

Morgan Lewis

DIGITAL INNOVATION AND DISRUPTION

2021-2022 WEBINAR SERIES

Tech and Sourcing - The Year in Review

May 17, 2022



Technology Marathon 2022

Our Technology Marathon is an annual series of tailored webinars focused on hot topics, trends, and key developments in the technology industry that are of essential importance to our friends and clients. Now in its 12th year, our expansive curriculum kicks off in May and continues into June.

For more information:

<https://www.morganlewis.com/events/technology-marathon>

Presenters

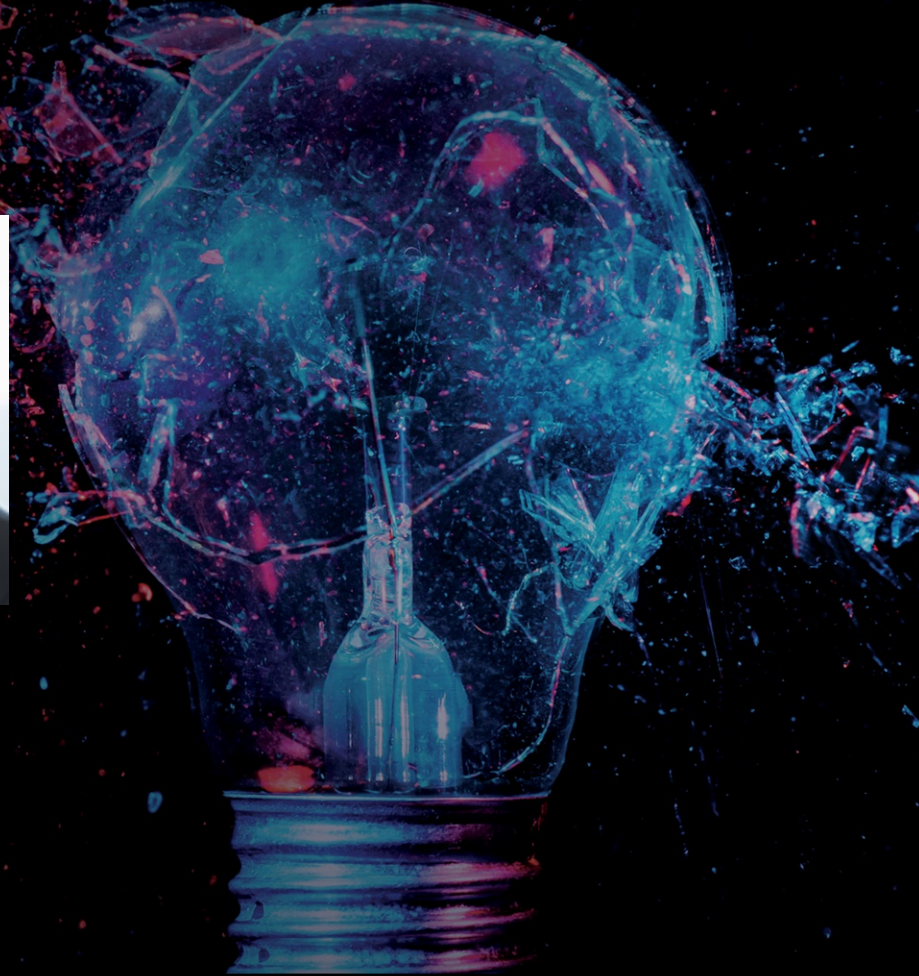


Mike Pierides



Peter M. Watt-Morse

Morgan Lewis



Before we begin

Tech Support

If you are experiencing technical difficulties, please contact WebEx Tech Support at +1.866.779.3239.

Q&A

The Q&A tab is located near the bottom right hand side of your screen; choose "All Panelists" before clicking "Send."

CLE

We will mention a code at some point during the presentation for attendees who requested CLE. Please make note of that code, and insert it in the pop-up survey that will appear in a new browser tab after you exit out of this webinar. You will receive a Certificate of Attendance from our CLE team in approximately 30 to 45 days.

Audio

You will hear sound through your computer speakers/headphones automatically. Make sure your speakers are ON and UNMUTED.

To access the audio for by telephone, please click the "phone" icon below your name on the Participants Panel for teleconference information.

