdiction – is there a risk that the borrower will be able to bring proceedings in Russia, irrespective of the disputes clause in your agreement?

Where the lender is a sanctioned entity, consider:

- Payments – can the borrower make payments to the agent (and thereby discharge its debt) if the agent agrees to freeze the amount due to a sanctioned lender (even though the agent acts for all lenders and payment to it is equivalent to payment to all lenders)? In a debt capital markets context, where an issuer of an outstanding bond is aware that a bondholder is a sanctioned entity (perhaps because the bond was originally structured for that holder), it may want to consider appropriate steps with the clearing systems, as well as its agent.
- Partial payments clause – if the borrower deducts any amounts due to a sanctioned lender when making a payment, can the agent distribute to the other lenders irrespective of the obligation to pay pro rata to all lenders under the partial payments clause?
- Enforcement – if the sanctioned lender is the majority lender, could enforcement of share security, or the automatic transfer of voting rights on an event of default, result in the sanctioned lender “controlling” the borrower for the purposes of sanctions and therefore in the borrower itself becoming a sanctioned entity?

Parties may also need to consider whether the sanctions on Russia impact on the legality of intra-group financing arrangements involving Russian entities (and any consequential implications for the solvency of the relevant entities).

## 9. Personal data, cybersecurity, confidential information, paper trails and privilege

In relation to personal data, you may wish to:

- Be mindful of data protection requirements if you are embarking on new forms of data processing in the context of your emergency response (for example if re-patriating employees, addressing travel and other restrictions or supporting displaced people), including considering the legal bases for processing.
- Assess data security risk in directly affected jurisdictions. Depending on the scope of processing operations and the nature of the data streams, consider whether access to and from systems based in Ukraine, Russia and Belarus should be restricted or the data securely retrieved, in each case to protect against data breach and high risks to the rights and freedoms of individuals. If control over data is lost, consider whether this amounts to a personal data breach and take steps to mitigate its consequences and comply with notification obligations.
- Re-assess existing safeguards in place to support regulatory compliant international transfers of personal data where these may be at risk, including: the basis on which data is transferred to or accessed from directly affected jurisdictions; country and data transfer impact assessments for those jurisdictions; and the effectiveness

of any supplementary measures. If it is impossible to implement measures that enable a compliant international data transfer, consider how to achieve business aims without reliance on those data transfers. Consider immediate restrictions on data processing (full or partial) or destruction of the data if your assessment identifies high risks.

- Keep assessments under review as operational decisions are taken and as the political and legal landscape develops in Ukraine and Russia, including by monitoring any new emergency legislation for its potential impact on data protection, privacy and information security.
- Review your data protection contracts with counterparties in Ukraine, Russia and Belarus, as well as any agreements with any other entities in relation to processing personal data in these jurisdictions.

In relation to non-personal data and other information, you may wish to:

- Keep a record of decisions and steps taken in response to the crisis and preserve the documents you create, for example where this may be necessary to comply with obligations, support claims in any future dispute, or demonstrate efforts to comply or mitigate risk.

- Consider whether and how documents and data might be protected from disclosure in any dispute on grounds of legal privilege (or otherwise), but be aware that this will not protect all information.
- Assess confidentiality and security arrangements relating to trade secrets and other confidential information that may be accessible in, or from, the conflict zone. Consider the enforceability of contractual provisions in practice.
- Consider the security of your systems operating in Russia and Belarus in light of sanctions imposed and the risk of governmental access potentially exposing or compromising systems. Consider the risk of IT suppliers suspending sales and support of existing products in these jurisdictions.
- Monitor developments in relation to infrastructure, media and internet access to ensure that restrictions or blocks on the same do not inadvertently limit your access to your own data and information. Secure any business-critical data hosted or accessed from these jurisdictions.
- Review your cybersecurity protections in light of the increased risk of state-sponsored cyber-attacks. Consider:
  - Reviewing advice provided by regulatory and expert bodies, refreshing risk training and policies, and reviewing security systems, access rights, passwords and privileges.
- Revisiting and testing your business continuity plans and back-ups and ensuring familiarity with incident processes. You may also wish to consider shortening escalation procedures to respond to threats and/or increasing service levels to ensure a faster response.
- Reviewing cybersecurity protections in your supply chain to identify and address weaknesses.
- Monitoring systems for potential misuse by any threat actors or use by activist employees participating in the information war between Ukraine and Russia.
- Reinforcing your defences against ransomware attacks, bearing in mind that paying ransoms under current circumstances might result in liability for financing war and violation of sanctions.
- Establishing partnerships with national and international security teams.
- Monitoring closely any legislative and regulatory developments for new obligations in the area of information security and cybersecurity generally and in relation to your specific sector or industry.

## 10. Insurance implications

Commercial parties and their insurers will want to review their policies to check whether losses incurred are covered. Consider:

- Exclusion clauses – certain claims might be excluded by “war risks” or “cyber war” exclusion clauses.
- Notification requirements – parties who have incurred losses or who may incur losses as a consequence of the invasion should check the notification requirements under their policies and comply strictly.
- Consent requirements – insured parties may also need insurer consent before taking certain steps to respond to events (for example, terminating contracts, commencing proceedings or incurring legal fees).
- Mitigation – it may also be necessary to consider whether mitigation activities fall under any available head of cover.
- Limits on cover due to sanctions – the sanctions regimes in some jurisdictions (including the UK and the EU) limit the ability to provide cover in certain circumstances.