AGENDA

1 A Brief Overview of the Metaverse and the Legal Challenges It Will Present

2 NFTs: Key Considerations for Rights Clearance

3 ESMA Publishes Guidelines on Outsourcing to Cloud Service Providers

4 Cracks in the Confidentiality Exception Boilerplate

5 Phishing for Force Majeure – What's the Catch?

6 Service Level Methodology Basics – 10 Key Components

7 Considerations for Updating Standard Contractual Clauses

8 Suspension Rights in SaaS Agreements

A Brief Overview of the Metaverse and the Legal Challenges it Will Present

Morgan Lewis



Metaverse

What is it?

- A virtual-reality space in which users interact with each other using avatars.

Types of Metaverse platforms

- **Blockchain-based:** Allows users to purchase land and build environments using non-fungible tokens & cryptocurrencies (e.g. Decentraland).
- **A general virtual world:** Users can, via a virtual economy, work, play, or socialize (e.g. Minecraft).

How will it develop?

- Both Artificial Intelligence & machine learning will play key roles in the development of the metaverse.

The Aim

- To merge physical reality and the digital universe in the ultimate culmination of virtual reality and augmented reality.

Metaverse: Legal Implications

1. Collaboration

The success of the metaverse depends on accessibility, e.g.:

- tech companies agreeing a standard for creating/operating platforms;
- companies licensing the rights to use another company's underlying technology in building its own metaverse.

2. IP Ownership Issues

Virtual creation by avatars and/or AI may be denied IP protections as they are not deemed human creations.

The US patent and copyright right law operates on the basis of human authorship.

3. Protecting Copyright

Policing copyright infringement on the metaverse could prove difficult.

Content licensees should review their license agreements to ensure that they have the right to use the licensed content in the metaverse, as many license agreements may not have anticipated its use in such forums.

NFTs: Key Considerations for Rights Clearance

Morgan Lewis



Non-fungible Tokens (NFTs)

Definition:

An NFT is a unique blockchain-based token that records ownership of a digital or physical asset (like a deed to a house).

Transfer

Allows documentation of transfer of ownership without transferring physical asset and without third party recording entity (no need for Recorder of Deeds)



Non-fungible Tokens (NFTs)

Use-cases

NFTs are commonly used to document ownership of sports memorabilia, artwork, videos, images gaming assets, digital collectables or other creative content.



[#13] Off-White™ x Nike Air Jordan 1 "Chicago" Rare NFT Jordan 1 Series

23 owned by Sneakerhead-NFT  170 views  5 favorites

 [Make offer](#)

Key Considerations Relating to Rights Clearance and NFTs

An NFT is a token, not the underlying asset

- Creation or ownership of an NFT does not mean that the owner has the intellectual property rights in the underlying asset.
- If the NFT-linked work is an exact copy of a copyrighted work, then this could infringe on the rights of the copyright owner.
- To create an NFT (known as "minting"), you must either own the underlying asset or have the right to mint and sell the NFT.

Verify your rights in the underlying asset, first

- Before minting an NFT associated with a particular asset for commercial purposes, you should verify what rights you have in the asset and whether they extend to the creation and use of NFTs.
- As per copyright and trademark laws, minting NFTs without the requisite ownership, consent, or rights, could result in you accounting to the various right holders for any profits made.

Document the transfer of rights

- The best practice for obtaining the necessary underlying rights in an asset would be through an express grant in writing.
- The same applies where you use third-party IP to create an asset e.g. a license granting the right to use music in the creation of a video, may allow for the video to be distributed online but the license might not extend to creating an NFT from the video which incorporates the music.

Key Considerations Relating to Rights Clearance and NFTs

Do not forget about names and likenesses

- The common law right of publicity prevents the unauthorized commercial use of a person's name, likeness, or recognizable aspects of an individual's persona without their consent therefore minting and selling an NFT which incorporates one or more of these aspects may violate such rights.

Review terms of service of NFT marketplaces

- Terms of use can vary between NFT marketplaces or platforms; it is common for it to require minters to represent and warrant that they have obtained all rights, licenses, consents, and permissions to create, display, and sell an NFT.



ESMA Publishes Guidelines on Outsourcing to Cloud Service Providers

Morgan Lewis

ESMA Guidelines

Purpose

In 2021, the European Securities and Markets Authority (ESMA) published guidelines (ESMA Guidelines) to help firms and competent authorities identify, address, and monitor the risks and challenges posed by cloud outsourcing arrangements.

Application

The ESMA Guidelines apply to:

- investment firms;
- alternative investment fund managers;
- undertakings for collective investment in transferable securities (UCITS);
- management companies and depositaries of alternative investment funds and of UCITS; and
- central counterparties, and central securities depositaries operating in the EU.

Scope

The ESMA Guidelines became effective from July 31, 2021, and affect:

- all in-scope cloud outsourcing arrangements agreed, renewed, or amended on or after that date; and
- existing agreements. Companies must review/amend existing agreements to ensure compliance by December 31, 2022.

Definition

The ESMA Guidelines contain nine principles, some of which refer, or are limited in application, to the outsourcing of “critical or important functions”, defined as any function whose defect or performance-failure would materially impair:

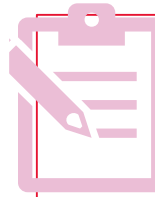
- a firm's compliance with its obligations under the applicable legislation;
- a firm's financial performance; or
- the soundness or continuity of a firm's main services and activities.

The Nine Principles



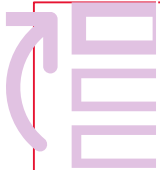
1. Governance, oversight, and documentation

Firms should have up-to-date cloud outsourcing strategies including an oversight function, undergo periodic re-assessment of such arrangements, and ensure accurate record-keeping.



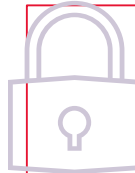
2. Pre-outsourcing analysis and due diligence

Outsourcing important or critical functions requires a detailed pre-outsourcing analysis and due diligence on the prospective cloud service provider that is proportionate to the nature, scale, and complexity of the outsourced function.



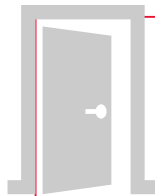
3. Key contractual elements

Cloud outsourcing agreements should include (a) an express right for a firm to terminate “where necessary”; (b) a clear description of the outsourced function; (c) whether sub-outsourcing is permitted; (d) locations in which data will be processed and stored; (e) service levels including performance targets; and (f) access and audit rights for the firm and its competent authorities.



4. Information security

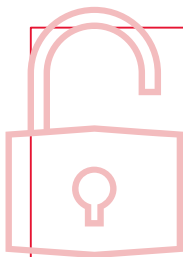
In addition to establishing information security requirements through internal policies, procedures, and cloud outsourcing agreements, ESMA imposes specific requirements on firms outsourcing a critical or important functions such as identity and access management, use of encryption technologies, and business continuity and disaster recovery controls.



5. Exit strategies

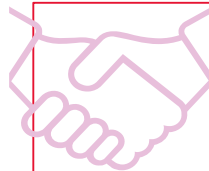
Where an outsourced arrangement includes a critical or important function, ESMA requires firms to have established mechanisms to ensure that it can exit the arrangement e.g.: defined trigger events, tested exit plans, transitional service agreements.

The Nine Principles



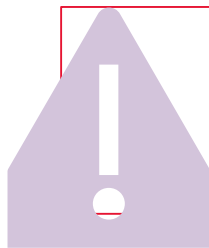
6. Access and audit rights

The written agreement should not limit a firm's and competent authority's effective exercise of the access and audit rights and oversight options over the cloud service provider.



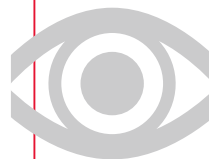
7. Sub-outsourcing

Clear controls should be incorporated into agreements that permit sub-outsourcing of critical or important functions e.g. conditions for sub-outsourcing, require service provider to give prior written notice of its intention to sub-outsource, and appropriate termination rights if a firm objects to the sub-outsourcing.



8. Notification

Firms should notify their relevant competent authority (in writing) of cloud outsourcing involving a critical or important function.