## 11. Insolvency risks

Businesses with substantial exposures to Russia, Belarus and Ukraine are facing severe disruption and uncertainty which may lead to the rapid onset of acute financial distress. In addition to the serious difficulties resulting if sanctions are imposed on persons directly or indirectly involved in the business, many businesses are anticipating near term liquidity issues caused by the unavailability of finance, particularly in the capital markets, supply chain disruptions and material deterioration in asset values and the reduction or even cessation of intra-group revenue streams. Businesses that are not directly affected may also experience financial distress as a result of indirect effects of the conflict and the resulting imposition of sanctions, such as material increases in prices for essential commodities such as oil and gas.

Severe financial distress may result in directors needing to file for insolvency proceedings to satisfy mandatory requirements in certain jurisdictions. Directors should take

advice and consider their duties carefully to ensure that the interests of all relevant stakeholders are being given due consideration and that the directors are complying with their fiduciary obligations. In particular, directors should be mindful of making significant payments to creditors outside the ordinary course of trading. Consideration should also be given to any other liabilities that could potentially arise, both for local directors and other individuals or group entities. In some cases directors may need to consider their ability to access advice and insolvency officeholder support.

The feasibility of implementing a balance sheet restructuring may be impacted by challenges in valuing or obtaining access to or control over assets which are located in, connected to or otherwise dependent on Russia, Belarus and Ukraine. Sales processes of such assets are likely to be similarly affected. We expect to see near term standstills and forbearances, with a focus on equality of treatment between creditors and preservation of assets.

## 12. Proposed deals

In relation to any new deals, the parties will need to consider whether sanctions prohibit or restrict the negotiation of or entry into particular transactions. Care may need to be taken in relation to which employees are party to any decisions, as well as communications, such as emails or meetings, in which such transactions are being discussed.

On any deal with a Russian nexus, parties may also need to consider their disputes clauses, including whether to provide for disputes to be resolved in a jurisdiction that has not imposed sanctions on Russian entities. This may in some cases help to reduce the risk that the Russian courts take exclusive jurisdiction over any dispute.

### M&A activity

Uncertainty tends to dampen M&A market activity, and it may be that the activity and valuation levels we have seen in recent years will start to moderate. Deals involving sanctioned entities, people or assets will, in most cases, be completely off the table. Potential acquisitions of companies with particular exposure to the situation will come under a high degree of scrutiny, and due diligence to assess a target's potential exposure is likely to be key; even targets with no obvious direct exposure to the situation may face supply chain disruptions and price increases. Contractual protections may be less relevant than determining whether or not an affected acquisition can or should proceed at all and, if so, at what price. In terms of foreign direct investment controls, transactions involving Russian investors may well face in-depth reviews and extended timelines.

Ceasing activities in Russia may also involve disposing of companies or businesses. These disposals will obviously need to be structured carefully to comply with sanctions and Russian laws, where applicable. They are also giving rise to some novel considerations. For example: Should the

disposal be for a nominal consideration? Should there be a call option over the entities sold? How best to separate local businesses from the rest of the parent group in the absence of a typical transitional services arrangement? What are the implications of the current situation on governing law and dispute resolution choices as well as antitrust considerations?

### Capital Markets

There is currently significant volatility in the capital markets. In particular, we anticipate a significant reduction in initial public offering volumes, but a potential for greater volumes of follow-on equity raisings and other transactions. Parties involved in new debt securities issuance or debt programme updates may need to review the wording of sanctions language in documentation and consider risk factors and other prospectus disclosure depending on the impact of the invasion on the issuer's or guarantor's business. Issuances by sanctioned entities in relevant jurisdictions will clearly not be possible. Issuers may also see adjustments to the wording of sanctions confirmations required by competent authorities and stock exchanges when submitting documents for review and listing purposes.

### Funding

When entering into new credit agreements, parties should review the sanctions language to determine whether any updates are required. Lenders may wish to consider whether the sanctions provisions will operate as they would like them to and look at whether there is any way of improving their position if new sanctions come into effect. Parties may also want to consider how they can disenfranchise sanctioned lenders in the future and whether they can make amendments to allow the agent to make payments to all lenders other than a sanctioned lender.



## Contacts

---

**For more information on the potential impact of these events on your business or transaction, please speak to your usual A&O contact or one of the following.**



**David Broadley**  
Partner and Global Co-Head –  
London, Corporate  
Tel +44 20 3088 3258  
david.broadley@allenoverly.com



**Dirk Meeus**  
Partner and Global Co-Head –  
Brussels, Corporate  
Tel +32 27 802 432  
dirk.meeus@allenoverly.com



**Karen Seward**  
Partner –  
Silicon Valley, Litigation  
Tel +16 50 207 0581  
karen.seward@allenoverly.com



**Vicki Liu**  
Co-Head of Global Banking  
Practice and Managing Partner –  
Hong Kong, Banking  
Tel +85 22 974 7027  
vicki.liu@allenoverly.com



**Philip Bowden**  
Partner – London, Banking  
Tel +44 20 3088 2511  
philip.bowden@allenoverly.com



**David Lucking**  
Partner – New York, ICM  
Tel +12 12 756 1157  
david.lucking@allenoverly.com



**Emma Dwyer**  
Partner – London, ICM  
Tel +44 20 3088 3754  
emma.dwyer@allenoverly.com



**Karen Birch**  
PSL Counsel – London, Litigation  
Tel +44 20 3088 3737  
karen.birch@allenoverly.com

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen & Overy (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen & Overy LLP and Allen & Overy (Holdings) Limited are authorised and regulated by the Solicitors Regulation Authority of England and Wales. The term partner is used to refer to a member of Allen & Overy LLP or a director of Allen & Overy (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of the members of Allen & Overy LLP and of the non-members who are designated as partners, and a list of the directors of Allen & Overy (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

© Allen & Overy LLP 2022. This document is for general information purposes only and is not intended to provide legal or other professional advice.