9. Supervision

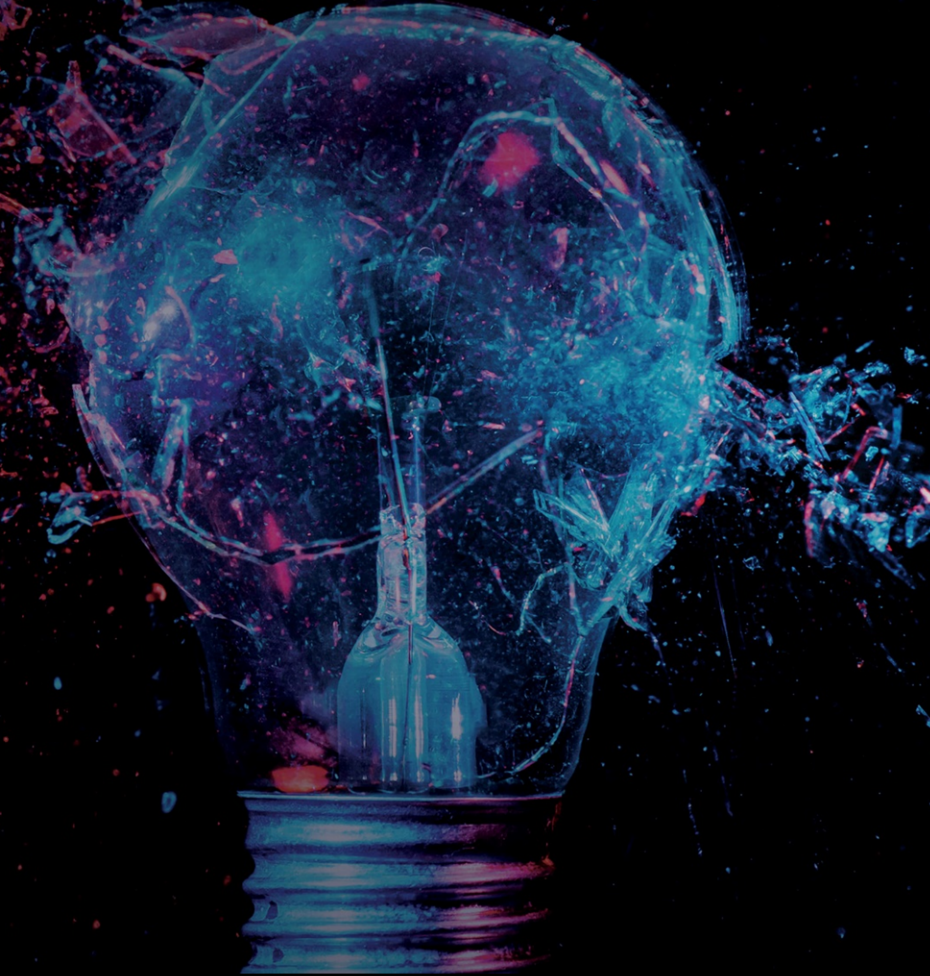
Competent authorities should perform effective supervision, particularly, on firms outsourcing critical or important functions that are performed outside of the EU.



ESMA Guidelines do not apply to firms operating only in the UK; the UK Prudential Regulation Authority's supervisory statement should be the primary source of reference when the firm is operating solely in the UK.

2022 Contract Corner Updates

Morgan Lewis



Cracks in the Confidentiality Exception Boilerplate

Morgan Lewis



Confidentiality Provisions: Pre-drafting Considerations

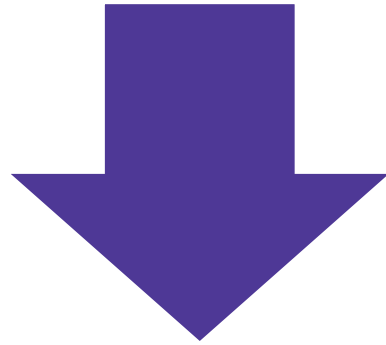
Repurpose?

Repurposing confidentiality provisions, e.g. non-disclosure agreements (NDAs), during a contract drafting process may undermine the key aims of the transaction.

Context

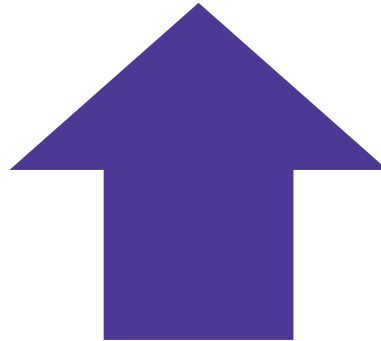
Although an NDA often seems like a logical starting point, it may not be appropriate in the context of a commercial or a corporate transaction.

Context: NDAs vs Commercial Transactions



NDA: Parties engage in a preliminary discussion during which each party discloses some of its confidential information.

Commercial & Corporate Transactions: Many contracts exist within a larger context resulting in the scope of each party's confidential information not being clear-cut e.g. prior affiliation.



Common Issues



A template NDA may be incompatible where one party is already in possession of the other's confidential information e.g. due to a prior affiliation during which they had no obligation to treat that information as confidential.



Some parties attempt to protect their critical proprietary materials by listing them (without limitation) within the definition of "Confidential Information", however, traditional confidentiality exceptions may erode such safeguards. Therefore, the scope of such exceptions should be reviewed for any unintended consequences.

Confidentiality Exceptions: Suggested Re-drafting Points

1. Confidential Information excludes information that:
 - (i) without any breach of this Agreement, or through any wrongful act or omission by or on behalf of the Receiving Party, is or becomes generally known to the public;
 - (ii) was in the Receiving Party's possession or known by it prior to receipt from the Disclosing Party or its affiliates ~~the Effective Date~~;
 - (iii) is rightfully disclosed to the Receiving Party by a third party without restriction, if the Receiving Party reasonably believed that such third party had the right to make the disclosure; or
 - (iv) is independently ~~developed~~ [Note to lawyer: Independent of what? The performance of the Agreement? The parties' relationship?] developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

Key Take-aways



Confidentiality exceptions should not be set in stone – they should fit the contemplated circumstances.

Exceptions could also be framed as carve-outs to the confidentiality obligations instead of exceptions to the definition of Confidential Information.

Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:

XY765TD

Phishing for Force Majeure – What's the Catch?

Morgan Lewis



Anticipated Issues: Force Majeure

With the recent increase of ransomware attacks, it's time to revisit force majeure clauses (again). Previous reviews concentrated on the impact of Covid-19 on force majeure provisions.

With the increase of ransomware attacks causing firms to worry about security and the implications of disruptions to its wider supply chain, force majeure provisions may, again be under attack.



Excusing Non-performance due to a Cyber Attack?

Issues to Consider



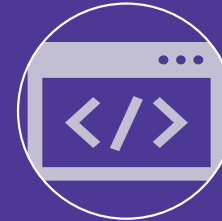
Control

Is a cyber attack beyond the party's reasonable control or could the party have avoided or mitigated the attack by exercising reasonable precautions. Did the cyber attack result from the party's negligence or any breach of its obligations?



Supply Chain Failures

Does the force majeure provision include a failure of the party's suppliers, subcontractors, data providers, or other third parties? To what extent should a party be responsible for the acts or omissions of the third party?



Issues of Interpretation

Should cyber-risks be specifically included in the list of force majeure events, or will the non-performing party try to rely on the "beyond its reasonable control" catchall language?

Excusing Non-performance due to a Cyber Attack?

Issues to Consider



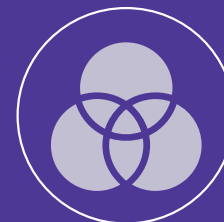
Mandatory Performance

Even if a cyber attack falls within the scope of a force majeure event, is it appropriate to nonetheless require a party to perform some of its obligations? E.g. to implement its disaster recovery and business continuity plans?



Mitigation

If the excused party is required to resume performance as soon as possible, does this mean that the excused party must pay the ransom in order to minimize downtime and mitigate the impact? Cost of ransomware vs. damages from downtime and market/governmental practices



Drafting

Force majeure concepts can creep into other parts of a contract beyond the "Force Majeure" section. If a vendor excludes certain circumstances from service level or warranty obligations, such exceptions should match the general force majeure provision.

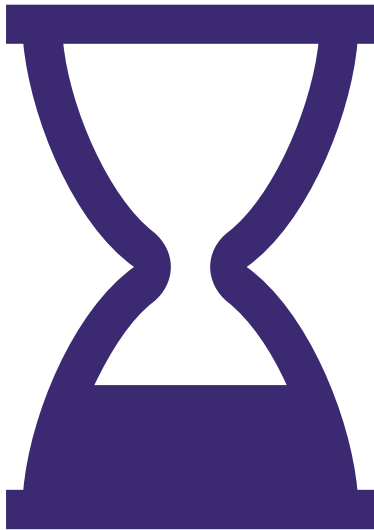
Other Considerations

Is cybersecurity an important aspect of the business relationship? Is the vendor providing hosting or other cybersecurity-related services? If so, excused performance for force majeure event may be more limited for cybersecurity event.

If the cyber incident is a force majeure event then consider incorporating the pre-agreed commercial and operational remedies e.g.:

- partial refund or termination rights:
and/or
- reimbursement for costs incurred in implementing a replacement service.

Conclusion



It is important to note that the applicability of force majeure clauses is dependent on the precise language of the clause, the particular facts of the event and services and, in the United States, state contract law which varies between states. In addition, outside the United States, the applicable law and interpretation of force majeure provisions can vary widely.

Service Level Methodology Basics – 10 Key Components

Morgan Lewis



The Benefits

In the last year, there has been a significant shift to the use of “as a service” models, cloud solutions, and outsourcing as a means of enabling scalability, improving services, and accelerating access to in-demand resources. This increased reliance on vendor performance to enable business operations has underscored the importance of implementing a solid service level methodology in order to:

- 1
align performance metrics with business requirements
- 2
measure, monitor, and report performance against the metrics
- 3
establish remedies for service level defaults e.g. service level credits
- 4
agree to events which may excuse performance

10 Key Components to Consider when Negotiating a Services Contract:

1. Establishing metrics based on

- a) a continuous availability of the services;
- b) a specific requirement (e.g. does supplier provide service at required time); or
- c) quantitative measures (e.g. number of errors; response time)

2. Minimum metrics

Performance standards should meet expectations and be achievable therefore parties may consider differentiating between “expected” and “target” metrics which attract different credit mechanisms.

3. Critical vs key service levels

Consider distinguishing between business critical and key service levels with clear consequences for missed service levels (root cause investigation, remediation, credits).

10 Key Components to Consider when Negotiating a Services Contract:

4. Monitoring tools

Monitoring tools should be able to monitor the full scope of metrics and relevant services and part of normal ongoing operations.

5. Reporting

Reporting usually aligns with the metric duration; trend analyses across reporting periods are also common.

6. Continuous improvement

Improvement of performance standards through formal review processes and/or automatic increases in service levels at certain milestones.

7. Service Level Credits

Parties agree on fee credits for failures for certain critical service levels - may have ramp-up period and have potential earn-back or bonus amounts for vendors for superior performance.

10 Key Components to Consider when Negotiating a Services Contract:

8. Right to make changes

Consider including the right (with or without consent) to make event-specific changes to services levels e.g.:

- a) promotion/demotion of critical and key service levels;
- b) changing the metric or at-risk amount; and/or
- c) adding/deleting service levels.

9. Termination rights

Consider termination rights for certain critical services or repeated breaches e.g.:

- a) whether termination in whole, or in part, are permitted; and
- b) any special notice periods for such termination rights; and/or

10. Excused events

Consider addressing occurrences for which the supplier would be excused for missing service level metrics e.g. customer dependency failures; force majeure; appropriate adjustment of the service level metrics and any credits/incentives.

Considerations for Updating Standard Contractual Clauses

Morgan Lewis



NEW SCCs

In 2021, the European Commission adopted its updated Standard Contractual Clause (New SCCs) for use by organizations transferring personal data outside of the European Economic Area (EEA) to third countries that do not provide adequate protections in respect of personal data.



Organizations Should Consider

Timing

Use of the new SCCs is mandatory for contracts concluded on or after September 27, 2021. Use of SCCs concluded prior to this date (Old SCCs) continue to be permitted provided that (a) they are updated to the new SCCs by December 27, 2022; and (b) they are subject to the requirement to implement supplementary measures pursuant to the *Schrems II* judgement.

Contract Audit

Organizations should undertake full audits of their contracts involving international transfers of personal data to check:

- a) if the contracts currently contain SCC? If not, are they required?
- b) What type(s) of transfer are being undertaken (See Module section below)?
- c) Is the data subject to UK and/or EU GDPR?
- d) If any *Schrems II* supplementary measures are currently being implemented?

Organizations Should Consider:

Roadmap

Once Organizations are clear on their position in respect of SCCs, they should formulate a roadmap to compliance by the deadline. Reviewing, updating, and engaging contract counterparties as soon as possible will provide the best chance to achieve compliance by the deadline.

Module

The New SCCs are split into modules that deal with four types of transfers:

- a) Controller to Controller
- b) Controller to Processor
- c) Processor to Processor
- d) Processor to Controller

Organizations should adopt the appropriate module to cover the type of transfer being undertaken.

Compliance Review

The New SCCs impose several substantive obligations on the parties and organizations should ensure that they fully review these obligations to ensure compliance.

Organizations Should Consider:

Schrems II Supplementary measures

While the New SCCs are designed to work with the *Schrems II* judgment, organizations will still need to assess whether additional supplementary measures are required to provide adequate protections for data being transferred pursuant to the New SCCs.

United Kingdom

***Update**

The UK's Information Commissioner's Office (ICO) recently issued an International Data Transfer Addendum to the New SCCs (Addendum) for organizations transferring personal data that are subject to UK GDPR.



SCCs are not currently required for the transfer of personal data between the EEA and the United Kingdom following the European Commission's adequacy decision on June 28, 2021.

Suspension Rights in SaaS Agreements

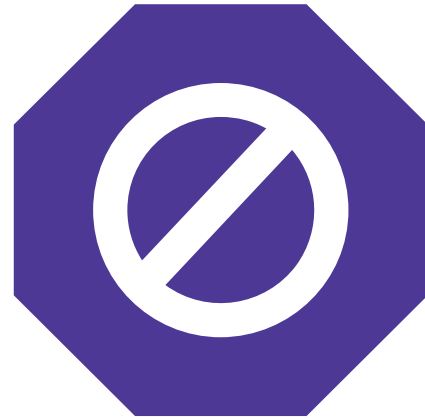
Morgan Lewis



SaaS: Template Suspension Provisions

Software as a service (SaaS) form agreements often contain one or more provisions giving the vendor favorable rights to suspend the services being provided under the contract. E.g. suspension rights relating to:

- non-payment;
- security issues;
- disruptive use of the services; and
- violation of law through use of the services.



Impact of Suspension

If suspension of the services could have disastrous consequences for the business, review substituting suspension rights with alternative methods for addressing concerns (alternative payments (up-front, letter of credit), heightened security measures, etc.)



Suspension Rights: Additional Considerations



Trigger: Review reasons for suspension and should they be limited? E.g. use of the services in violation of law may result in a suspension right, but non-payment does not (Dispute issues).



Discretion: Is the exercise of a suspension right at the vendor's sole, reasonable, or other standard of discretion?



Notice: Is the vendor required to give prior notice of suspension, how much notice is required, and is the customer given the opportunity to cure the issue prior to suspension?



Duration: Suspension should only last for the duration of the violation or until mitigative steps are taken and the vendor should restore the services immediately after violation is cured or threats mitigated.



Requested suspension: if applicable, may add right for customer to request that vendor suspend its services e.g. if the services pose a threat to the security of the customer's systems.

Your CLE Credit Information

For ALL attorneys seeking CLE credit for attending this webinar, please write down the alphanumeric code on the right >>

Kindly insert this code in the **pop-up survey** that will appear in a new browser tab after you exit out of this webinar.

THE CLE CODE IS:

XY765TD

Biography



Mike Pierides

London

T +44.20.3201.5686

E mike.pierides
@morganlewis.com

Mike Pierides' practice encompasses a wide breadth of commercial and technology transactions. Mike advises on major outsourcings, strategic restructurings following divestments or acquisitions, and technology-specific transactions such as licensing and "as a service" arrangements. He is also active advising on new technologies such as blockchain and artificial intelligence.

His clients include companies across a multitude of sectors, including technology, financial services, aviation and telecommunications. Within the financial services sector, he advises a wide range of clients, including retail banks, investment banks, investment managers, payments providers, and others. Mike has also worked at the intersection of financial services compliance and technology, advising clients on their related systems and compliance procedures. Mike represents both customers and suppliers, allowing him to bring opposing parties' perspectives to transactions.

Mike is recognized by Chambers UK as an authority on outsourcing and information technology and is highly regarded for his work on complicated BPO and information technology outsourcing (ITO) transactions. Clients and sources told Chambers that Mike "[has] excellent understanding of our sector and the services we provide...", that "he is particularly strong around the negotiating table," and that "he leads from the front rather than merely offering opinion."

Mike was also nominated as an Acritas Star Lawyer, with a client noting he is "an expert in the industry and in the specific subject matter that we've asked advice on. He has really helped to move the deal forward by being proactive. Excellent project management skills as well."

Biography



Peter M. Watt-Morse

Pittsburgh, PA

T +1.412.560.3320

E peter.watt-morse
@morganlewis.com

Peter M. Watt-Morse, one of the founding partners of the firm's Pittsburgh office, has worked on all forms of commercial and technology transactions for more than 30 years. Peter works on business and intellectual property (IP) matters for a broad range of clients, including software, hardware, networking, and other technology clients, pharmaceutical companies, healthcare providers and payors, and other clients in the life science industry. He also represents banks, investment advisers, and other financial services institutions.

Peter advises companies on business process (BP) and information technology (IT) outsourcing transactions. He also handles technology acquisition, development, licensing, and distribution agreements; strategic alliances and joint ventures; IP creation and strategy; university and governmental technology transfer issues; and general corporate and commercial matters.

Peter developed innovative outsourcing arrangements for clinical trial services for major pharmaceutical companies and essential back-office operations of banks and investment advisors. The equity/license structure Peter developed helped launch the commercialization of revolutionary semiconductor technology for the networking industry. On behalf of consumer product and manufacturing clients, Peter has created long-term supply arrangements for essential commodities and components. He has also developed complex intellectual property agreements to carve up technologies in divestiture transactions, and cutting-edge agreements and procedures regarding e-commerce.

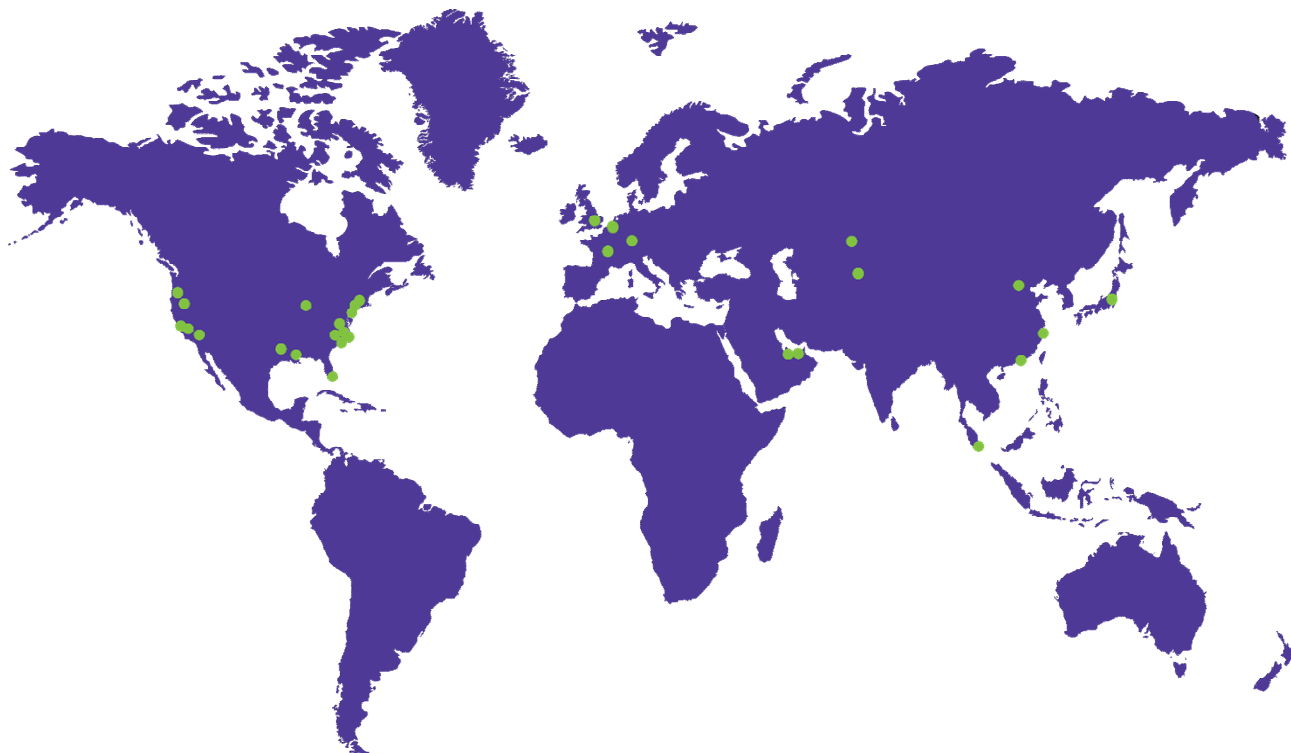
Peter is an adjunct professor at the University of Pittsburgh Law School, where he teaches classes related to technology transactions and IP. He frequently speaks and writes about outsourcing, IP, and technology-related topics, including an annual seminar he moderates on Internet Law. He also has an extensive background in technology use in the practice of law and is past chairman of Morgan Lewis's Technology Steering Committee.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2022 Morgan, Lewis & Bockius LLP
© 2022 Morgan Lewis Stamford LLC
© 2022 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorized and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.